CRIPTOGRAFÍA Y CINE

Análisis y uso didáctico de la representación de la criptografía en el cine

David Fajardo Rodríguez

Máster Universitario en Ciberseguridad y Privacidad

Protocolos criptográficos y aplicaciones de seguridad

Nombre Tutor de TF

Rafael Páez Reyes

Profesor/a responsable de la asignatura

Andreu Pere Isern Deyà

Cristina Pérez Solà

Enero 2023

Universitat Oberta de Catalunya

AGRADECIMIENTOS

A Elisabet,
por las horas y las pelis.

A Noe,
por la compañía en rutas agrestes.

A Rafael,
por la ayuda para elaborar este proyecto.

A mi familia y amigos,
por el cariño y el apoyo.

"I believe a leave of grass is no less
than the journey-work of the stars"
Walt Whitman

RESUMEN

El cine ha reflejado en multitud de ocasiones escenas de la vida diaria pero también momentos históricos más que conocidos (entre ellos, muchas batallas), lugares existentes o míticos, vidas de personajes famosos y formas distintas de entender la vida humana desde un punto de vista sociológico y psicológico. Sin embargo, las disciplinas técnicas y científicas han tenido peor acomodo en el cine. La ciencia y la tecnología son más complejas de explicar desde un punto de vista narrativo y se suelen contentar con apariciones breves, en ocasiones funcionales y con una discutible semejanza a la realidad. Centrándonos en la criptografía, los sistemas de códigos y criptográficos han formado parte de la humanidad desde hace miles de años, en variadas formas y con importante implicación en la historia. ¿Cómo ha representado el cine esa historia de la criptografía?

El objetivo de este trabajo de fin de Máster es el de evaluar esa representación a partir de una serie de conceptos criptográficos o momentos dentro de la historia de la criptografía y de un listado de películas que los contengan. Adicionalmente, se busca poder usar esa correlación entre los materiales para construir un proyecto divulgativo que permita explicar partes de la historia de la criptografía apoyándonos en un medio de gran alcance como es el cine.

ABSTRACT

Cinema has often reflected scenes from everyday life, but also more than well-known historical moments (including many battles), existing or mythical places, the lives of famous people and different ways of understanding human life from a sociological and psychological point of view. However, technical and scientific disciplines have been less well represented in cinema. Science and technology are more complex to explain from a narrative point of view and are usually satisfied with brief appearances, sometimes functional and with a debatable resemblance to reality. Focusing on cryptography, code and cryptographic systems have been part of humanity for thousands of years, in various forms and with important implications in history. How has cinema represented the history of cryptography?

The objective of this Master's thesis is to evaluate this representation based on a series of cryptographic concepts or moments in the history of cryptography and a list of films that contain them. Additionally, the aim is to be able to use this correlation between the materials to build an educational project to explain parts of the history of cryptography using the powerful medium of cinema.

CONTENIDO

1. INTRODUCCIÓN 1
1.1. Contexto y justificación del trabajo 1
1.2. Objetivos del trabajo 2
1.3. Impacto en sostenibilidad, ético-social y de diversidad 3
1.4. Enfoque y método seguido 4
1.5. Planificación del trabajo 6
1.6. Breve sumario de productos obtenidos 10
1.7. Breve descripción de los otros capítulos de la memoria 10
1.8. Riesgos 11
1.9. Estado del arte 13
2. CRIPTOGRAFÍA: HISTORIA Y SELECCIÓN DE CONCEPTOS 14
2.1. Una aproximación inicial 14
2.2. Breve historia de la criptografía 15
2.2.1. Criptografía clásica 17
2.2.2. El cifrado de sustitución monoalfabético y su criptoanálisis 19
2.2.3. El camino hacia el cifrado de sustitución polialfabético 21
2.2.4. Cifrados de sustitución polialfabéticos 24
2.2.5. Primera Guerra Mundial 28
2.2.6. Segunda Guerra Mundial 29
2.2.7. Criptografía moderna 32
3. FILMOGRAFÍA: SELECCION 35
4. EVALUACIÓN DE PELÍCULAS 37
4.1. The Numbers Station (Código de defensa) 37
4.2. Midway (La batalla de Midway) 40
4.3. Red Sparrow (Gorrión rojo) 42
4.4. Harry Potter and the Chamber of Secrets (Harry Potter y la cámara secreta) 44
4.5. National treasure (La búsqueda) 45
4.6. National treasure 2: book of secrets (La búsqueda 2: El diario secreto) 47
4.7. Los crímenes de Oxford 50
4.8. Gone in 60 Seconds (60 segundos) 52
4.9. Aelita, Queen of Mars 54
4.10. Now You see Me 2 (Ahora me ves 2) 56
4.11. All the Queen's Men 58
4.12. Batman Gotham by Gaslight (Batman Gotham a luz de gas) 60
4.13. Cipher Bureau 62
4.14. Cold Weather 65

4.15. Contact 67
4.16. From Russia With Love (Desde Rusia con amor) 69
4.17. Dope 71
4.18. The Da Vinci Code (El codigo Da Vinci) 73
4.19. The Fourth Protocol (El cuarto protocolo) 75
4.20. El escarabajo de oro 77
4.21. The Goldbug TV Special (El escarabajo de oro Especial televisión) 79
4.22. The Final Countdown (El final de la cuenta atrás) 81
4.23. The Falcon and the Snowman (El juego del halcón) 82
4.24. Enola Holmes 84
4.25. Enola Holmes 2 87
4.26. Sphere (Esfera) 90
4.27. Gravity Falls 92
4.28. A Christmas Story (Historias de Navidad) 95
4.29. Hunt 97
4.30. Johnny Mnemonic 99
4.31. Sharpe's Sword (La espada de Sharp) 101
4.32. Les Vampires 103
4.33. Manhunter (Hunter) 106
4.34. Mercury Rising (Al rojo vivo) 107
4.35. Midway 109
4.36. Murdoch Mysteries: The Prince and the Rebel 111
4.37. Paycheck 113
4.38. Rendezvous 115
4.39. Sebastian 117
4.40. Sherlock Holmes The Secret Weapon 120
4.41. Sherlock Holmes and the Valley of Fear 122
4.42. Sherlock Holmes: A Game of Shadows (Sherlock Holmes: Juego de sombras) 124
4.43. Sneakers (Los fisgones) 126
4.44. Snowden 128
4.45. Stargate (Stargate, puerta a las estrellas) 130
4.46. Summer Wars 132
4.47. The Bit Player 134
4.48. The Imitation Game (Descifrando Enigma) 136
4.49. Feng sheng. The Message 138
4.50. The Red Machine 140
4.51. The Silent War 142
4.52. The Thomas Beale Cipher 144
4.53. The Man Who Never Was (El hombre que nunca existió) 147
4.54. Travelling Salesman 149
4.55. U-571 151

4.56. A Beautiful Mind (Una mente maravillosa) 153
4.57. Lemony Snicket's a Series of Unfortunate Events (Una serie de catastróficas desdichas de Lemony Snicket) 155
4.58. Viaje al centro de la Tierra 157
4.59. Windtalkers 159
4.60. Zodiac 161
5. EVALUACIÓN GLOBAL Y LÍNEAS DE TIEMPO 164
5.1. Distribuciones por género y década 164
5.2. Distribución por país 166
5.3. Evaluación de los conceptos según definición, funcionamiento y representación 167
5.4. Distribuciones por avance de trama, reutilización y marketing 172
5.5. Conclusiones del análisis 174
6. PROYECTO DIDÁCTICO 177
6.1. Descripción general del curso 177
6.2. Público destinatario del curso 177
6.3. Competencias generales 178
6.4. Objetivos del curso 178
6.5. Actividades de evaluación 178
6.6. Distribución de contenidos del curso completo 179
6.7. Materiales generales del curso 180
6.8. Detalle de unidad didáctica de ejemplo 180
7. CONCLUSIONES Y TRABAJO FUTURO 182
8. GLOSARIO DE TÉRMINOS 185
9. BIBLIOGRAFÍA 188
ANEXO I. LISTADO DE PELÍCULAS 190
ANEXO II. PELÍCULAS ANALIZADAS 196

LISTA DE FIGURAS

Figura 1: Diagrama de Gantt 9
Figura 2: Micropuntos encontrados en 1961 en posesión de Helen Kroger 16
Figura 3: Ejemplo de escítala (Singh, 2000) 17
Figura 4: Cuadrado de Polibio que se usa para este cifrado 18
Figura 5: Piedra Rotbrunna y codificación de runas 18
Figura 6: cifrado Atbash en hebreo y correspondencia al español 20
Figura 7: Nomenclátor utilizado por María Estuardo (Singh, 2000) 21
Figura 8: Los papeles Beale 23
Figura 9: Rejilla empleada en la serie TURN 23
Figura 10: Cifrado con una rejilla con desplazamiento 24
Figura 11: Discos de Alberti 25
Figura 12: Tabla de Vigenère 26
Figura 13: Máquina Enigma 30
Figura 14: The numbers station – Interior de la estación 38
Figura 15: The numbers station – Hoja de one time pad 39
Figura 16: The numbers station – Correo con mensaje oculto 39
Figura 17: Red Sparrow – Escítala 43
Figura 18: National Treasure – Mensaje que se hace visible con limón y calor 46
Figura 19: National Treasure – Código de sustitución por libro 46
Figura 20: National Treasure 2 – Cifrado Playfair 48
Figura 21: National Treasure 2 – Jeroglíficos 49
Figura 22: Gone in 60 seconds – Tinta invisible 53
Figura 23: Now you see me 2 – Tinta invisible 57
Figura 24: All the queen's men – Fábrica de la máquina Enigma 59
Figura 25: Batman Gotham by Gaslight – Cifra de sustitución, hombres danzantes 61
Figura 26: Cipher bureau – Interceptando mensajes 63
Figura 27: Cipher bureau – Análisis de frecuencias y doble transposición 64
Figura 28: Contact – Los mensajes extraterrestres cifrados 68
Figura 29: From Russia with Love – Máquina Lektor 70
Figura 30: The Da Vinci Code – Tinta invisible 74
Figura 31: The fourth protocol – Rejilla de Cardano 76
Figura 32: El escarabajo de oro – Mensaje en pergamino y copia en pizarra 78
Figura 33: The goldbug tv special – Mensaje en pergamino 80
Figura 34: The falcon and the snowman – Clave del día 83
Figura 35: The falcon and the snowman – Mensaje cifrado 83
Figura 36: Enola Holmes – Cifrado por transposición 85

Figura 37: Enola Holmes – Cifrado de sustitución 86
Figura 38: Enola Holmes 2 – Mensaje oculto 88
Figura 39: Enola Holmes 2 – Cifrado por libro 89
Figura 40: Enola Holmes 2 – Anagrama 89
Figura 41: Sphere – Cifrado de sustitución monoalfabético 91
Figura 42: Gravity falls – Cifrado Vigènere (clave, mensaje) 93
Figura 43: Gravity falls – Mensajes cifrados (César) 94
Figura 44: Gravity falls – Tinta invisible (forma parte de la trama) 94
Figura 45: A Christmas story – Anillo decodificador 96
Figura 46: Hunt – Cifrado con tabla 98
Figura 47: Johnny Mnemonic – Imágenes cifrado 100
Figura 48: Sharpe's sword– Descifrado del mensaje usando "Candide" 102
Figura 49: Les vampires – Código de transposición 104
Figura 50: Les vampires - Anagrama 105
Figura 51: Les vampires – Código numérico 105
Figura 52: Mercury rising – Pasatiempo con cifrado 108
Figura 53: Murdoch Mysteries – Rejilla de Cardano 112
Figura 54: Paycheck - Micropunto 114
Figura 55: Rendezvous – Oficina de cifrado y disco de cifrado 116
Figura 56: Sebastian – Algunos de los extraños esquemas usados 119
Figura 57: The secret weapon – Cifrado monoalfabético 121
Figura 58: Sherlock Holmes and the valley of fear – Cifrado por libro 123
Figura 59: Sherlock Holmes: A game of shadows – Cifrado por libro 125
Figura 60: Stargate – Jeroglíficos 131
Figura 61: Summer Wars – Mensaje y descifrado 133
Figura 62: The imitation game – Máquina de Turing 137
Figura 63: The message – Código Morse y cifrado de sustitución 139
Figura 64: The red machine – Máquina Red 141
Figura 65: The Thomas Beale Cipher – Noticias 145
Figura 66: The Thomas Beale Cipher – La máquina "Enigma" 145
Figura 67: The Thomas Beale Cipher – Papeles de Beale 146
Figura 68: The Thomas Beale Cipher – Juego "Meet me at platform seven" 146
Figura 69: The man who never was – Secráfono 148
Figura 70: U-571 – Máquina Enigma a capturar 152
Figura 71: U-571 – Máquina Enigma dentro del submarino alemán 152
Figura 72: Lemony Snicket – Escítala serpiente 156
Figura 73: Lemony Snicket – Mensaje escondido (sustitución simple) 156
Figura 74: Viaje al centro de la tierra – Cifrado por transposición 158
Figura 75: Windtalkers – Código navajo 160
Figura 76: Zodiac – Mensaje cifrado real enviado por el asesino del zodiaco 162
Figura 77: Zodiac – Mensaje recibido tal y como se muestra en la película 163

Figura 78: Zodiac – Analisis de frecuencias (símbolos dobles reemplazando la doble ll – se señalan dos pares)..... 163
Figura 79: Líneas de tiempo 176

1. INTRODUCCIÓN

1.1. Contexto y justificación del trabajo

A lo largo de la historia, una buena parte del arte ha mantenido una intención manifiesta de reflejar la realidad social del tiempo en el que se producía, o de otros pasados. La pintura, la escultura o la arquitectura, entre otras, han otorgado un lugar destacado a escenas cotidianas, al pensamiento de la época, a los momentos históricos relevantes, a las formas de vestir o a los lugares que resultaban importantes para el hombre. Con los años esta función más representativa del arte se ha visto alterada en mayor o menor medida y otras formas de comunicación han venido a ocupar parte de ese papel.

El cine, uno de los elementos que ocupan este trabajo, es un medio de masas, y un arte también, que cuenta historias, pero que a la vez ofrece una mirada sobre el hombre, sus costumbres, sus formas de ser y de hacer, los sitios en los que vive, las funciones que desarrolla, por nombrar sólo algunos de los miles de detalles que podemos encontrar en una película. El cine ha reflejado en multitud de ocasiones escenas de la vida diaria pero también momentos históricos más que conocidos (entre ellos, muchas batallas), lugares existentes o míticos, vidas de personajes famosos y formas distintas de entender la vida humana desde un punto de vista sociológico y psicológico. Este reflejo tiene mayor o menor detalle o está más cerca o más lejos de la realidad en función de la película, pero no faltan las investigaciones que se preguntan cómo el cine ha representado variados temas sociales o históricos, desde el feminismo a la representación LGTBIQ+, o desde el Antiguo Egipto a la guerra de Vietnam.

No obstante, las disciplinas técnicas y científicas han tenido peor acomodo en el cine. No es tan fácil encontrar películas que hablen de las matemáticas de Fermat, o que empleen las aportaciones de Einstein para algo que no se acerque demasiado a la ciencia ficción. La ciencia y la tecnología son más complejas de explicar desde un punto de vista narrativo y se suelen contentar con apariciones breves, en ocasiones funcionales y con una discutible semejanza a la realidad.

Y así llegamos a la criptografía, el centro de atención de este trabajo. Los sistemas de códigos y criptográficos han formado parte de la humanidad desde hace miles de años, en variadas formas y con importante implicación en la historia. Y, con esas investigaciones mencionadas anteriormente como inspiración, surge la pregunta: ¿Cómo ha representado el cine esa historia de la criptografía? ¿Se encontrarán reflejos fidedignos gracias a los cuales se puedan aprender algunos conceptos? ¿O

será un uso muy funcional y más cercano a la ficción necesaria para hacer avanzar una trama?

El objetivo de este trabajo de fin de Máster es el de evaluar esa representación a partir de una serie de conceptos criptográficos o momentos dentro de la historia de la criptografía y de un listado de películas que los contengan. Y una segunda aspiración es poder usar esa correlación entre los materiales para construir un proyecto didáctico o divulgativo que permita explicar partes de la historia de la criptografía apoyándonos en un medio de gran alcance como es el cine.

1.2. Objetivos del trabajo

El objetivo principal del presente trabajo es la evaluación de la representación de conceptos criptográficos en el cine y su uso en el planteamiento de un proyecto didáctico o divulgativo.

Este objetivo principal se apoya en la siguiente lista de objetivos parciales:

1. Seleccionar momentos históricos o conceptos criptográficos relevantes a partir del estudio de la historia de la criptografía.
2. Relacionar películas a partir de listados obtenidos durante la fase de investigación con los conceptos criptográficos.
3. Evaluar la representación del concepto o conceptos en cada película (completa o sólo escenas dentro de ella) utilizando una serie de criterios.
4. Construir líneas de tiempo, histórica y cinematográfica, que reflejen la relación entre las dos disciplinas.
5. Valorar globalmente la representación de la criptografía en el cine.
6. Plantear, a partir de los elementos anteriores, un proyecto didáctico o divulgativo que permita mostrar o enseñar la historia de la criptografía usando el cine como medio de apoyo. Este proyecto didáctico estará orientado a alumnos de ESO o Bachillerato, alumnos de cursos de tarde/noche o público general en conferencias.

Se determinan también una serie de objetivos de entrega:

1. Completar las entregas parciales siguiendo las instrucciones y respetando el plazo y formato requerido.
2. Escribir siguiendo los requerimientos de la UOC la memoria final del trabajo.
3. Elaboración del vídeo de presentación del trabajo.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Desde el punto de vista de la sostenibilidad, el impacto de este trabajo es inexistente. Esto se justifica porque se está desarrollando un trabajo de análisis que no va a generar ningún producto tecnológico o un proceso que pueda impactar en ninguna de las áreas de la sostenibilidad que se contemplan a la hora de realizar los trabajos de fin de master. Por el contrario, puedo considerar su impacto en temas éticos y de diversidad.

Desde un punto de vista ético, en primer lugar, hay un producto final presente en mi trabajo, el proyecto divulgativo o didáctico, que considero que podría llegar a muchos tipos de público y presentarles una disciplina compleja pero que forma parte de manera invisible de las vidas de todos. Y todo eso partiendo de elementos de la cultura de masas al alcance de mucha gente. Compartir conocimiento tiene por sí mismo la capacidad de impactar positivamente en la sociedad, ya sea por la vía directa de introducir ideas nuevas como por la indirecta de crear interés en personas jóvenes y no tan jóvenes para redirigir una carrera profesional.

Siguiendo con el análisis de la perspectiva ética, en segundo lugar, es necesario ser especialmente cuidadoso con la legislación en términos de propiedad intelectual a la hora de utilizar las películas seleccionadas para el análisis. Debo, en cada caso, proporcionar toda la información de las mismas y usarlas en el contexto académico.

En tercer lugar, desde un punto de vista ético y deontológico, es importante considerar el componente de análisis y evaluación de las películas. No es este un trabajo de crítica cinematográfica y no caben opiniones o consideraciones de este tipo, salvo las que tengan que ver con la representación de las tecnologías, siempre manteniendo el respeto por las obras y centrándome en el análisis más objetivo posible.

Desde un punto de vista de la diversidad, a la hora de realizar la investigación voy a considerar el cine de diferentes partes del mundo sin centrarme únicamente en el cine que proviene de Estados Unidos. Siendo plenamente consciente de que una gran parte de fuentes que voy a utilizar llegarán de ese país, voy a intentar diversificar y buscar películas de otros continentes que contengan elementos significativos de criptografía. Es importante desde el punto de vista de la diversidad, evitar selecciones sesgadas de películas, puesto que, con independencia de su creador o creadora o su origen, deben ser consideradas para el desarrollo de este trabajo.

Por último, me comprometo también a utilizar un lenguaje inclusivo de la manera más correcta posible y a considerar las fuentes encontradas con independencia de su autor u origen, siempre que puedan tener una aportación relevante para el desarrollo de la investigación.

1.4. Enfoque y método seguido

El enfoque de este trabajo de fin de master es principalmente de investigación y análisis con una parte final más práctica que tiene por objetivo crear un proyecto didáctico que se seguirá desarrollando en el futuro.

La metodología que se seguirá se resume en las siguientes fases:

1. Documentación sobre historia de la criptografía
2. Extracción de conceptos / momentos históricos criptográficos
3. Listado de películas
4. Consulta/visionado de las películas
5. Correlación entre películas y conceptos / momentos históricos
6. Evaluación de las películas con los criterios definidos

Los criterios que se emplearán para la evaluación de las películas o escenas son los que se presentan a continuación:

	Nombre del criterio	**Definición**	**Valor**
1	TIEMPO DE REPRESENTACIÓN	Tiempo que se dedica en la escena al concepto criptográfico representado	Se dará como valor el tiempo y un porcentaje del tiempo total del metraje
2	DEFINICIÓN	Aparición del nombre y descripción del concepto criptográfico representado.	1.INDEFINIDO (ni se dice el nombre ni se define) 2.PARCIAL (se dice el nombre o se define) 3.DEFINIDO (se dice el nombre y se define)
3	FUNCIONAMIENTO Y USO	Se muestra el funcionamiento del concepto criptográfico representado	1.NO MOSTRADO (no se ve el funcionamiento/uso) 2.INCORRECTO (el funcionamiento/uso del concepto no es real) 3.IMPRECISO (el funcionamiento/uso aparece, pero con información omitida; no se puede decir que está mal porque no se muestra totalmente)

			4.CORRECTO (el funcionamiento/uso es correcto)
4	REPRESENTACIÓN GRÁFICA	Representación en imagen del concepto	1.DRAMATIZADA (no se parece a la realidad) 2.NEUTRO (se parece sin precisión) 3.REALISTA (es una representación correcta)
5	AVANCE DE TRAMA	El concepto criptográfico avanza la trama o tiene aplicación funcional	Booleano, sí o no
6	REUTILIZACIÓN	Reutilización del concepto criptográfico en la misma película	Booleano, sí o no
7	REFERENCIAS EN MARKETING	Aparición de referencias al concepto en título/sinopsis/imagen publicitaria	Booleano, sí o no

Una vez finalizado el proceso de evaluación, forman también parte del enfoque de este trabajo la realización de los siguientes productos:

- líneas de tiempo histórica y fílmica paralelas
- evaluación global de la representación
- proyecto didáctico
    - definición del tema, enfoque y objetivos
    - público al que se dirige
    - temas y planificación
    - resumen de materiales y elementos de apoyo

Los hitos parciales, y en particular la segunda entrega parcial (PEC 2), permitirán evaluar la viabilidad del método y de todos los objetivos que se han planteado. En este punto será posible redefinir algunos de los objetivos y limitar todo aquello que no sea realizable en el tiempo que se ha previsto para la elaboración de este proyecto.

Las herramientas que se van a utilizar para recopilar la información son dos: por un lado, Google Drive para almacenamiento de documentación y versiones de las diferentes entregas del TMF y por el otro, un espacio Evernote, pues es una herramienta que he usado en el pasado en otros proyectos y es muy útil para guardar listados de recursos, almacenar informaciones más breves y preparar esbozos de las diferentes partes del TFM. En el mismo espacio Evernote voy a crear las fichas de

evaluación a las que luego accederé desde un dispositivo móvil para poder realizar los análisis más fácilmente mientras veo las películas. Las dos herramientas me sirven para almacenarlo todo online y facilitarme el desarrollo del proyecto donde quiera que esté, teniendo en cuenta que combino el TFM con otras ocupaciones y viajes de trabajo.

1.5. Planificación del trabajo

A continuación, se detallan las tareas que se realizarán en cada una de las fases del trabajo de fin de máster:

1. Planteamiento inicial

En esta fase inicial se elabora un planteamiento inicial del tema a estudiar con una búsqueda de documentación.

- 1.1. Documentación previa
  - Búsqueda inicial del estado del arte en el tema del trabajo.
- 1.2. Establecimiento de la orientación y el ámbito del trabajo
  - Se concretan objetivos y lista principal de tareas del trabajo.

2. Plan de trabajo

Se completa la primera fase del trabajo detallando el plan de trabajo que se presentará en el primer entregable (PEC 1). Este plan de trabajo contiene las siguientes tareas

- 2.1. Contexto y justificación
- 2.2. Metodología
- 2.3. Listado de tareas
- 2.4. Planificación: cálculo de tiempos para las tareas
- 2.5. Riesgos preliminares
- 2.6. Productos obtenidos

3. Historia de la criptografía

Esta tarea consistirá en la revisión de la documentación elegida sobre historia de la criptografía

- 3.1. Documentación
- 3.2. Selección de conceptos / momentos históricos
- 3.3. Explicación de los conceptos (imagen gráfica, definición breve)

4. Listado de películas

Elaborar un listado de películas que contengan elementos de criptografía y documentación breve sobre las películas. Esta tarea acabará con una selección inicial, si es necesario después de obtener las listas.

- 3.1. Búsqueda de lista de películas que contengan temas de criptografía
- 3.2. Documentación breve de las películas
- 3.3. Selección

5. Evaluación de películas

En esta tarea se identifica cada película con conceptos criptográficos, se hace una pequeña ficha de ellas con datos básicos de producción y se evalúa según los criterios definidos en el apartado de metodología.

- 5.1. Visionado detallado y análisis
- 5.2. Identificación con un concepto criptográfico
- 5.3. Elaboración de ficha con datos básicos
- 5.4. Evaluación según criterios

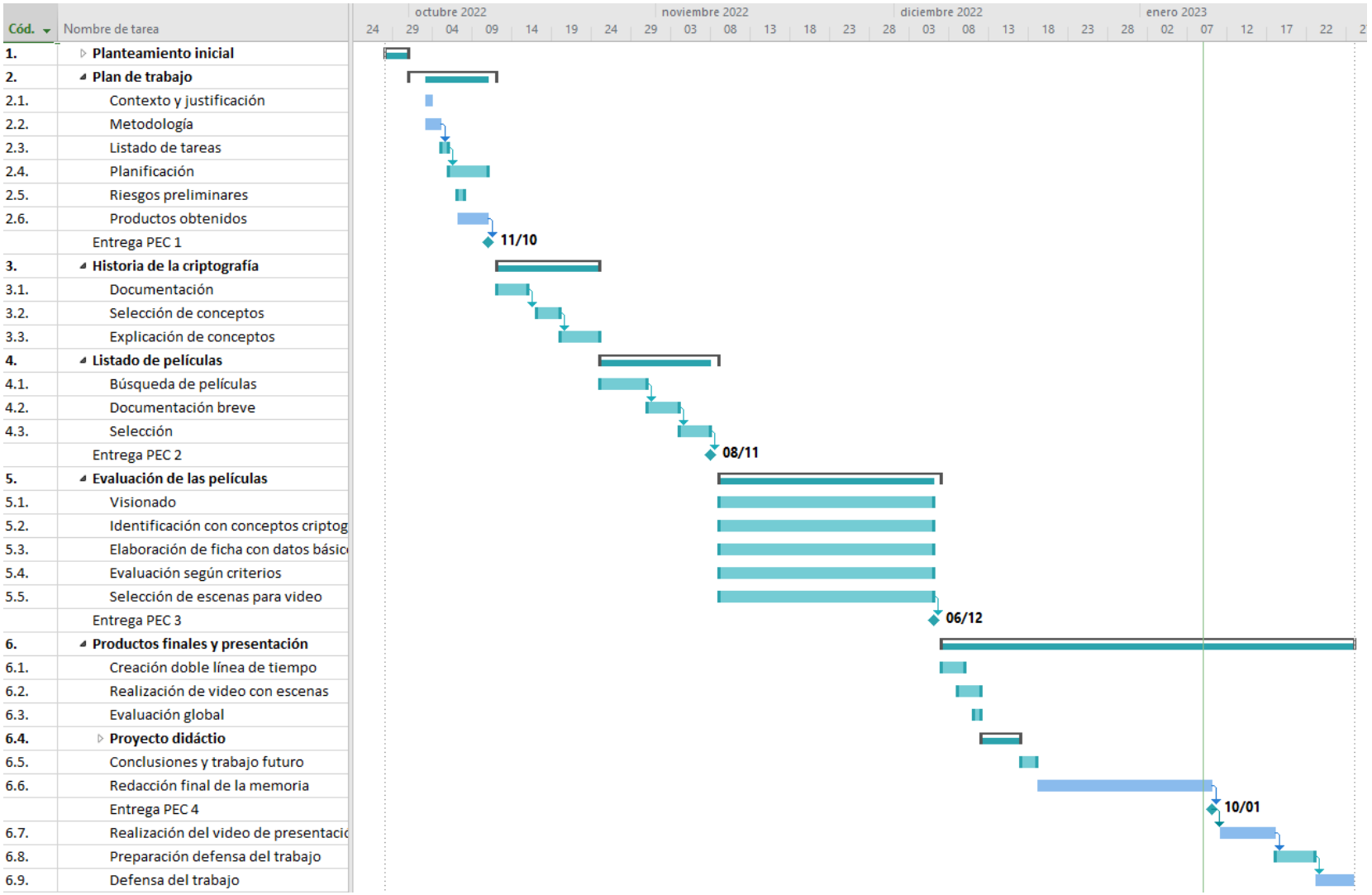
6. Productos finales y presentación

- 6.1. Finalizar fichas de películas
- 6.2. Creación de la doble línea de tiempo
  (momentos históricos de la criptografía versus representación fílmica)
- 6.3. Evaluación global
- 6.4. Proyecto didáctico
  - 6.4.1. Definición del tema, enfoque, objetivos y público al que se dirige
  - 6.4.2. Temas y planificación
  - 6.4.3. Resumen de materiales y elementos de apoyo
- 6.5. Conclusiones y trabajo futuro
- 6.6. Redacción de la versión final de la memoria
- 6.7. Realización del vídeo de presentación
- 6.8. Defensa del trabajo

A continuación, se presenta la planificación que se ha hecho de las tareas en días y una vista general del diagrama de Gantt.

Planificación temporal mediante Diagrama de Gantt

Cód.	Nombre de tarea	Duración	Comienzo	Fin
	Trabajo final de máster	**88 días**	**28/09/2022**	**27/01/2023**
1.	**Planteamiento inicial**	**3 días**	**28/09/2022**	**30/09/2022**
1.1.	Documentación previa	2 días	28/09/2022	29/09/2022
1.2.	Orientación y ámbito de trabajo	1 día	30/09/2022	30/09/2022
2.	**Plan de trabajo**	**7 días**	**01/10/2022**	**11/10/2022**
2.1.	Contexto y justificación	1 día	03/10/2022	03/10/2022
2.2.	Metodología	2 días	03/10/2022	04/10/2022
2.3.	Listado de tareas	1 día	05/10/2022	05/10/2022
2.4.	Planificación	3 días	06/10/2022	10/10/2022
2.5.	Riesgos preliminares	1 día	07/10/2022	07/10/2022
2.6.	Productos obtenidos	2 días	07/10/2022	10/10/2022
HITO	Entrega PEC 1	0 días	11/10/2022	11/10/2022
3.	**Historia de la criptografía**	**9 días**	**12/10/2022**	**24/10/2022**
3.1.	Documentación	4 días	12/10/2022	15/10/2022
3.2.	Selección de conceptos	3 días	17/10/2022	19/10/2022
3.3.	Explicación de conceptos	3 días	20/10/2022	24/10/2022
4.	**Listado de películas**	**11 días**	**25/10/2022**	**08/11/2022**
4.1.	Búsqueda de películas	5 días	25/10/2022	30/10/2022
4.2.	Documentación breve	4 días	31/10/2022	03/11/2022
4.3.	Selección	2 días	04/11/2022	07/11/2022
HITO	Entrega PEC 2	0 días	08/11/2022	08/11/2022
5.	**Evaluación de las películas**	**20 días**	**09/11/2022**	**06/12/2022**
5.1.	Visionado	20 días	09/11/2022	06/12/2022
5.2.	Identificación con conceptos	20 días	09/11/2022	06/12/2022
5.3.	Elaboración de ficha básica	20 días	09/11/2022	06/12/2022
5.4.	Evaluación según criterios	20 días	09/11/2022	06/12/2022
HITO	Entrega PEC 3	0 días	06/12/2022	06/12/2022
6.	**Productos finales y presentación**	**38 días**	**07/12/2022**	**27/01/2023**
6.1.	Finalizar fichas de películas	4 días	07/12/2022	12/12/2022
6.2.	Creación doble línea de tiempo	1 día	11/12/2022	11/12/2022
6.3.	Evaluación global	1 día	12/12/2022	12/12/2022
6.4.	**Proyecto didáctico**	**5 días**	**13/12/2022**	**19/12/2022**
6.4.1.	Definición y público	1 día	13/12/2022	13/12/2022
6.4.2.	Temas y planificación	2 días	14/12/2022	15/12/2022
6.4.3	Materiales y elementos apoyo	2 días	16/12/2022	19/12/2022
6.5.	Conclusiones y trabajo futuro	2 días	20/12/2022	21/12/2022
6.6.	Redacción final de la memoria	16 días	21/12/2022	09/01/2023
HITO	Entrega PEC 4	0 días	10/01/2023	10/01/2023
6.7.	Vídeo de presentación	5 días	11/01/2023	17/01/2023
6.8.	Preparación defensa del trabajo	4 días	18/01/2023	22/01/2023
6.9.	Defensa del trabajo	5 días	23/01/2023	27/01/2023



Cód.	Nombre de tarea
1.	**Planteamiento inicial**
2.	**Plan de trabajo**
2.1.	Contexto y justificación
2.2.	Metodología
2.3.	Listado de tareas
2.4.	Planificación
2.5.	Riesgos preliminares
2.6.	Productos obtenidos
	Entrega PEC 1
3.	**Historia de la criptografía**
3.1.	Documentación
3.2.	Selección de conceptos
3.3.	Explicación de conceptos
4.	**Listado de películas**
4.1.	Búsqueda de películas
4.2.	Documentación breve
4.3.	Selección
	Entrega PEC 2
5.	**Evaluación de las películas**
5.1.	Visionado
5.2.	Identificación con conceptos criptog
5.3.	Elaboración de ficha con datos básic
5.4.	Evaluación según criterios
5.5.	Selección de escenas para video
	Entrega PEC 3
6.	**Productos finales y presentación**
6.1.	Creación doble línea de tiempo
6.2.	Realización de video con escenas
6.3.	Evaluación global
6.4.	**Proyecto didáctio**
6.5.	Conclusiones y trabajo futuro
6.6.	Redacción final de la memoria
	Entrega PEC 4
6.7.	Realización del video de presentacio
6.8.	Preparación defensa del trabajo
6.9.	Defensa del trabajo

Figura 1: Diagrama de Gantt

1.6. Breve sumario de productos obtenidos

Las diferentes entregas parciales en forma de PEC deberían contener los siguientes hitos parciales:

- PEC 1: Introducción, objetivos, lista de tareas y planificación; definición de riesgos preliminares y entregables.
- PEC 2: documentación sobre la historia de la criptografía; extracción de conceptos/momentos históricos y explicación de esos conceptos; listado de películas, información básica y selección.
- PEC 3: lista final de películas a analizar y correlación con los conceptos criptográficos; ficha de la película y evaluación.
- PEC 4: creación de líneas de tiempo y proyecto didáctico, conclusiones y memoria final.

Forman parte de los productos obtenidos dentro de la memoria final:

- La doble línea de tiempo con la evaluación global
- La ficha del proyecto didáctico

1.7. Breve descripción de los otros capítulos de la memoria

A continuación, presento el contenido genérico de los siguientes capítulos de la memoria.

Capítulo 2: Historia de la criptografía. En este capítulo se describe el proceso de documentación sobre la historia de la criptografía y la selección de los momentos que se representan, presentando las razones. Para cada uno de ellos se añade una pequeña explicación y algunas imágenes gráficas.

Capítulo 3: Filmografía utilizada. En este capítulo se explica el proceso de búsqueda de películas y un listado.

Capítulo 4: Evaluación. En este capítulo presenta la evaluación de las películas con respecto a los conceptos criptográficos. Incluye la ficha de evaluación para cada una de las películas incluidas en el análisis.

Capítulo 5: Evaluación global y líneas de tiempo. Con los datos de los capítulos anteriores se realiza una evaluación global y se construyen las dos líneas de tiempo.

Capítulo 6: Proyecto didáctico. En este capítulo se detalla el proyecto didáctico que forma parte de los objetivos del trabajo.

Capítulo 7: Conclusiones y trabajo futuro. En este capítulo se presentan las conclusiones de la investigación en relación con la introducción y los objetivos y se presentarán posibles líneas de trabajo futuro.

Capítulo 8: Glosario de términos. Este capítulo contiene un glosario de términos utilizados a lo largo de la memoria.

Capítulo 9: Bibliografía. Contiene la bibliografía utilizada en la investigación y redacción de la memoria.

1.8. Riesgos

He definido los siguientes riesgos, incluyendo una descripción, la probabilidad de que ocurra (medida en una escala de 1 a 5), el impacto que tendría sobre el desarrollo del trabajo final (medido en una escala de 1 a 5) y medidas que se podrían implementar para mitigar ese impacto.

Riesgo	Descripción	Prob.	Impacto	Mitigación
Sobredimensionado del ámbito del trabajo	Siendo un proceso de investigación lento, ya que implica la búsqueda de películas, su visionado y el análisis detallado para llegar a los objetivos del proyecto, existe el riesgo de haber sobredimensionado el periodo que quiero abarcar (la historia general de la criptografía) o que algunos de los objetivos y productos finales a realizar como las líneas de tiempo o el proyecto didáctico/divulgativo sean demasiado exigentes considerando el tiempo limitado.	3	5	Reevaluar en las entregas parciales si el ámbito y los diferentes objetivos son realizables y adaptarlos, con el acuerdo del tutor.
Falta de estado de arte	Ya en las búsquedas iniciales quedó claro que no existe mucha documentación sobre la relación entre la criptografía y el cine. Se encuentran algunos libros sobre matemáticas y cine con breves referencias a la criptografía, y algunos artículos muy generales en	5	4	No existen medidas claras de mitigación de este riesgo, salvo la discusión con el tutor en algunos casos o búsquedas específicas sobre ciertas películas que podrían tener alguna mención a algún uso en la trama de la

	revistas e Internet. Existe el riesgo que la falta de documentación tenga un impacto en el desarrollo del proyecto, puesto que no hay fuentes con las que contrastar.			criptografía.
Acceso a las películas para visionados completos	La base del trabajo es poder ver películas que contengan conceptos criptográficos, que traten el tema por completo o en las que aparezca algún elemento de criptografía. Aún con la existencia de muchas plataformas de streaming, hay películas que serán difíciles de encontrar completas y es un riesgo que puede impactar en la selección final y en la aplicación de los criterios.	3	4	Buscar información de la película puede permitir obtener datos que nos lleven a poder aplicar parcialmente los criterios. Buscar otras películas alternativas que traten el mismo concepto criptográfico puede ayudar a que este riesgo no afecte a los objetivos del trabajo.
Riesgo personal: carga de trabajo y obligaciones	La carga de trabajo en mi caso no es algo fijo y que pueda prever. Esta inestabilidad puede afectar a la planificación prevista del proyecto y a sus resultados.	3	4	Revisar la planificación para ver si en las etapas del desarrollo de trabajo hay margen de adaptación a pequeños imprevistos. En el caso de grandes imprevistos, revisar los objetivos y modificarlos con el acuerdo del tutor para adaptarse a la nueva disponibilidad.
Riesgo personal: enfermedad importante	Los problemas de salud personales son otro de aquellos riesgos imposibles de prever y que pueden afectar completamente al proyecto.	3	5	En este caso el impacto puede ser muy alto sin posibilidad de mitigación y habría que acordar posponer el proyecto a un semestre posterior.
Riesgo personal: obligaciones familiares	Este problema personal es también imprevisible y puede afectar la capacidad de completar el proyecto. Se puede tratar de algún asunto familiar inesperado o enfermedad.	3	4	En función de la importancia del asunto se debería revisar el ámbito de trabajo y reconsiderar los objetivos. En una

				situación de gravedad se debería posponer el trabajo a un semestre posterior.

1.9. Estado del arte

Tal y como se ha explicado en un punto anterior en las búsquedas iniciales no he encontrado documentación sobre el tema de criptografía o cine. No he podido localizar estudios detallados del tema ni tampoco artículos donde se enfoque desde un punto de vista riguroso más que algunos comentarios de películas. Hay algunos libros de matemáticas y cine en los que hay algunas referencias limitadas a la criptografía, pero nada especializado.

Para la búsqueda de listados de películas emplearé búsquedas en Google, Imdb o Filmafinity. Y utilizaré sitios web como Justwatch.com, que permiten encontrar la plataforma en la que visualizarlas.

Para la investigación tengo acceso a los recursos que ofrece la Biblioteca de la UOC y la Biblioteca de la Filmoteca de Catalunya, entidad donde puedo hacer búsquedas físicas en su catálogo de libros y películas y también en la base de datos ProQuest.

Los recursos que se voy a utilizar en este trabajo se clasifican en tres áreas:

- Recursos sobre criptografía: hay bastante bibliografía que trata la historia de la criptografía.
- Recursos sobre matemáticas y cine: la falta de recursos específicos sobre criptografía y cine la voy a mitigar usando libros que tratan de la representación de las matemáticas en el cine. Incluyen algunos ejemplos de criptografía y también sirven para obtener perspectiva sobre cómo tratar el tema.
- Artículos en revistas o en internet: hay poco material especializado, pero he encontrado algunas fuentes que estoy revisando y que pueden resultar útiles para ir encontrando películas a partir de ellas.

2. CRIPTOGRAFÍA: HISTORIA Y SELECCIÓN DE CONCEPTOS

2.1. Una aproximación inicial

Recordando las primeras páginas de esta memoria, me gustaría recuperar dos de las preguntas que me hacía y que originan este trabajo: *¿Cómo ha representado el cine esa historia de la criptografía? ¿Se encontrarán reflejos fidedignos gracias a los cuales se puedan aprender algunos conceptos?* Desde un punto de vista romántico, y espero que este término no resulte poco adecuado para un trabajo de este tipo, dichas cuestiones constituyen la brújula que guía todo el proceso realizado y definen el ámbito de trabajo, el alcance y el nivel de detalle.

Añado este comentario porque al plantearme este capítulo consideré necesario ser pragmático. La historia de la criptografía se ha explicado extensamente en muchos libros, artículos, cursos y todo tipo de publicaciones. Pretender explicarla al mismo nivel en un trabajo de esta índole multiplicaría el esfuerzo de manera inabarcable en el tiempo disponible y sería un error porque estaría perdiendo el camino que marca la brújula de las preguntas principales.

Es evidente que la base teórica es necesaria. Conocer cómo ha evolucionado la criptografía a lo largo de la historia y el funcionamiento de sus aportaciones principales es imprescindible para realizar el análisis, pero no debo olvidar que lo importante es ver cómo se ha reflejado en el cine y cómo puedo aplicar todo eso a un proyecto didáctico que, tal y como presentaré en su momento, no pretende centrarse en las ecuaciones y mínimos detalles sino crear un conocimiento general y despertar el interés en la materia partiendo de elementos que puedan ser accesibles para todo el mundo.

Cinco libros me han servido como documentación general de este proceso: los cinco están reflejados en la bibliografía y sus autores son Simon Singh, Joaquín García Carmona, David Kahn y Craig P. Bauer. Cuatro de los libros aportan una visión histórica de la criptología y el último de ellos, el segundo de Bauer, se sumerge en casos más particulares, algunos no resueltos, pero que aportan también puntos de vista e ideas interesantes. Estas fuentes principales son el origen de la brevísima historia de la criptografía que se presenta a continuación y del detalle de los momentos históricos y conceptos criptográficos destacados.

Voy a precisar en este punto una primera clasificación dentro de la criptografía que facilitará después una narración más fluida del relato histórico. Dentro de la

criptografía encontramos dos ramas: la transposición y la sustitución. En la transposición, las letras de un mensaje se distribuyen de manera diferente. En la sustitución, hay un cambio de las letras por otro símbolo (cifra) o de las palabras por otro símbolo (código). Dentro de estas ramas, hay técnicas y método criptográficos de mayor o menor complejidad y los hay que combinan también ambas ramas para construir técnicas más seguras.

Un último comentario sobre terminología. En todo este trabajo se habla principalmente de criptografía puesto que los sistemas de cifrado son el punto focal de la mayoría del análisis. En algunos momentos del trabajo se verán reflejados también algunos procesos de criptoanálisis, pero serán menos frecuentes, y por ello mantengo el uso general del término criptografía y no el de criptología, que incluiría ambas disciplinas al mismo tiempo.

2.2. Breve historia de la criptografía

La necesidad de mantener la información segura y secreta existe desde épocas tempranas de la historia de la humanidad. Primero, con técnicas que no forman parte directa de la criptografía como la esteganografía, que se entiende como un conjunto de técnicas que permite la ocultación de mensajes dentro de otros elementos portadores, ya sean estos inteligibles o no. En la esteganografía no hay voluntad de cifrar y si el mensaje se descubre, se trata de texto claro directamente identificable. Los griegos hicieron uso de técnicas muy tempranas de esteganografía: Herodoto narra que se ocultaron mensajes escritos en la cabeza afeitada de un mensajero o en piedras enceradas cuya capa de cera se limpiaba para escribir un mensaje antes de encerarlas de nuevo **(Singh, 2000)**. Además de los métodos de la época griega, podemos considerar algunos otros como las tintas invisibles o la ocultación de un mensaje dentro de otro inteligible y que se descubre seleccionando unas letras determinadas que forman parte del mensaje portador.

Otra técnica sería el micropunto que, por ejemplo, los alemanes usaron durante la Segunda Guerra Mundial, y que mediante técnicas fotográficas lograba reducir una página entera al tamaño de una microficha de un milímetro.

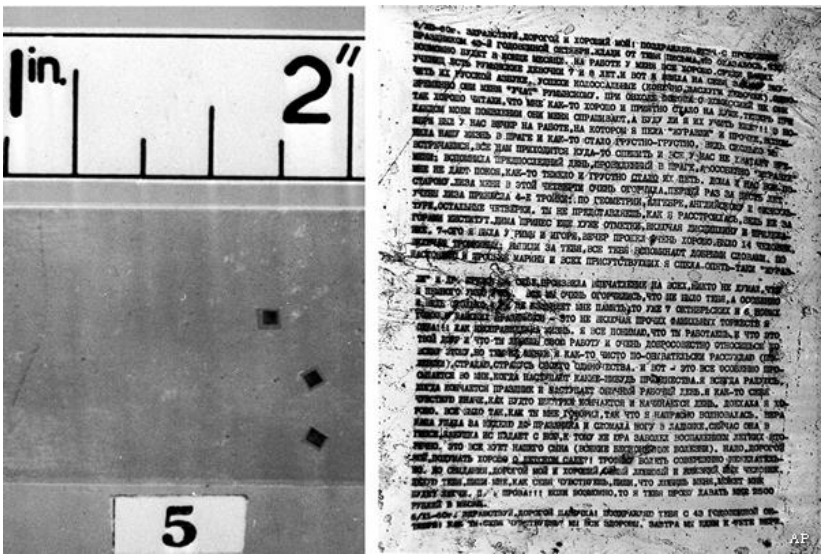


Figura 2: Micropuntos encontrados en 1961 en posesión de Helen Kroger[1]

En la actualidad, la esteganografía se emplea de forma digital para camuflar información en imágenes, audio y vídeo mediante técnicas como las marcas de agua o algoritmos de compresión para insertar información en el bit menos significativo.

Antes de empezar con la criptografía clásica, me gustaría dedicar un breve espacio a los jeroglíficos. No se puede hablar en el caso de los jeroglíficos de criptografía puesto que en origen esta escritura no escondía una intención explicita de cifrar u ocultar un mensaje. Sin embargo, desde un punto de vista posterior en el que no existían registros evidentes de la correspondencia entre los símbolos jeroglíficos y los lenguajes modernos, el proceso de descifrado de los mismos ha implicado técnicas muy similares a las que se enmarcan dentro del criptoanálisis. Singh les dedica un espacio importante en su libro "Los códigos secretos" y comenta lo siguiente: *"los principios del desciframiento arqueológico son esencialmente los mismos que los del criptoanálisis militar convencional. De hecho, muchos descifradores militares se han sentidos atraídos por el desafío de desenmarañar una escritura antigua. Esto se debe probablemente a que los desciframientos arqueológicos suponen un cambio refrescante con respecto al desciframiento militar, ofreciendo un rompecabezas puramente intelectual en vez de un desafío militar. En otras palabras, la motivación es la curiosidad en vez de la animosidad"* **(Singh, 2000)**. Pueden, por tanto, servir como ejemplo para explicar dichas técnicas y el trabajo que se hace en una disciplina tan compleja.

[1] Helen Kroger formaba parte de la red de espías de Portland, un círculo de espionaje soviético que operó en Inglaterra entre finales de los años 50 y el 1961. https://www.mi5.gov.uk/portland-spy-ring Fecha consulta: 10/11/22

2.2.1. Criptografía clásica

De la escítala a las cifras vikingas

Entre los primeros registros de criptografía se encuentra la escítala, usada por los espartanos en el 404 a.C. La escítala es un método de cifrado por transposición, un cifrado en el que las letras o las unidades de texto que se definan cambian su posición según un esquema determinado. Se trata un cilindro de madera, marfil u otro material, con un determinado grosor y longitud sobre el que se enrolla una tira de papel hasta cubrirlo. Se escribe sobre este papel el mensaje longitudinalmente por lo que en cada vuelta del papel va a aparecer una letra que corresponde a la palabra o texto longitudinal que se está escribiendo. El receptor del mensaje necesita tener un cilindro del mismo grosor en el que enrollar el papel y poder leer el mensaje. Es uno de los métodos más antiguos y sencillos.

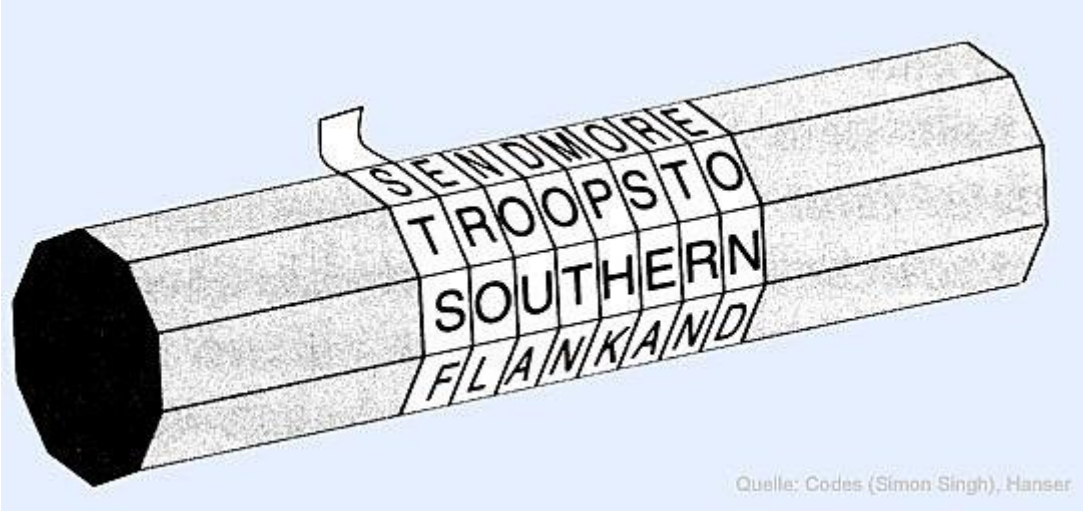


Figura 3: Ejemplo de escítala (Singh, 2000)

Antes de seguir avanzando con otros métodos utilizados en la criptografía griega, si pensamos en una modificación del orden de las letras para ocultar una palabra podemos hablar del **anagrama**. Un anagrama no se puede considerar un cifrado puesto que no hay una clave que se transmite y define el proceso de cifrado, pero es un buen ejemplo de ocultación de mensajes de uso común.

Un segundo ejemplo de la criptografía griega es la **cifra de Polibio**, que reemplazaba cada letra por un par de números. Tenemos aquí un **cifrado de sustitución monoalfabético**, que es aquel en el que cada letra del texto en claro se sustituye por otra letra o signo en el texto cifrado. La característica principal de este cifrado es que cada letra se ve sustituida siempre por el mismo signo en el alfabeto de cifrado. En la cifra de Polibio, cada letra se va a identificar por dos números al estar dispuestas en

una tabla. Las letras pueden estar ordenadas alfabéticamente o usando una palabra clave y situando a continuación el resto del abecedario.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figura 4: Cuadrado de Polibio que se usa para este cifrado

Hay dos elementos interesantes de esta cifra: por un lado, el mensaje se dobla puesto que cada letra se cifra con un par de números; por el otro, este sistema se usaba para comunicarse a largas distancias, ya que con un número determinado de antorchas en cada mano se enviaba el par numérico que identificaba la letra **(Bauer, 2016)**.

Acabaré esta aproximación a los registros tempranos hablando de la criptografía que empleaban los vikingos: un ejemplo lo tenemos en la piedra Rotbrunna en Suecia, en la se vemos unas marcas que determinan un par de números que hacían referencia a la posición de una runa en una tabla, como se hace en el cifrado de Polibio.

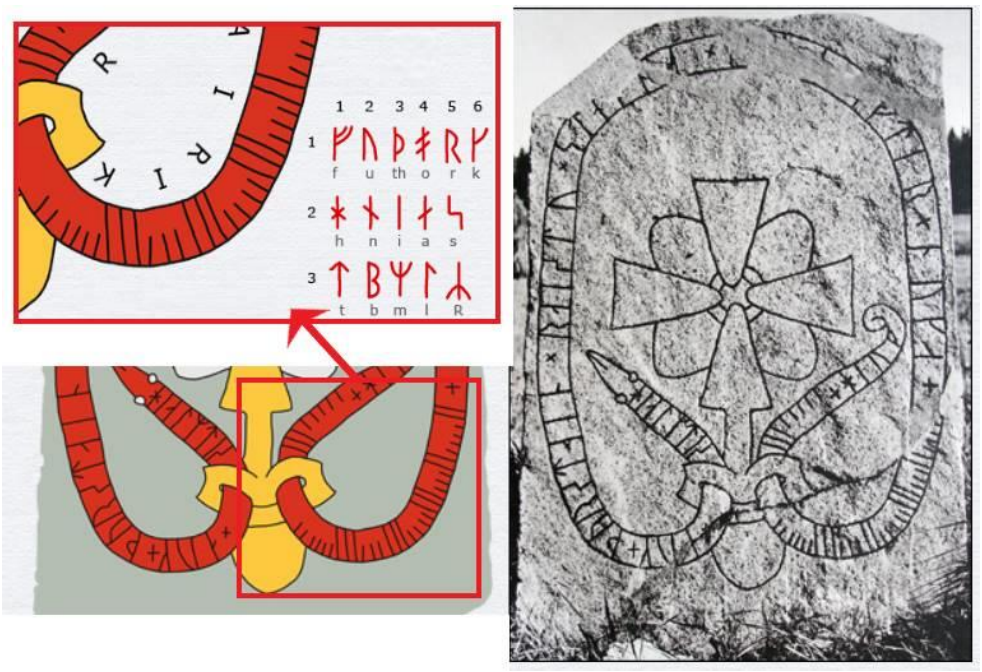


Figura 5: Piedra Rotbrunna y codificación de runas

2.2.2. El cifrado de sustitución monoalfabético y su criptoanálisis

Los siguientes siglos estarán marcados por las diferentes evoluciones del cifrado de sustitución monoalfabético. Algunos de los métodos que podemos destacar son:

Cifrado por desplazamiento / Cifrado del César

El cifrado del César o cifrado por desplazamiento consiste en sustituir cada letra por otra del mismo abecedario, pero desplazada varias posiciones. Podemos representar este cifrado con la fórmula siguiente:

***C = M + K (mod L)**, siendo M la letra en claro, K el desplazamiento, L la longitud del alfabeto y C la letra cifrada*

Este cifrado se llama así porque existen registros que Julio César lo utilizaba desplazando tres letras en el alfabeto, y fue utilizado de forma general hasta que la técnica del análisis de frecuencias fue capaz de romper este cifrado, al igual que hizo con muchos otros cifrados de sustitución monoalfabéticos.

Cifrado con palabra clave / libro código

El cifrado con palabra clave consiste en crear un alfabeto de cifrado que se inicia con una palabra clave y a continuación se colocan el resto de letras en orden. La siguiente figura muestra un ejemplo de este tipo de cifrado:

Palabra clave: S E C R E T O M A N I F I E S T O
Alfabeto en claro: A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z
Alfabeto de cifrado: S E C R T O M A N I F B D G H J K L P Q S U V W X Y Z

Cualquier mensaje se codificaría usando ese alfabeto de cifrado. Es importante una selección correcta de la palabra clave para que haya un gran número de letras que sufran una variación. En el caso anterior vemos que las últimas letras del abecedario mantienen sus equivalentes.

Cifrado Atbash

Es un cifrado que aparece ya mencionado en la Biblia. Este cifrado se usó originariamente para encriptar el alfabeto hebreo, aunque se puede usar con cualquier alfabeto. Consiste en mapear un alfabeto con su reverso, es decir la primera letra se cifra con la última. No hay ninguna clave y la seguridad es bastante reducida.

Original	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Clave	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
Clave	Z	Y	X	W	V	U	T	S	R	Q	P	O	Ñ	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Figura 6: cifrado Atbash en hebreo y correspondencia al español

La historia de la criptografía corre en paralelo a la del criptoanálisis. La creación de nuevos cifrados van en paralelo a los esfuerzos por romperlos en lo que podemos considerar una de las batallas más largas en la historia del hombre. El cifrado de sustitución monoalfabético fue superado gracias al análisis de frecuencias. La descripción más antigua que se conoce de la técnica es del científico del siglo IX Al Kindi y que en su texto *Sobre el desciframiento de mensajes criptográficos* escribe lo siguiente **(Singh, 2000)**:

> *Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano diferente escrito en la misma lengua y que sea lo suficientemente largo para llenar alrededor de una hoja, y luego contar cuántas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos «primera», a la siguiente en frecuencia la llamamos «segunda», a la siguiente «tercera», y así sucesivamente, hasta que hayamos cubierto todas las letras que aparecen en la muestra de texto llano. Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con más frecuencia y lo sustituimos con la forma de la letra «primera» de la muestra de texto llano, el siguiente símbolo más corriente lo sustituimos por la forma de la letra «segunda», y el siguiente en frecuencia lo cambiamos por la forma de la letra «tercera», y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver.*

En realidad, el análisis de frecuencias es un poco más complejo puesto que la frecuencia de aparición de cada letra en una lengua determinada es un promedio y no se puede hacer una correspondencia tan directa. Pero combinando estas frecuencias con la aparición de combinaciones de letras o buscando las palabras más frecuentes de una lengua, el análisis de frecuencias se convierte en una gran herramienta de descifrado.

2.2.3. El camino hacia el cifrado de sustitución polialfabético

El Renacimiento en Europa es una época en la que el uso de la criptografía se extiende y, de la misma manera, el criptoanálisis se convierte en una herramienta esencial. Las relaciones entre estados y la necesidad de mantener ventajas en la transmisión de la información son un agente motivador de suma importancia para el desarrollo de nuevas técnicas. De la misma manera, la vulnerabilidad del cifrado de sustitución monoalfabético empujó a la introducción de variaciones como el uso de nulos, el deletreo incorrecto de palabras o el paso al código de sustitución reemplazando palabras por otras palabras o símbolos. Este código por sustitución tiene dos problemas principales: los libros de códigos son mucho más complejos, tanto para el redactado como el trasporte o envío, y si eran interceptados, implicaba iniciar el complejo proceso de nuevo. Algunos de los métodos de cifrado o codificación que se pueden destacar se presentan a continuación.

Nomenclátor

Se introduce en el siglo XVI el uso del nomenclátor, que es una variante de la cifra de sustitución en el que se empleaban códigos o caracteres para reemplazar palabras específicas y el resto del texto normalmente se cifra con una cifra de sustitución monoalfabética. Existen variados usos históricos de esta cifra: María Estuardo la empleó para comunicarse con los conspiradores durante la conspiración Babington en la que la decodificación de unos mensajes encriptados con un nomenclátor llevó a su ejecución **(Singh, 2000)**, la Gran Cifra desarrollada por Antoine y Bonaventure Rossignol para Louis XIV o el código de ruta de la Unión usado por los federales durante la guerra de Secesión.

Figura 7: Nomenclátor utilizado por María Estuardo (Singh, 2000)

Cifrado Playfair

Se trata de un tipo de cifrado de sustitución pero que sustituye bigramas siguiendo unas reglas muy específicas. Aunque el creador fue Charles Wheatstone en 1854, su uso fue promovido por Lord Playfair, de ahí su nombre.

El cifrado consiste en primer lugar en la creación de una matriz 5 por 5 con una clave y a continuación una serie de reglas para cifrar para cada par de letras:

- Si las dos letras son iguales, se añade una x y se codifica el nuevo par de letras
- Si las dos letras están en la misma fila, se escogen las dos que están en el cuadro inmediatamente a la derecha
- Si las dos letras están en la misma columna, se escogen las dos que están en el cuadro inmediatamente debajo
- Si las dos letras no están en la misma fila o en la misma columna, se escogen las dos que están en las esquinas opuestas del rectángulo que forman las dos letras originales.

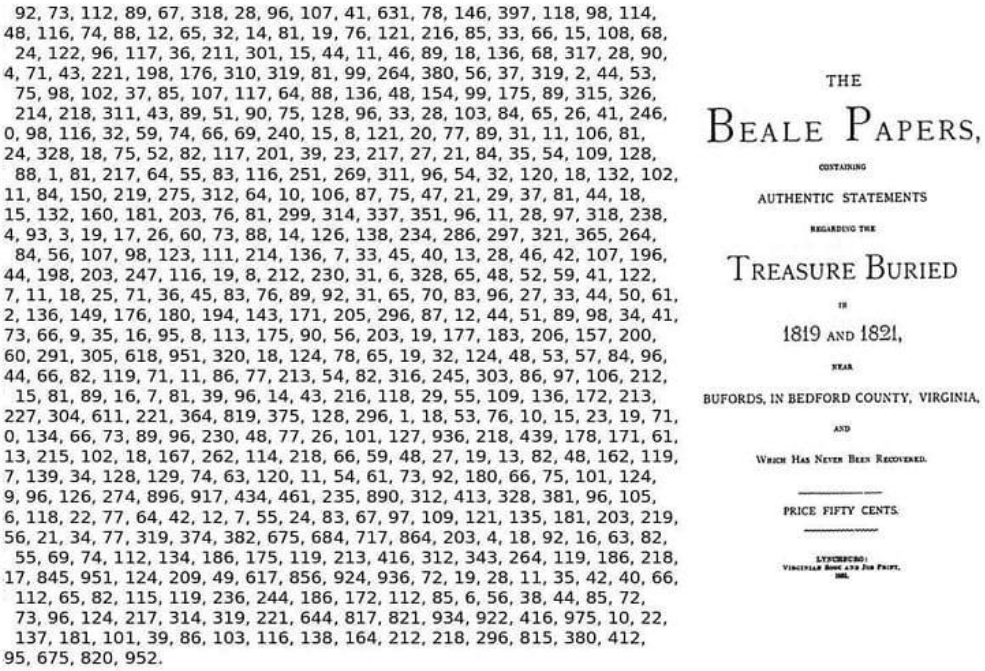
C	H	A	R	L	Texto en claro: **casita**
E	S	B	D	F	**ca** (misma fila) -> **HR**
G	I/J	K	M	N	**si** (misma columna) -> **IP** o **JP**
O	P	Q	T	U	**ta** (rectángulo) -> **QR**
V	W	X	Y	Z	

Cifrado homofónico

El cifrado homofónico se introduce con el fin de reducir el riesgo de romper la cifra con análisis de frecuencias. En este caso, las letras más comunes en un alfabeto tienen varias posibilidades para ser representadas. Si la letra a o la letra e son las más comunes se le asignarían un número de símbolos proporcionalmente más grande que a la letra z, por ejemplo. Estos símbolos pueden ser pares de números u otro tipo de símbolos que se definan en la cifra. Un ejemplo sería el método de cinta móvil o método oficial de guerra **(García Carmona, 2011)**.

Podemos considerar el cifrado de sustitución por libro como un caso del cifrado homofónico. Se utilizaba el fragmento de un libro o documento de texto como base del cifrado de mensajes entre las personas que realizan la comunicación. En este cifrado se eligen páginas y posiciones de letras (o de palabras) para ir codificado el mensaje en claro. Es necesario que las personas que se comunican tengan la misma edición del libro.

Un ejemplo interesante de este cifrado son los papeles Beale, un conjunto de textos que ocultaban la localización de un tesoro. Estos papeles se atribuyen Thomas J. Beale que dejó una caja con tres textos encriptados. En 1885 aparece un panfleto con la explicación de la existencia de un tesoro y los textos. Desde su aparición, ha habido numerosos intentos de descifrarlo sin éxito. Uno de los documentos se descifró utilizando la Declaración de Independencia de Estados Unidos **(Singh, 2000)**.



71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53,
75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326,
214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246,
0, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81,
24, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128,
88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102,
11, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18,
15, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238,
4, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264,
84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196,
44, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122,
7, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61,
2, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41,
73, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200,
60, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96,
44, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212,
15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213,
227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71,
0, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61,
13, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119,
7, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124,
9, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105,
6, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219,
56, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82,
55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218,
17, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66,
112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72,
73, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22,
137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412,
95, 675, 820, 952.

THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

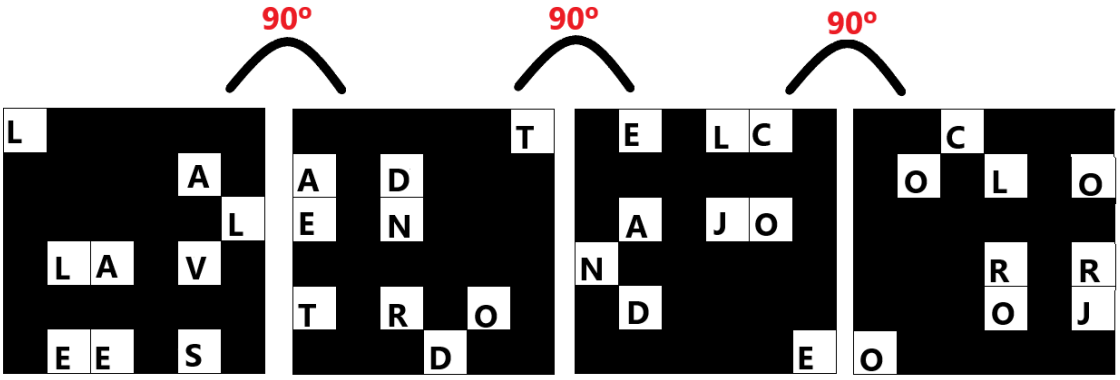
Figura 8: Los papeles Beale

Rejilla de Cardano

Jerónimo de Cardano inventó este método en el siglo XVI **(García Carmona, 2011)**. Consiste en tomar un cartón o papel en el que se recortan huecos para dejar una serie de espacios en blanco en los que se puede escribir un determinado mensaje que luego se completa alrededor con un texto portador inteligible. Variaciones permitían obtener mensajes de determinados libros o documentos a partir de una determinada rejilla. Este uso formaría parte de la esteganografía.

Figura 9: Rejilla empleada en la serie TURN

También se puede usar como un cifrado por transposición. Se recortan una serie de agujeros sobre un cartón y este se coloca en un folio en blanco. Se empiezan a escribir las letras y cuando ya no quedan espacios el cartón se gira dejando nuevos espacios para escribir y así sucesivamente hasta que se termina de escribir todo el mensaje. Una vez se retira el cartón el mensaje original se ha convertido en un texto cifrado por transposición.



L	E	C	L	C	T
A	O	D	L	A	O
E	A	N	J	O	L
N	L	A	R	V	R
T	D	R	O	O	J
O	E	E	D	S	E

Texto en claro: La llave está dentro del cajón de color rojo
Texto cifrado: LECLCTAODLAOEANJOLNLARVRTDROOJOEEDSE

Figura 10: Cifrado con una rejilla con desplazamiento

2.2.4. Cifrados de sustitución polialfabéticos

El siguiente paso en el cifrado de mensajes por sustitución fue el uso de varios alfabetos llegando al cifrado de sustitución polialfabético. En esta técnica se utilizan varios alfabetos de cifrados alternando entre ellos, es decir, cada letra o cada conjunto definido de letras se va a cifrar con un alfabeto diferente. Se le está añadiendo al cifrado de sustitución una capa de robustez pues se acaba con el patrón que permite al análisis de frecuencias romper el cifrado, pero también se le añade complejidad tanto para el emisor como para el receptor del mensaje. En general, en estos cifrados se suele preparar una tabla con los diferentes alfabetos y se utiliza una palabra clave para determinar el orden de los mismos.

Discos de Alberti

Podemos situar sus orígenes en el siglo XV de la mano de León Battista Alberti, que elaboró un disco de cifrado con dos anillos, el externo con un alfabeto más cuatro números (texto plano) y el interno sólo con el alfabeto (texto cifrado). Los números permitían codificar palabras particulares con un libro de códigos, añadir nulos al cifrado o utilizar varios alfabetos.

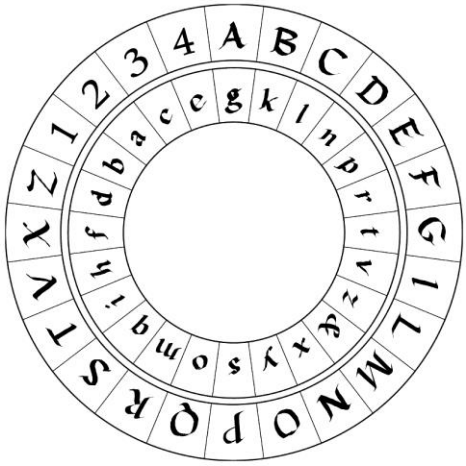


Figura 11: Discos de Alberti

Existen varios métodos de uso de este disco, pero uno que ejemplifica el cifrado polialfabético es el siguiente:

- Se encara una letra del disco móvil con la letra A del disco fijo, por ejemplo, la g, como en la figura 10.
- Imaginemos que la frase que queremos cifrar es “EL TERROR LLEGARÁ”
- Se hace un preprocesado de esta frase eliminando espacios, eliminando letras dobles o cambiándolas por nulos y añadiendo unos números en medio para indicar el cambio de alfabeto (usando los 1, 2, 3 y 4 del disco exterior).
- La frase quedaría “EL3TEROR2L&EGARA”, por ejemplo
- Cuando se empieza a cifrar e se convierte en p, l en z y el 3 en c. Pero este número también indica un nuevo alfabeto e implica que desplazamos la letra del disco movible debajo de la A, así que ahora la c estaría debajo de la A. De esta manera tenemos un nuevo alfabeto de cifrado.
- Seguimos avanzando con la encriptación aplicando las mismas reglas y desplazando la rueda cada vez que aparece un número.

Cifrado Vigenère

A continuación, en el siglo XVI, destaca el cifrado de Vigenère, un cifrado de sustitución polialfabético en el que se crea una tabla que tiene 26 versiones del alfabeto en diferentes líneas. Estas 26 líneas son las que se van a usar para cifrar y descifrar. Una muestra de dicha tabla la podemos encontrar en la siguiente figura.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 12: Tabla de Vigenère

Para cifrar un texto se emplea una clave que indica el alfabeto que se va a usar para cada letra. Si la clave fuese CLARO, la primera letra del mensaje se cifraría con la fila C, la segunda con la L y así sucesivamente. La clave se va repitiendo para cubrir toda la longitud del mensaje.

El criptoanálisis de este cifrado es complejo y se puede atribuir en primer lugar a Charles Babbage a mediados del siglo XIX, aunque no publicó sus resultados probablemente porque el gobierno británico decidió que suponía una ventaja mantener el método de descifrado oculto. A consecuencia de esto, el mérito del descifrado se atribuye a Friedrich Wilhelm Kasiski que descubrió la misma técnica de forma independiente a finales del siglo XIX, lo que se ha dado en llamar la prueba Kasiski **(Singh, 2000)**. Kasiski sugiere que se deben buscar por fragmentos repetidos en el texto cifrado y compilar las distancias que separan estas repeticiones. La longitud de la

clave es probablemente un divisor de estas distancias[2]. Otro método de criptoanálisis de este cifrado fue definido por William Friedman **(Bauer, 2016)** en 1920. Para romper el cifrado, Friedman parte del concepto del índice de coincidencia, que se define como la probabilidad de que dos letras seleccionadas aleatoriamente sean iguales. Este índice permitía averiguar la longitud de la clave dividiendo el texto en subcadenas (considerando diferentes longitudes de clave) y calculando para estas subcadenas los índices de coincidencia. Si el promedio de estos índices se acerca al índice de coincidencia de la lengua del texto, la longitud de esas subcadenas es la longitud probable de la clave[3].

Por tanto, el problema principal del cifrado de Vigenère es que la clave se va repitiendo a lo largo del texto permitiendo el criptoanálisis. Para aumentar la robustez se encontraron alternativas como el cifrado de flujo (en el que la clave es una frase larga o parte de un libro). Sin embargo, esto tenía el problema de usar palabras inteligibles para la clave de cifrado, de ahí que se saltase a usar un cifrado de flujo con letras aleatorias, como la libreta de un solo uso desarrollada por Gilbert Vernam en 1917 **(Bauer, 2016)**.

Cifrado Vernam / Libreta de un solo uso

El cifrado Vernam consistía en encriptar el mensaje en claro con una clave formada por una serie de caracteres aleatorios del mismo tamaño que el mensaje usando una función XOR. Para descifrar el mensaje se usaba la misma clave y la misma operación. Sólo debían existir dos copias de la clave, aleatoria, que debían destruirse después de cada cifrado y por tanto no reutilizarse. Se creó en 1917 y su evolución es la libreta de un solo uso. En la libreta de un solo uso se crean claves aleatorias de la misma longitud del mensaje que se combinan mediante suma modular con el texto en claro para obtener el texto cifrado.

La idea de libreta de un solo uso viene de la forma en la que se distribuían las claves, en una pequeña libreta. Este cifrado, aunque demostrado como indescifrable desde un punto de vista teórico, no es práctico por varias razones: la distribución y mantenimiento en secreto de las claves y la generación verdaderamente aleatoria de claves.

[2] La Universidad Tecnológica de Michigan tiene un tutorial detallado sobre este método que se puede encontrar aquí: https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Kasiski.html Fecha de consulta: 15/11/22

[3] La Universidad Tecnológica de Michigan cuenta con un tutorial donde explican el uso del IC para la estimación de la longitud de la clave: https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-IOC-Len.html Fecha de consulta: 15/11/2022

2.2.5. Primera Guerra Mundial

La Primera Guerra Mundial trajo nuevos desarrollos a la criptografía. En Alemania se creó el cifrado ADFGX (el 21 de marzo de 1918) y una modificación, el ADFGVX (el 1 de junio del mismo año). Una tabla de Polibio transforma cada letra del texto en claro en una combinación de ADFGVX y estos pares después se separan en columnas que se reordenan con una segunda clave **(Bauer, 2016)**. Estas 6 letras se eligieron porque al ser retransmitidas por alfabeto Morse son muy distintas y se reducían los errores de transmisión. Se considera el último gran cifrado "manual" antes de la aparición de las máquinas.

	A	D	F	G	X
A	T	I/J	L	K	U
D	B	A	D	M	R
F	Q	V	E	F	Y
G	N	S	P	C	Z
X	W	G	O	H	X

A continuación, muestro un ejemplo rápido de este cifrado. Partimos de la tabla de Polibio generada con ADFGVX.

El mensaje SECRETO se cifraría usando la tabla como GD FF GG DX FF AA XF.

A continuación, se elige una palabra clave, en nuestro caso por simplificar KEY, y se ordena estas letras en columnas bajo la palabra clave. Estas columnas se reordenan alfabéticamente.

K	E	Y
G	D	F
F	G	G
D	X	F
F	A	A
X	F	

E	K	Y
D	G	F
G	F	G
X	D	F
A	F	A
F	X	

El mensaje cifrado se obtiene concatenando cada columna ordenada alfabéticamente:

Texto en claro: S E C R E T O
Texto cifrado: DG XA FG FD FX FG FA

La Oficina de Cifrado (USA) / Las Cámaras Negras

El origen de la Oficina de Cifrado (Cipher Bureau) en los Estados Unidos se encuentra en la figura de Herbert O. Yardley. Trabajaba como operador de telégrafos y tenía acceso a mensajes codificados. Su carácter emprendedor le llevó a poder convencer a

la jerarquía de la necesidad de una oficina criptográfica, y este es el origen del Cipher Bureau fundado en 1919 bajo el llamado Departamento de Guerra[4].

El Bureau comenzó a operar en Nueva York donde confluían varias compañías de cable con conexiones internacionales. Sus funcionas incluían tanto proteger las comunicaciones de los Estados Unidos como interceptar comunicaciones extranjeras. El Bureau fue desmantelado en 1929.

La Oficina de Cifrado es una forma de las Cámaras Negras que se emplearon de forma habitual a partir del siglo XVI. Cada poder europeo constituyó una de estas Cámaras como centro para descifrar mensajes y acumular inteligencia **(Singh, 2000)**.

Estaciones de números (Numbers stations)

No se conoce el origen o la intención de estas estaciones que transmiten por onda corta, pero iniciaron sus transmisiones posiblemente en la Primera Guerra Mundial y se relacionan con servicios de inteligencia[5]. Retransmiten números, letras, código Morse o datos en general utilizando voces masculinas o femeninas generadas de forma artificial.

Los mensajes tienen normalmente un formato compuesto por una música de sintonización, un identificador del emisor, la cabecera con el identificador del agente, el tamaño del mensaje o el número de grupos que se van a enviar y a partir de ahí una serie de grupos de 4 o 5 números que se repiten un determinado número de veces.

Esta falta de un origen o propósito claro los han convertido en objeto de mucha especulación y del uso en la ficción.

2.2.6. Segunda Guerra Mundial

El final de la Primera Guerra Mundial y la transición hacia la segunda estará marcado por las máquinas de cifrado, que serán el objetivo principal del criptoanálisis de la época. Es el periodo en el que se desarrolla uno de los grandes artefactos dedicados a la encriptación: la máquina Enigma. De la base de esta máquina, los discos de cifrado, hemos hablado anteriormente, pero entre el año 1918 y 1923 se desarrollan en paralelo varias versiones de la máquina y es finalmente el alemán Arthur Scherbius el

[4] National Security Agency – The Black Chamber https://www.nsa.gov/History/Cryptologic-History/Historical-Events/Article-View/Article/2740622/the-black-chamber/ Fecha de consulta: 20/11/2022

[5] En el siguiente vídeo "Estaciones de números: radio y servicios de inteligencia" se dan más datos de las mismas. https://www.youtube.com/watch?v=0a-T5bmepsA Fecha de consulta: 27/12/2022

que lanza al mercado la primera versión. El advenimiento de Hitler y la llegada de la Segunda Guerra Mundial incrementaron la producción y el desarrollo de la Enigma y en paralelo todo el proceso de criptoanálisis que incluye el trabajo de Alan Turing en Bletchley Park (Reino Unido).

La máquina Enigma de Scherbius está formada por tres elementos: un teclado mediante el cual se escribe el texto en claro, un sistema de engranajes modificador para cifrar las letras y un panel que tiene las letras del alfabeto.

El modificador está constituido por unos rotores conectados entre sí. Cada uno de estos rotores es un disco con 26 contactos en cada cara, cada contacto de una cara cableado y conectado a otro de la opuesta. Por ejemplo, en un rotor el contacto que correspondería a la c puede estar conectado al contacto de la d, y en otro rotor el contacto de la c puede estar conectado a la s.

En la mayoría de máquinas Enigma había tres ranuras para rotores, lo que permitía establecer permutaciones de los rotores para aumentar el número de alfabetos. Los rotores van girando a medida que se van tecleando letras y al completar una vuelta de uno se inicia la vuelta del siguiente y así sucesivamente. También se añadió en modelos posteriores un clavijero que permitía intercambiar 6 pares de letras antes de iniciar el proceso de cifrado con los rotores. Este clavijero permitía conectar la a la d, por ejemplo, por lo que al teclear una a en realidad esta estaba siguiendo el camino de la d.

Figura 13: Máquina Enigma[6]

[6] Imagen obtenida de la web del Imperial War Museum en Londres. https://www.iwm.org.uk/collections/item/object/30005172 Fecha de consulta: 18/11/2022

Cuando un operador necesita enviar un mensaje debe primero colocar los rotores en un orden determinado, en una posición inicial también determinada y el clavijero con las conexiones de letras que se han decidido. Cada golpe de tecla envía los impulsos eléctricos por el modificador que ilumina al final el tablero y tras cada tecla se produce el giro de los rotores. El proceso de desencriptado era similar pues las máquinas funcionan de forma simétrica. La información sobre los rotores, su disposición en las ranuras, su posición inicial y los clavijeros se distribuían en libros de códigos.

La máquina Enigma constituye un elemento fundamental durante la Segunda Guerra Mundial y el ejército alemán compró a Scherbius más de 30000 para asegurar sus comunicaciones. La carrera por descifrarla tiene diversos protagonistas como el alemán Hans-Thilo Schmidt o el polaco Marian Rejewski, pero la figura más conocida en este proceso y que trabajó desde Bletchley Park es Alan Turing. Bletchley Park en Buckinghamshire fue la sede de la Government Code and Cypher School, una organización de desencriptación que albergaba operadores, matemáticos y criptoanalistas con el fin de hacer frente a la Enigma y descifrar los mensajes alemanes, de cualquier fuente.

Alan Turing publica en 1937 “Sobre los números computables”, un artículo en el que describe una máquina imaginaria que podía llevar a cabo una operación matemática a partir de una serie de pasos predefinidos. Llevando el concepto más allá, imaginó una máquina programable, es decir, una máquina a la que se le pudieran introducir las instrucciones para realizar cualquier posible operación. De esta definición podemos inferir que la máquina universal de Turing es una concepción inicial del ordenador y la computación.

Aun siendo la figura más visible en el proceso de romper la Enigma, el trabajo de Turing no se habría podido desarrollar sin sus compañeros en Bletchley Park o sin éxitos militares como los que en mayo de 1941 permitieron capturar por un lado un barco que tenía en su interior equipos y códigos de cifrado o el submarino U-110 que transportaba una máquina Enigma.

Enigma no fue la única máquina utilizada por los alemanes: dispositivos como diversos modelos de Lorenz también se utilizaron y concentraron los esfuerzos de los criptoanalistas aliados. En paralelo a los esfuerzos que los británicos hicieron para romper la máquina Enigma, los norteamericanos desde su Signals Intelligence Service SIS (una transformación del antiguo Cipher Bureau fundado por Herbert O Yardley después de la Primera Guerra Mundial) hicieron lo propio con las máquinas japonesas. Liderados por William Friedman, realizaron el criptoanálisis de las máquinas Roja, Naranja y Púrpura **(Bauer, 2016)**.

Secráfono

El secráfono (secraphone o scramble phone en inglés) se desarrolló en el Reino Unido alrededor de 1937 como un sistema telefónico seguro. Churchill lo utilizó para sus comunicaciones con el gobierno y el ejército. El teléfono venía acompañado por una caja que se encargaba de la encriptación de las comunicaciones mediante una inversión de frecuencias[7]. El teléfono tenía un botón "Secret" que las dos partes accionaban para poner en marcha el proceso de ocultación.

Los Nativos Americanos – Code Talkers

El concepto de Code Talker se refiere a aquellas personas que fueron empleadas por el ejército para emplear códigos basados en lenguajes poco conocidos y utilizados.

Durante la Segunda Guerra Mundial se emplearon Code Talkers Navajos con el fin de asegurar las comunicaciones y reducir la cantidad de mensajes captados por los japoneses. Para adaptar términos militares se emplearon palabras en navajo de elementos que pudieran parecerse y esta codificación utilizaba dichas palabras con una versión transformada del alfabeto. Las letras del alfabeto se hacían corresponder con los nombres de animales u otros elementos que luego se traducían al navajo y se empleaban varias palabras para cada letra, usando por tanto un cifrado homofónico al que se le unían palabras codificadas.

2.2.7. Criptografía moderna

Claude Shannon

Para empezar a hablar de criptografía moderna es importante mencionar la figura de Claude Shannon, creador de diferentes conceptos utilizados en años posteriores. Shannon demostró que la codificación con la libreta de un solo uso es indescifrable y su idea de entropía es importante para desarrollos posteriores. Shannon extrae el concepto de entropía de la información del concepto existente en termodinámica. Simplificando, lo podemos definir de la siguiente manera: cuanto menos se sepa sobre lo que el mensaje debe decir, más cantidad de información hay que enviar. Así explicado puede parecer lógico, pero Shannon estableció un cálculo detallado y desgranó diferentes ideas, una de las cuales es que existe un límite de cuanto se

[7] Scramble Phones https://blog.sciencemuseum.org.uk/scrambled-phones/ Fecha de consulta: 31/12/2022

puede comprimir un mensaje sin tener pérdidas en un canal (sin ruido o con)[8]. De aquí se deriva el concepto de redundancia: un mensaje con elevada entropía, tiene baja redundancia mientras que un mensaje con baja entropía tiene elevada redundancia. Uno de los elementos principales de toda la teoría de Shannon y que tendría gran impacto en los desarrollos criptográficos posteriores es su conclusión de que la forma más eficiente de enviar cualquier tipo de información es convirtiéndola en bits antes de transmitirla.

DES – Data Encryption Standard

En 1975 se publica el algoritmo DES (Data Encryption Standard), resultado de la colaboración entre IBM y la National Security Agency (NSA) y usado como estándar en Estados Unidos hasta que fue desencriptado en 1999. El creador de este algoritmo es Horst Feistel. DES es un algoritmo de cifrado por bloques de clave simétrica, es decir, utiliza la misma clave para cifrar y descifrar la información. Explicar el funcionamiento de DES en estas páginas no es posible por la complejidad de los detalles. En resumen, el algoritmo divide la información en bloques de 64 bits que reciben un tratamiento por separado: en primer lugar, se permutan los bits del bloque; en segundo lugar, sobre cada bloque se van a ejecutar 16 rondas del algoritmo; para acabar, se aplica una permutación inversa a la inicial **(Bauer, 2016)**. Para cada una de las rondas mencionadas en el segundo paso:

- se divide el bloque en dos partes, Izquierda I y Derecha D
- la D de una ronda pasa a ser la I de la siguiente
- la I de esta ronda se combina mediante una operación XOR con la D de la ronda transformada por una función de Feistel, que involucra una subclave de la clave simétrica. Se trata de una subclave porque al tener que hacer 16 rondas hay que tener 16 claves diferentes.

Los problemas de este algoritmo llegaron puesto que la clave de 56 bits resultó ser demasiado corta y en enero de 1999 se logró descifrar mediante un ataque de fuerza bruta.

Criptografía de clave pública

También conocida como criptografía asimétrica. En este caso se van a utilizar dos claves, una pública y una privada, y una función simple de calcular en una dirección, pero difícil de revertir (one-way function). Estas dos claves van a estar relacionadas, la

[8] Shannon C. “A mathematical theory of communications” https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf Fecha de consulta: 01/12/2022

pública se utilizará para el cifrado y la privada para el descifrado. En un esquema sencillo de criptografía de clave pública el destinatario genera ambas claves y envía al emisor la clave pública. Éste cifrará el mensaje con la pública y se lo enviará al destinatario que utilizará la privada para descifrar. En este caso la distribución de claves es más sencilla y es un sistema que aumenta la confidencialidad e integridad del mensaje; como desventajas, el tiempo de proceso es más grande y las claves deben tener más tamaño que en las simétricas. Existen una gran cantidad de tecnologías o protocolos de clave asimétrica. A continuación, algunos ejemplos:

Tecnologías	
RSA (Rivest, Shamir y Adleman)	Desarrollado en 1979, es un sistema de cifrado de clave pública en el que la seguridad la proporciona el problema de la factorización de números enteros grandes. Los números que se utilizan son primos del orden de 10^{300} y el tamaño puede aumentarse cuando la capacidad de computación crezca **(Bauer, 2016)**. También se emplea para la firma de mensajes.
DSA – Digital Signature Algorithm	Propuesto en 1991 y estandarizado en 1994 por el NIST, es un algoritmo de firma (autenticación) de mensajes, no de cifrado.
Criptografía de curva elíptica	Desarrollado en 1985 por Neal Koblitz y Victor S. Miller, es una evolución de RSA que usa un problema matemático diferente, el problema del logaritmo discreto en curvas elípticas **(Bauer, 2016);** permite un nivel de seguridad similar con claves más cortas.
Protocolos	
PGP – Pretty Good Privacy	Es un protocolo de cifrado híbrido, que emplea criptografía simétrica y asimétrica, desarrollado por Phil Zimmermann en 1991. En primer lugar, el texto se comprime; a continuación, el sistema genera una clave de sesión a partir de movimientos del ratón y letras que se piden en el momento del cifrado; con esta clave se usa un algoritmo simétrico para cifrar. La clave se cifrará con la clave pública del receptor y se envían el mensaje cifrado y la clave. El receptor hará el proceso contrario.
SSH – Secure Shell	Es un protocolo de acceso remoto a un servidor que utiliza la gestión de claves RSA para encriptar la sesión de conexión.

El futuro de la criptografía dependerá de los medios que existan para romper los cifrados existentes, tal y como ha ocurrido a lo largo de la historia. La computación cuántica podría poner en dificultades a algoritmos como RSA o la criptografía de curva elíptica. Si esto ocurre, creo que, tras este breve repaso de la historia de la criptografía, podemos estar bastante seguros que nuevos sistemas llegarán para cifrar nuestras comunicaciones.

3. FILMOGRAFÍA: SELECCION

La selección de un listado de películas que pudieran servir de base para el visionado posterior no ha sido un proceso obvio ni realizado de una sola vez. Para acometerlo he utilizado desde búsquedas en Internet, referencias en libros y artículos, recomendaciones del tutor de este TFM, de compañeros que realizan el mismo tipo de trabajo e incluso de amigos que te dan una pista de películas ocultas o de otras nacionalidades que podrían servir. A continuación, listaré las diferentes fuentes de las que he extraído películas:

1. **Búsquedas en Internet**
    a. Listados obtenidos en IMDB:
        i. https://www.imdb.com/search/keyword/?keywords=cryptography
        ii. https://www.imdb.com/search/keyword/?keywords=cipher
        iii. https://www.imdb.com/search/keyword/?keywords=cryptocurrency
        iv. https://www.imdb.com/search/keyword/?keywords=encryption
    b. Otros listados en Internet
        i. What is my movie? - Item
        ii. What are the best movies which involves ciphers and cryptography? - Quora
        iii. The Complete List of Hacker And Cybersecurity Movies (cybersecurityventures.com)
        iv. From Zodiac to The Imitation Game, Movies and Series About Codes & Codebreakers (spyscape.com)
        v. The Chatter Podcast: Cryptography in History and in the Movies with Vince Houghton - Lawfare (lawfareblog.com)
        vi. Six Times Encryption Made It to the Movies (mozilla.org)
        vii. Four movies about the Enigma Machine - Cliomuse.com
2. **Artículos**
    a. El artículo “Decoding a legacy” **(Thompson, 2015)** hace un estudio breve de “The imitation game”.
    b. El artículo “Creating a Stilyzed Caper” **(Argy, 2009)** habla sobre la película “The red machine”.
    c. El artículo “Peeping Tom: A Second Look” **(Macnab, 2001)** da algunos indicios de la posible presencia de la criptografía en película como “Peeping Tom” o “Sebastian”.
3. **Libros**
    a. Obras de J. M. Sorando: “Sherlock Holmes. Juego de Sombras”, “Contact” **(Sorando, 2015)**, “The Imitation Game”, “A Beautiful Mind”, “The Da Vinci Code **(Sorando, 2020)**, “Zodiac” y “Dirty Harry” **(Sorando, 2016)**.

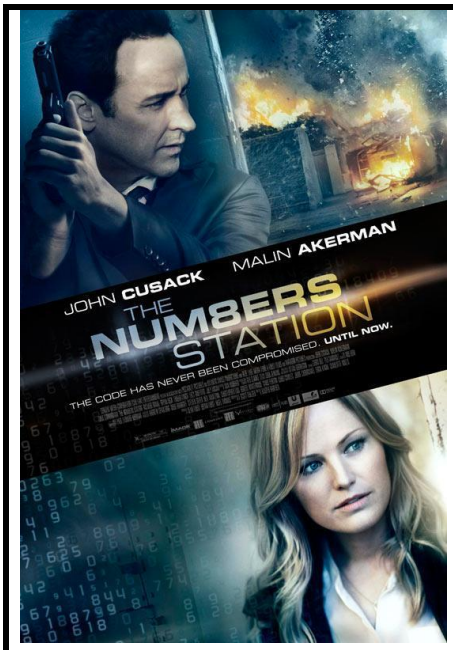
b. "Math goes to movies": listados de películas sobre criptografía **(Polster y Ross, 2012)**.
c. "The Maltese Falcon to Body of Lies: Spies, Noirs and Trust": referencias a "The good shepherd" y "The amateur" **(von Hallberg, 2015)**.
d. Novelas: "Viaje al centro de la tierra" de Jules Verne, "El escarabajo de oro" de Edgar Allan Poe, "The Key to Rebecca" de Ken Follet, "La aventura de los bailarines" de Arthur Conan Doyle, "Sherlock Holmes y el valle del miedo" de Arthur Conan Doyle, "Johny Mnemonic" de William Gibson, "El código Da Vinci" de Dan Brown.

A estas fuentes como base se fueron uniendo recomendaciones y búsquedas que aparecían a partir de otras películas y el resultado es la lista de películas que se puede encontrar en el Anexo I de esta memoria. De esta lista fui viendo películas en función de los temas que aparentemente se podían encontrar, intentando elegir películas de diferentes nacionalidades, aunque la gran mayoría fueran de Estados Unidos, y variando los géneros en lo posible, aunque los temas de criptografía aparecen principalmente en géneros como el thriller o el bélico. He priorizado en más de un 90% las películas (estrenadas en cine o en televisión) pero también he incluido en la lista algunas series, en general aquellas con episodios autoconclusivos. Un listado exhaustivo de series necesitaría de una investigación de similares características pues hay muchos productos televisivos que han abordado temas de criptografía. Por último, hay algunos productos de animación que me han parecido interesantes para diversificar el catálogo.

El tiempo disponible para realizar este trabajo no ha permitido poder ver las más de 100 películas de la lista y el total de films visionados ha sido de 76, sumando un total de 8687 minutos, lo que suponen casi 145 horas (6 días completos) contando únicamente el tiempo de visionado de la película, sin añadir tiempo de análisis, revisión y elaboración de la ficha. De ellas, 60 contenían conceptos relevantes y han originado una ficha de análisis.

4. EVALUACIÓN DE PELÍCULAS

4.1. The Numbers Station (Código de defensa)



Duración: 88 minutos
País: Reino Unido
Género: Thriller
Año: 2013
Director: Kasper Barfoed

A un agente especial estadounidense caído en desgracia (John Cusack) se le encarga la rutinaria misión de proteger a una joven civil (Malin Akerman), cifradora de códigos de defensa, en una estación emisora secreta en Gran Bretaña. Después de sufrir un ataque a la entrada, protegida y protector se refugian en la estación, donde empieza para ellos una auténtica lucha por la supervivencia. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
0:00	1:45	En títulos de crédito aparece una voz recitando números y el siguiente texto: "Since World War II, intelligence agencies have used secret stations to send encrypted assignments to agents in the field. Unlike digital and celular communications, these shortwave broadcast of encoded numbers are untraceable. Governments deny the use of such stations, but the numbers can still be heard today".
3:45	4:40	John Cusack copia números, en paralelo hay una conversación. Termina de copiar los números e inmediatamente ha descifrado el mensaje que contiene sin que haya ningún tipo de explicación sobre el cifrado. Se muestra una página de lo que parece una libreta de un solo uso (one time pad) de la que arranca una hoja y la quema.
10:20	11:30	Lo asignan a una estación en Inglaterra que se usa para retransmitir códigos a agentes en Europa como guardaespaldas de una retransmisora especialista en criptología, "una de las pocas personas que saben procesar códigos a ese nivel". Se explica lo que es una estación de números (numbers station) y en general la labor de la codificadora.
34:45	35:35	Comprueba las transmisiones y se encuentran algunas fuera de lo habitual. Cuando la experta en códigos pregunta si no se pueden deshacer (pregunta extraña teniendo en cuenta su cargo de experta en códigos), el personaje de John Cusack le explica el principio de la libreta de un solo uso de forma breve sin entrar en el cifrado, pero haciendo referencia a las imágenes del principio de la película (minuto 3:45).
58:08	58:50	La protagonista recibe un email en el que escondido entre el texto que planifica un viaje están los números escondidos de la clave.

Concepto 1: Estación de números (numbers stations)

Es el motivo y escenario central de la película. Se explica su cometido claramente en dos momentos del metraje y es escenario en el resto (esta parte no la considero para la evaluación). Según la información que se tiene las voces se generaban artificialmente por lo que emplear a una mujer parece un uso dramático.

Tiempo de representación	2min 55s (3,4%)	
Definición	Definido	Se explica dos veces lo que es una estación de números.
Funcionamiento y uso	Impreciso	El uso de una mujer para leer los mensajes se aleja de la realidad.
Representación gráfica del concepto	Dramatizada	Se trata de un búnker totalmente aleatorio, se podría parecer a algunas estaciones de números, pero no creo que sea la voluntad del film. El uso de una mujer para leer los mensajes se aleja de la realidad.
Avance de trama	Sí	Es parte integral de la trama puesto que se trata del escenario principal.
Reutilización	Sí	Aparece continuamente en la trama.
Referencias en marketing	Sí	Aparece explicado en el tráiler https://www.youtube.com/watch?v=M3gAOMiYeIw

Figura 14: The numbers station – Interior de la estación

Concepto 2: One time pad (cifrado de sustitución polialfabético)

Dos apariciones interconectadas en el metraje. No hay una explicación detallada, sino que es una referencia rápida al método en general.

Tiempo de representación	1min 45s (1,98%)	
Definición	Parcial	Se dice el nombre sin definición.
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Realista	Las páginas de la libreta podrían corresponder a fotos que se encuentran de one time pads reales.
Avance de trama	Sí	Es parte de la trama puesto que es el origen de la asignación del

		protagonista a la estación de números y del desarrollo final en el que se tienen que reenviar mensajes cancelando los que se han enviado no oficialmente.
Reutilización	Sí	
Referencias en marketing	Sí	Aparece una imagen en el tráiler https://www.youtube.com/watch?v=M3gAOMiYeIw

Figura 15: The numbers station – Hoja de one time pad

Concepto 3: Esteganografía

En un email aparentemente normal sobre un viaje hay escondidos una serie de números que son la clave que se ha usado para enviar los mensajes.

Tiempo de representación	42s (0,8%)	
Definición	Indefinido	No se dice el nombre del concepto.
Funcionamiento y uso	Correcto	En la imagen se van destacando los números insertados en un mail normal.
Representación gráfica del concepto	Realista	Se utilizan efectos cinematográficos para resaltar las letras, pero el uso es realista.
Avance de trama	Sí	Gracias a este uso se descubre el código.
Reutilización	No	
Referencias en marketing	No	

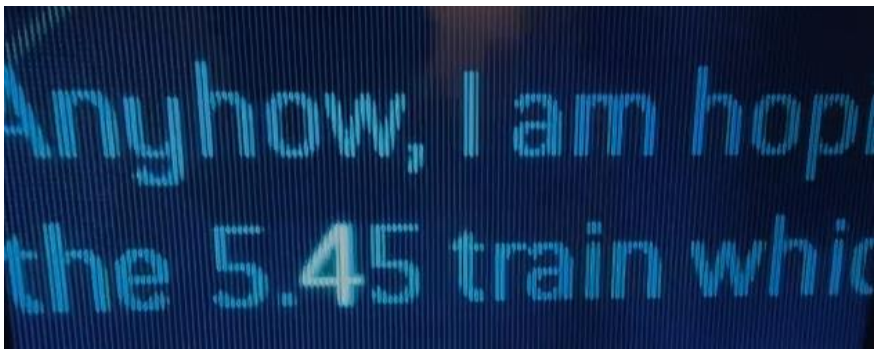
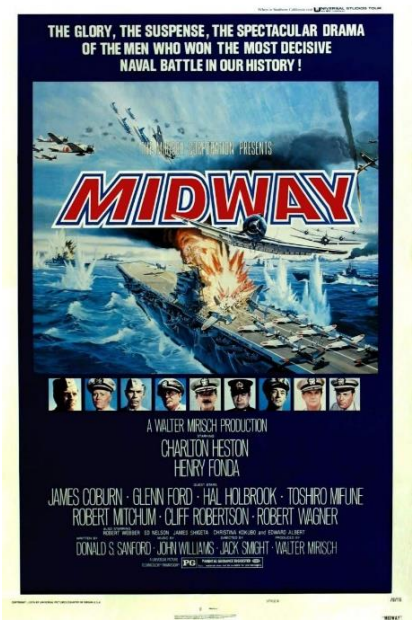


Figura 16: The numbers station – Correo con mensaje oculto

4.2. Midway (La batalla de Midway)



Duración: 132 minutos
País: Estados Unidos
Género: Bélico
Año: 1976
Director: Jack Smight

Segunda Guerra Mundial (1939-1945). En el verano de 1942 empezó la guerra naval, en la que norteamericanos y japoneses se enfrentaron por el dominio del Pacífico. Mientras la flota de portaaviones japoneses luchaba para destruir las naves enemigas y conquistar Midway, las fuerzas estadounidenses intentaban resistir el envite. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
6:45	7:35	En la base de Pearl Harbor se habla de los mensajes interceptados a Japón, se indica que se conoce la clave y que se puede descifrar un 10%.
8:35	8:45	Se intercepta un mensaje y se hace mención por primera vez a AF. En la imagen se ve una tira de papel con el mensaje interceptado.
17:30	18:35	Conversación entre los militares sobre AF, obtenido en varios mensajes. En un anterior mensaje desencriptado se obtuvo la misma mención y analizando la ruta del piloto que envió el mensaje se ha deducido la localización. Se pone en marcha un plan para asegurar que AF es Midway enviando un mensaje con una noticia falsa sobre Midway.
20:22	20:41	Llamada indicando que los norteamericanos han descifrado un mensaje en el que se confirma que para los japones AF es Midway.
27:42	28:00	Se indica que los japoneses han cambiado su clave JN25 que les permitía descifrar mensajes – tiempo para descifrar la nueva clave (1 mes o 2).

Concepto: Captura de mensajes cifrados que supone una ventaja táctica

El concepto sobre el que gira la película en su parte inicial es la importancia que la captura de mensajes tuvo en las batallas durante la Segunda Guerra Mundial, aquí reflejada entre Estados Unidos y Japón. No hay conceptos detallados, se muestra una situación histórica. A partir del minuto 30 la película se convierte en un film bélico sin referencias a mensajes o a criptografía.

Tiempo de representación	2min 42s (2,8%)	
Definición	Parcial	Se explica levemente la importancia de capturar mensajes sin entrar en detalle.
Funcionamiento y uso	Impreciso	Se muestra cómo se consiguen informaciones o cómo se confirman otras sin entrar en detalle.
Representación gráfica del concepto	Dramatizada	No es importante mostrar cómo se capturan informaciones.
Avance de trama	Sí	Gracias a los mensajes interceptados se consiguen ventajas tácticas
Reutilización	Sí	
Referencias en marketing	No	

4.3. Red Sparrow (Gorrión rojo)

Duración: 134 minutos
País: Estados Unidos
Género: Thriller
Año: 2018
Director: Francis Lawrence

Dominika Egorova (Jennifer Lawrence) es reclutada contra su voluntad para ser un "gorrión", una seductora adiestrada del servicio de seguridad ruso. Su primer objetivo es Nate Nash (Joel Edgerton), un funcionario de la CIA que dirige la infiltración más confidencial de la agencia en la inteligencia rusa. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:25	1:40	Nate Nash recibe un mensaje por teléfono, una serie de letras que apunta en una hoja en vertical.
2:00	2:05	Arranca la tira de papel.
2:10	2:20	Ejemplo claro del uso de la escítala. Enrolla esa tira en un lápiz y en una de las caras aparece el lugar y la hora de encuentro con su confidente.
1:07:30	1:08:10	Segundo uso de la escítala. No es explícito como el primero. Al ser repetido se intuye lo que el protagonista hace.

Concepto: Escítala

Tiempo de representación	1min 10s (0,9%)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	Se muestra el uso correcto de la escítala en el primer corte.
Representación gráfica	Realista	En este caso, la escítala es un lápiz.
Avance de trama	Sí	Los mensajes marcan el lugar y la hora de encuentro del protagonista con su confidente y forman parte de la trama.
Reutilización	Sí	
Referencias en marketing	No	

Figura 17: Red Sparrow – Escítala

4.4. Harry Potter and the Chamber of Secrets (Harry Potter y la cámara secreta)

Duración: 154 minutos
País: Reino Unido
Género: Aventuras
Año: 2002
Director: Chris Columbus

Terminado el verano, Harry no ve la hora de abandonar la casa de sus odiosos tíos, pero, inesperadamente se presenta en su dormitorio Dobby, un elfo doméstico, que le anuncia que correrá un gran peligro si vuelve a Hogwarts. En la escuela, un terror se está apoderando de todos. En tal circunstancia, la atención se centra en Harry, y todos empiezan a dudar de él. (FILMAFFINITY)

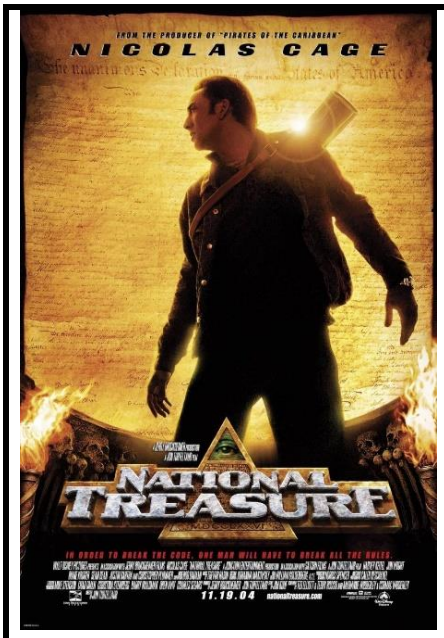
Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
2:02:30	2:03:10	Harry Potter se encuentra con el espectro de Tom Riddle en la cámara de los secretos. Le explica que ha utilizado a Gini para resucitar y que en realidad es Lord Voldemort. Se lo explica escribiendo con la varita en el aire, utilizando un anagrama con su nombre: “TOM MARVOLO RIDDLE/I AM LORD VOLDEMORT”

Concepto: Anagrama

Tiempo de representación	40s (0,4%)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	Se ve cómo se reordenan las letras del anagrama.
Representación gráfica	Realista	Es un anagrama que tiene sentido y es real, aunque se muestre con magia.
Avance de trama	Sí	Marca un descubrimiento importante para el protagonista.
Reutilización	No	
Referencias en marketing	No	

4.5. National treasure (La búsqueda)



Duración: 121 minutos
País: Estados Unidos
Género: Aventuras
Año: 2004
Director: John Turteltaub

Benjamin Franklin Gates (Nicolas Cage) ha dedicado su vida a buscar el legendario tesoro de los Caballeros Templarios, del que se decía que estaba escondido en algún lugar de Estados Unidos. Ben descubre la pista definitiva: un mapa oculto en el reverso de la Declaración de Independencia. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
14:38	17:05	Ben resuelve un enigma que indica que existe un mensaje cifrado invisible en el documento original de la Declaración de Independencia.
24:32	26:25	Ben explica a Abigail que en el documento original de la Declaración de Independencia hay un mensaje cifrado invisible.
1:01:00	1:04:00	Ben y Abigail descifran el mensaje cifrado invisible oculto en el documento. Lo consiguen utilizando zumo de limón y aplicando calor con un secador.
1:04:00	1:04:48	Aparece un código de sustitución por libro código. Es identificado directamente por los dos protagonistas, en lo que a priori no es un descubrimiento que se pueda considerar muy realista. Pero a continuación es explicado en detalle. Es una lista de agrupaciones de tres números que cada indican la posición de una letra en el texto clave (página, línea, número de letra en la línea). El texto clave son las cartas de Silence Dogood que se encuentran en el Instituto Benjamin Franklin en Philadelphia.
1:07:25	1:09:35	Riley utiliza a un niño para descifrar el código Ottendorf de las cartas de Silence. Se ve al niño entrar en el Instituto Benjamin Franklin y contar las letras del texto de las cartas. Visualmente lo revelan iluminando la letra.

Concepto: Esteganografía

Uso del limón y el calor para mostrar el mensaje invisible en la Declaración de Independencia.

Tiempo de representación	6 min 21s (5,2%). He contado también las dos escenas iniciales en las que se habla del mensaje invisible en la Declaración de Independencia.	
Definición	Parcial	
Funcionamiento y uso	Correcto	Se ve claramente como aplican limón y calor para hacer aparecer el mensaje en un procedimiento correcto.
Representación gráfica	Realista	Es una representación realista que muestra todo el proceso.
Avance de trama	Sí	Marca la aparición del "mapa del tesoro" que en realizad es otro cifrado.
Reutilización	Sí	.
Referencias en marketing	No	

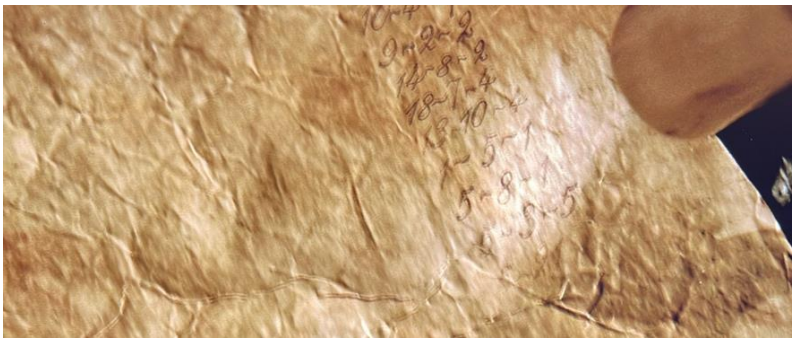


Figura 18: National Treasure – Mensaje que se hace visible con limón y calor

Concepto: Código Ottendorf o sustitución por libro código.

Tiempo de representación	2 min 58s (2,5%).	
Definición	Definido	
Funcionamiento y uso	Correcto	Se ve como el niño va obteniendo las letras y cinematográficamente éstas se iluminan.
Representación gráfica	Realista	
Avance de trama	Sí	Determina el mapa.
Reutilización	Sí	
Referencias en marketing	No	

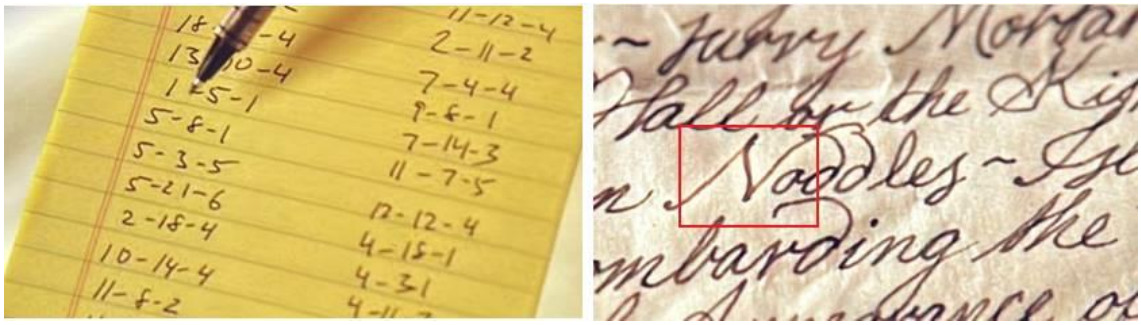
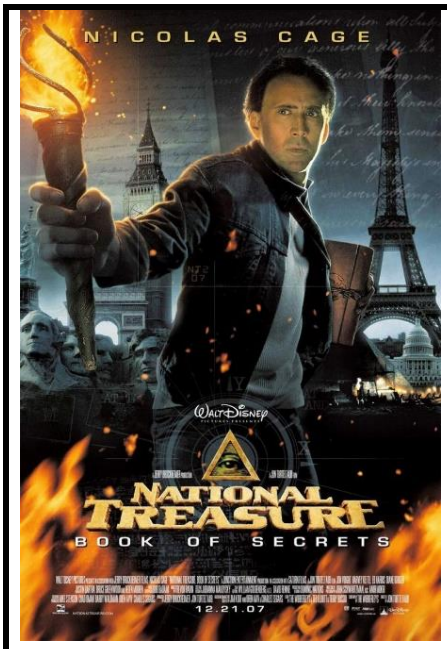


Figura 19: National Treasure – Código de sustitución por libro

4.6. National treasure 2: book of secrets (La búsqueda 2: El diario secreto)



Duración: 124 minutos
País: Estados Unidos
Género: Aventuras
Año: 2007
Director: John Turteltaub

Cuando una página del diario de John Wilkes Booth, el asesino de Abraham Lincoln, sale a la luz, el tatarabuelo de Ben se ve implicado como el principal instigador del magnicidio. Decidido a probar la inocencia de su antepasado, Ben y su equipo emprenden un viaje que los lleva a descubrir uno de los tesoros más buscados del mundo. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:30	2:10	Solicitan a Thomas Gates que examine un diario en el que aparece un mensaje cifrado (Código Playfair). Es identificado muy rápido lo que me parece poco realista, pero durante la escena explica que necesita una palabra o una clave para descifrar.
3:30	3:50	Aparece Thomas Gates resolviendo parcialmente el mensaje cifrado. No puede acabar de resolverlo porque le asesinan.
13:30	15:55	Ben le pide a Abigail que le deje ver una página del diario de Booth donde puede haber un mensaje cifrado. Van al museo y examinan la página con infrarrojos y en el reverso descubren un código cifrado (código Playfair).
16:55	17:11	Mediante un programa de ordenador tratan de descifrar el Playfair utilizando palabras clave aleatorias.
18:45	19:30	Ben Gates habla con su padre y gracias a un recuerdo descubre una posible palabra clave (Death) para descifrar el código. Ben le pide a Riley que la utilice en el programa y consiguen descifrar parte del texto.
20:12	20:45	Ben llama a Abigail para explicarle que han descifrado parte del mensaje. Con su ayuda deducen la otra palabra que estaba incompleta.
35:02	35:50	Ben y Abigail descubren en el escritorio de la reina en Buckingham Palace una parte de una tablilla que tiene grabado unos símbolos que creen que son incas o aztecas.
43:30	44:09	El padre de Ben reconoce los símbolos (indios americanos precoloniales) y puede identificar uno de ellos (Cíbola).
46:56	48:38	La madre de Ben es experta en traducción y confirma que es lengua Olmeca y traduce el grabado.
1:20:28	1:22:42	Mitch, el antagonista, pide a la madre de Ben que interprete la otra parte de la tablilla, ella dice no reconocerlo, pero Mitch la amenaza. El padre de Ben también va a pedirle la traducción.
1:45:35	1:45:50	La madre de Ben encuentra grabados en un altar y explica que permitirán traducir la lengua Olmeca y obtener conocimiento sobre las culturas precolombinas.

Concepto: Cifrado Playfair

Tiempo de representación	5 min (4%) – agrupando las diferentes escenas en las que se menciona o se intenta descifrar el mensaje.	
Definición	Parcial	Se nombra, pero no se explica.
Funcionamiento y uso	Impreciso	
Representación gráfica	Realista	El mensaje esté presentado en pares de letras para que lleve a los personajes a pensar en un cifrado digrámico y en el programa del ordenador se muestra la matriz de cifrado.
Avance de trama	Sí	Marca el siguiente paso de la investigación.
Reutilización	Sí	
Referencias en marketing	No	

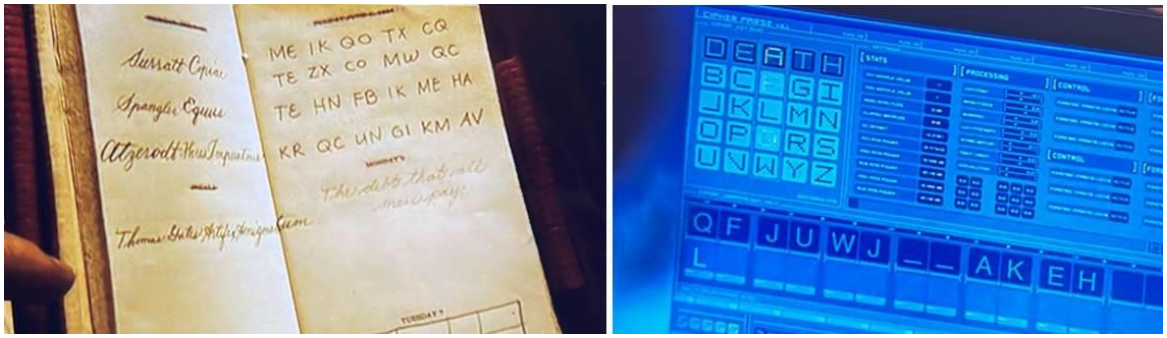


Figura 20: National Treasure 2 – Cifrado Playfair

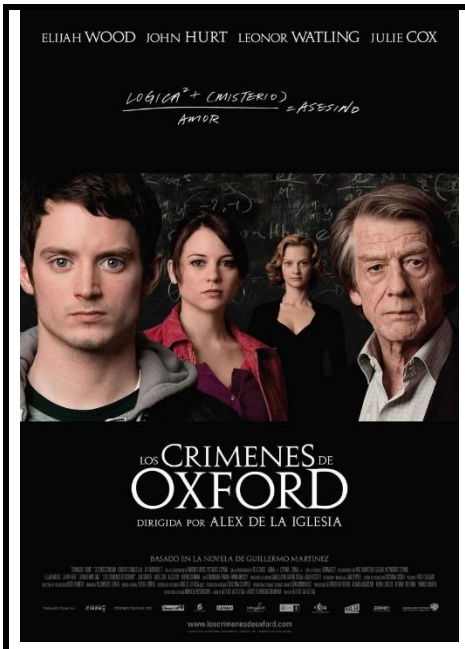
Concepto: Jeroglíficos - Olmeca

No se considera un tipo de código puesto que en su época no había intención de ocultar un mensaje. Lo añado porque, desde el punto de vista actual, el proceso de descifrado no se aleja del de un código intencional.

Tiempo de representación	5 min 38s (4,5%)	
Definición	Parcial	Se nombra, pero no se explica.
Funcionamiento y uso	Impreciso	Se descifran jeroglíficos, pero sin explicación y no es realista porque el proceso se hace muy rápido, teniendo en cuenta que en la realidad sólo se conoce parte de los jeroglíficos Olmeca.
Representación gráfica	Realista	Los jeroglíficos se parecen a los que se han encontrado en vestigios reales.
Avance de trama	Sí	Marca el lugar donde buscar las siguientes pruebas.
Reutilización	Sí	
Referencias en marketing	No	

Figura 21: National Treasure 2 – Jeroglíficos

4.7. Los crímenes de Oxford



Duración: 110 minutos
País: España
Género: Thriller
Año: 2008
Director: Alex de la Iglesia

Un joven americano que estudia en Oxford descubre el cuerpo sin vida de su casera, una mujer que en su juventud había formado parte del equipo que descifró el Código Enigma de la Segunda Guerra Mundial. Poco después, un profesor de lógica de la universidad recibe una nota en la que se advierte que ese es el primero de una serie de asesinatos. El estudiante y el profesor deciden investigar el caso. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

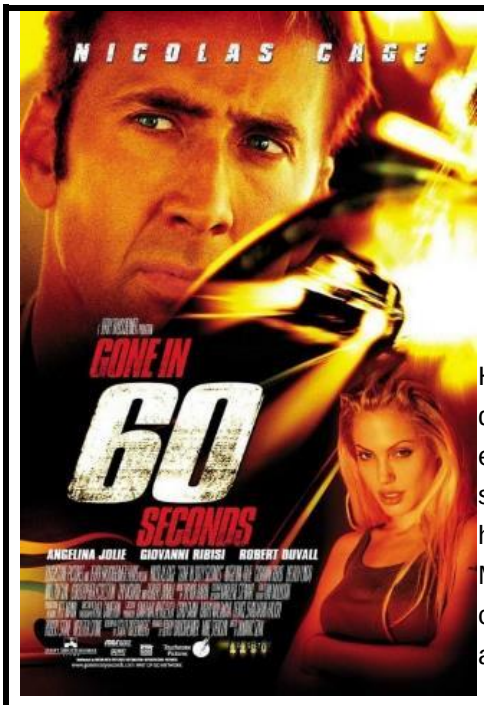
Inicio	Fin	Concepto
4:30	4:45	El protagonista encuentra una máquina Enigma en la casa donde ha alquilado una habitación para alojarse. La dueña de la casa le dice que es una copia.
4:55	5:25	En una de las fotos que hay en el salón la dueña de la casa está con Alan Turing y eso lleva a una breve conversación sobre él.
7:40	7:55	La dueña de la casa explica que los alemanes cambiaban continuamente la configuración de la Enigma y que era muy difícil descifrarla. Se establece que trabajó durante un tiempo como criptoanalista.
1:32:00	1:32:30	En una foto de la escena del crimen del día de la muerte de la dueña de la casa se ve un soporte de Scrabble con la palabra KREIS (círculo en alemán). La mujer conocía el alemán de sus años como criptoanalista y esto permite al protagonista descubrir al autor del crimen.

Concepto: Criptoanalistas durante la Segunda Guerra Mundial

En este caso el concepto representado es básicamente una persona que dedicó unos años de su vida a descifrar mensajes de los alemanes durante la Segunda Guerra Mundial. Eso conecta con el hecho de haber aprendido alemán y eso influye en el proceso de descubrir su asesino y todo el juego posterior de crímenes que se construye en la película. Las menciones a Turing y la copia de la máquina Enigma sirven para apoyar ese trabajo de juventud.

Tiempo de representación	1min 30s (1,3%)	
Definición	Definido	Se explica que descifraba mensaje y se dan detalles superficiales sobre el trabajo.
Funcionamiento y uso	No mostrado	
Representación gráfica	Dramatizado	No se dan detalles, todo queda en el terreno de la ficción.
Avance de trama	Sí	Es un elemento necesario para el descubrimiento del asesino.
Reutilización	Sí	
Referencias en marketing	Sí	Se explica en la sinopsis.

4.8. Gone in 60 Seconds (60 segundos)



Duración: 117 minutos
País: Estados Unidos
Género: Thriller
Año: 2000
Director: Dominic Sena

Hace ya tiempo que Randall "Memphis" Raines ha dejado atrás su pasado delictivo. Pero cuando se entera de que su hermano está en peligro, para salvarlo se ve obligado a hacer lo que mejor sabe hacer: robar coches. Fanático del automovilismo, Memphis es una leyenda en el negocio de robo de coches. No se le resiste ninguna cerradura, ninguna alarma. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
6:40	7:20	Atley les pide a sus secuaces que se encarguen de las paredes y de las luces cuando ve que la policía los ha descubierto. Se ve que las bombillas son negras y en las paredes hay una lista de coches. Al apagarlas la lista desaparece.
1:19:43	1:21:20	El detective Roland Castlebeck descubre que Atley Jackon ocultaba la lista de los coches que quería robar utilizando tinta invisible que se revela con luz ultravioleta. Lo hace gracias a la información del análisis de los trozos de vidrio rotos que encontraron en el almacén de Atley que corresponden a una bombilla de luz negra. Acuden al almacén y utilizando un fluorescente de luz ultravioleta ven cómo se revela la lista de coches en las paredes.

Concepto: Esteganografía (tinta invisible)

Tiempo de representación	2min 17s (2%)	
Definición	Definido	En la segunda escena se nombra y explica el funcionamiento.
Funcionamiento y uso	Correcto	A partir del principio explicado se muestra cómo se revelan los mensajes.
Representación gráfica del concepto	Realista	Aún en el contexto de una película, es una representación realista y correcta.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

Figura 22: Gone in 60 seconds – Tinta invisible

4.9. Aelita, Queen of Mars

Duración: 111 minutos
País: Unión Soviética
Género: Ciencia ficción
Año: 1924
Director: Yakov Protazanov

Adaptación de una novela del conde Alexei Tolstoi. Aelita, la reina de Marte, harta de vivir sometida a su despótico padre, lanza una llamada de socorro a la Tierra. Tras descifrar el mensaje, el ingeniero de la Estación de Radio de Moscú, al que se une el revolucionario Gusev, emprende un viaje a Marte en la nave que ha construido. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
0:55	2:40	En diferentes estaciones de Radio de la Tierra, se recibe un extraño mensaje ("Anta Odeli Uta"). Es ignorado por muchas. En Moscú, el jefe de ingeniería de la estación pide que se envíe a la oficina de cifrado.
3:30	4:10	El mensaje no se puede descifrar, aunque el protagonista, Loss, se obsesiona con que viene de Marte.
1:45:20	1:46:00	Después de mil peripecias en las que el protagonista parece que ha viajado a Marte e incluso asesinado a su esposa, se revela que el mensaje forma parte de una campaña publicitaria y que el resto de ideas son ensoñaciones de Loss. El elemento de criptografía es una falsa obsesión del protagonista.

Concepto: Códigos que vienen del espacio / empleo temprano en el cine de las oficinas de cifrado

Aunque el mensaje cifrado resulte al final ser una ensoñación de Loss, no deja de ser interesante que en una película de 1924 se empleen elementos que películas de ciencia ficción modernas, como "Contact", también utilizarán. El cifrado es un elemento anecdótico a nivel de argumento, aunque claramente lanza la acción, pero esta película es interesante como fuente de la representación temprana en el cine del uso militar del cifrado y de las oficinas de cifrado.

Tiempo de representación	3min 5s (2,8%)	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	El mensaje cifrado resulta ser una obsesión del protagonista.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	En la sinopsis.

4.10. Now You see Me 2 (Ahora me ves 2)

Duración: 129 minutos
País: Estados Unidos
Género: Thriller
Año: 2016
Director: John M Chu

Un año después de despistar al FBI y conseguir la admiración del público con sus espectáculos mentales, los cuatro jinetes vuelven a la luz pública, pero un nuevo enemigo se propone arruinar su golpe más espectacular y peligroso hasta la fecha. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
15:55	16:05	Dylan les revela el plan de "el Ojo". Para saber cómo ejecutarlo, utilizan unas linternas de luz ultra violeta para mirar un mapa que esta encima de la mesa
38:20	38:37	Walter habla de un chip que puede conectar con todos los ordenadores del planeta y que puede desencriptar cualquier cosa, romper un cortafuegos, manipular los mercados, espiar…
1:19:25	1:20:15	Dylan se encuentra atrapado en una caja que tiran al fondo del mar. Encuentra una aguja en el reloj de su padre y al retirarla se enciende una luz ultravioleta. Gracias a la luz encuentra la señal donde clavar una aguja que abre la caja.
1:24:30	1:24:40	Lula explica que el chip desencripta cualquier información.

Concepto 1: Esteganografía – tinta invisible

Tiempo de representación	1min (0,8%)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	Se usa una luz ultravioleta para revelar imágenes ocultas.
Representación gráfica del concepto	Realista	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

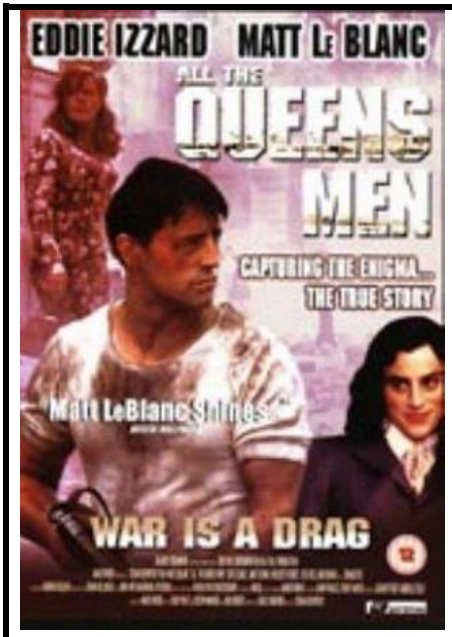
Figura 23: Now you see me 2 – Tinta invisible

Concepto 2: Máquina de desencriptado universal

Este concepto que aparece en otras películas, como “Sneakers”, tiene que ver con la necesidad de que el criptoanálisis encuentre soluciones a los métodos de cifrado de un momento determinado. En la actualidad con la criptografía de clave pública, el cifrado es altamente seguro y el cine se centra en repetir la idea de encontrar un algoritmo que puede descifrar cualquier mensaje. En esta película se lleva un poco más lejos y dicha máquina es prácticamente capaz de manipular cualquier cosa, pero el origen es el descifrado de mensajes y también de comunicaciones seguras que utilizan el mismo tipo de cifrado.

Tiempo de representación	27s (0,4%)	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	Usan la máquina para acceder a un ordenador.
Reutilización	No	
Referencias en marketing	Sí	Aparece en el tráiler https://www.youtube.com/watch?v=4I8rVcSQbic

4.11. All the Queen's Men



Duración: 99 minutos
País: Alemania
Género: Comedia
Año: 2001
Director: Stefan Ruzowitzy

Un equipo de agentes de los servicios especiales británicos dirigidos por un estadounidense debe infiltrarse, disfrazado, en una fábrica de máquinas Enigma gestionada por mujeres en Berlín y recuperar el dispositivo de decodificación que pondrá fin a la guerra. (IMDB)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
2:10	2:15	Un espía americano roba la Enigma que tiene el ejército alemán en Italia.
5:40	7:30	Los ingleses encuentran al espía americano. Se muestra la Enigma robada, y es nombrada. La Enigma es destruida por un oficial inglés (no muy brillante, lo que tiene sentido dentro del tono de comedia) por tratarse de equipo enemigo.
9:20	10:40	El ejército inglés vuelve a pedir al espía americano que consiga una Enigma. Después de su primer éxito, todas las Enigmas han sido retiradas de lugares vulnerables y los alemanes hunden barcos y submarinos que las transportan antes de ser capturadas. La misión es infiltrarse en la fábrica donde se producen, en Berlín.
12:30	13:00	Reunión con uno de los expertos en cifrado. Explica todas las combinaciones posibles de la Enigma al cifrar.
1:11:00	1:11:20	Se muestran imágenes del ensamblaje de la Enigma.
1:15:00	1:17:30	Estanterías repletas de Enigmas. El grupo de espías inglés/americano roban componentes y una Enigma.
1:24:30	1:24:50	Pierden la Enigma, pero han robado todos los componentes para construir una.
1:25:25	1:26:05	Construyen una Enigma con las partes y además, como es una máquina hecha desde cero, los alemanes no pueden saber que una fue robada.
1:29:55	1:30:10	Uno de los espías devuelve la Enigma construida porque se dan cuenta que la misión debía tener como resultado que los cogieran robando. Así los alemanes no saben que los ingleses ya tienen una y que por eso siguen intentando robarla.

Concepto: Obtención de la máquina Enigma por parte de los ingleses

El elemento más interesante de esta película es su género. Existen varios films que retratan los esfuerzos del ejército inglés por hacerse con la Enigma, como puntal para interceptar las comunicaciones alemanas durante la Segunda Guerra Mundial. Sin embargo, es muy difícil encontrar muestras de este argumento fuera del cine bélico o el thriller. El que se haga desde la comedia implica abrir la temática a otro tipo de público y darle a la criptografía otro espacio diferente al género habitual. Además, se profundiza en la idea de hacer creer al enemigo que no se tenía la máquina, para que éste no hiciera cambios en su uso.

Tiempo de representación	7min 50s (8%)	
Definición	Definido	En este caso, el concepto que trata la película no es la Enigma en sí misma, sino los esfuerzos por conseguirla y es algo que se discute en la película y que forma parte de la trama de forma clara.
Funcionamiento y uso	Impreciso	
Representación gráfica del concepto	Neutra	La Enigma se muestra, incluso el proceso de construcción, pero todo es en el contexto de una trama dramatizada para conseguirla.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	El tráiler habla de la Enigma y de la misión por conseguirla https://www.youtube.com/watch?v=Gx6zoypZwas

Figura 24: All the queen's men – Fábrica de la máquina Enigma

4.12. Batman Gotham by Gaslight (Batman Gotham a luz de gas)

Duración: 78 minutos
País: Estados Unidos
Género: Animación
Año: 2018
Director: Sam Liu

Adaptación de la novela gráfica creada por Brian Augustyn y Mike Mignola, que sitúa a Batman en el Gotham del siglo XIX con Jack el Destripador como villano. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
55:40	56:15	Bruce Wayne envía a su mayordomo un mensaje cifrado usando los hombres danzantes de Conan Doyle.

Concepto: Cifrado de sustitución monoalfabético – hombres danzantes

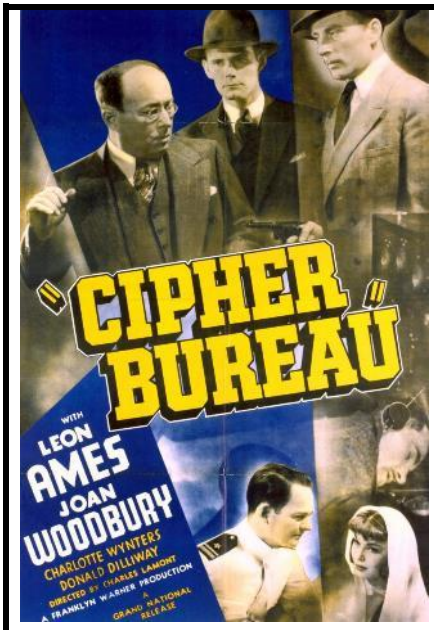
Unir Batman y Jack el Destripador en una película de animación ya resulta una combinación original que, no hay que olvidar, parte de un cómic del mismo nombre. Pero la aparición del cifrado de sustitución creado por Conan Doyle para Sherlock Holmes (los hombres danzantes) hace de esta mezcla cultural un ejemplo interesante de cómo elementos de la criptografía se cuelan en otras disciplinas y pueden generar curiosidad en el espectador. Aunque la aparición es muy breve, he decidido destacarla por tratarse de un producto muy distinto al resto de películas analizadas.

Tiempo de representación	25s (0,6%)	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Realista	No se detalla el funcionamiento del cifrado. Sin embargo, usando referencias sobre el código de los hombres danzantes, el mensaje se puede descifrar bastante correctamente “Escaping Prep Geag Bring Cycle”. El único problema es la última g de Geag que debería ser Gear. Y es consecuente con una escena posterior en la que los huérfanos le llevan una caja con la moto.

Avance de trama	Sí	El mensaje sirve para que Batman consiga el equipo necesario para perseguir a Jack el Destripador.
Reutilización	No	
Referencias en marketing	No	

Figura 25: Batman Gotham by Gaslight – Cifra de sustitución, hombres danzantes

4.13. Cipher Bureau



Duración: 64 minutos
País: Estados Unidos
Género: Thriller
Año: 1938
Director: Charles Lamont

El hermano menor de un agente secreto del gobierno se ve mezclado con una banda de espías y una hermosa agente doble. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
2:55	3:05	Encuentran libros de códigos alemanes.
5:00	5:15	Los espías alemanes escapan y su contacto les dice que usen un código alternativo.
5:30	5:45	En la oficina de cifrado americana se escucha como se están interceptando mensajes.
6:20	6:40	El tipo de cifrado que están recibiendo es totalmente diferente de lo habitual, llega en grupos de 8 letras.
17:10	17:30	Para intentar ver si el mensaje está en inglés, el mayor Waring le dice a uno de sus ayudantes que busque las frecuencias y posiciones relativas de ciertas letras.
19:15	20:00	Encuentran una estación de broadcasting con un agente emitiendo mensajes cifrados y libros de código.
21:45	22:30	Se muestra a los agentes haciendo un análisis de frecuencias. Escriben todas las letras en una pizarra y van añadiendo marcas cuando aparecen en el mensaje cifrado.
23:10	27:35	Continúan el análisis de frecuencia. Determinan que las frecuencias de las letras son consistentes con el inglés, siendo a, e, o, t las letras que más aparecen. A partir analizan las posiciones relativas entre letras que podrían ir juntas (t y h en la palabra the) porque sospechan de un cifrado por transposición. Encuentran que las combinaciones se repiten con una separación de dos líneas y empiezan a reordenar el mensaje retirando las líneas pares. Todo lo hacen usando una pizarra en la que pueden ir retirando filas de letras.
50:15	51:00	Los espías alemanes van a enviar un mensaje cifrado en música.
54:30	57:00	La espía alemana envía una carta al soldado inglés con un mensaje con un

		mensaje codificado que tiene como código tres, es decir, seleccionar una de cada 3 palabras.
1:01:40	1:05:10	Escriben la partitura del concierto que da el espía alemán. Cada nota se convierte en su letra (A,B,C, notación musical anglosajona) y lo descifran de forma rápida y sin una explicación clara.

Concepto 1: La oficina de cifrado (cipher bureau)

La película completa gira alrededor de este concepto, una oficina con militares y civiles que se dedican a labores de descifrado. Según lo que se conoce es muy improbable que las personas que trabajaban en una oficina de cifrado ejerciesen labores de espía estilo James Bond como muestra la película, pero la parte de trabajo en oficina que ocupa aproximadamente un tercio de la película está definida con relativo sentido.

Tiempo de representación	22 min (33%)	
Definición	Definido	Se nombra la oficina en la que trabajan y se explica su función.
Funcionamiento y uso	Impreciso	Se muestran las diferentes funciones de la oficina, algunas de ellas, las más propias de una película de espías, alejadas de la realidad.
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	SÍ	

Figura 26: Cipher bureau – Interceptando mensajes

Concepto 2: Análisis de frecuencias aplicado a una doble transposición

La película dedica un tiempo razonable mostrar cómo se analizan las frecuencias de las letras en un mensaje para determinar el inglés. En segundo lugar, a partir de las

posiciones relativas de palabras habituales en inglés se determina una doble transposición. El proceso está explicado con detalle, pero con suposiciones demasiado rápidas. El tiempo en el cine, y en particular en una película corta, es importante, pero hay que destacar el esfuerzo por enseñar un mínimo de técnica.

Tiempo de representación	5min 30s (8,9%)	
Definición	Definido	Se explica y nombra el análisis de frecuencias.
Funcionamiento y uso	Impreciso	El proceso de descifrado está detallado pero las deducciones son muy rápidas.
Representación gráfica del concepto	Neutra	
Avance de trama	Sí	Es importante para poder determinar los planes enemigos.
Reutilización	Sí	
Referencias en marketing	No	

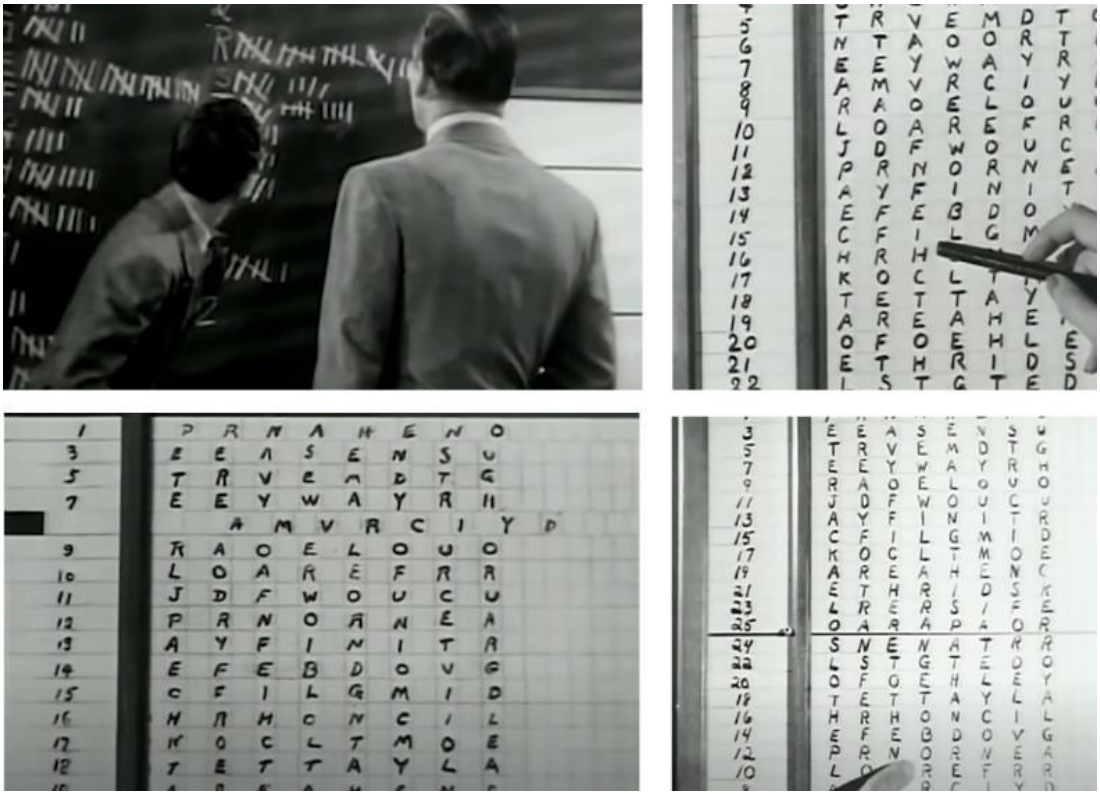
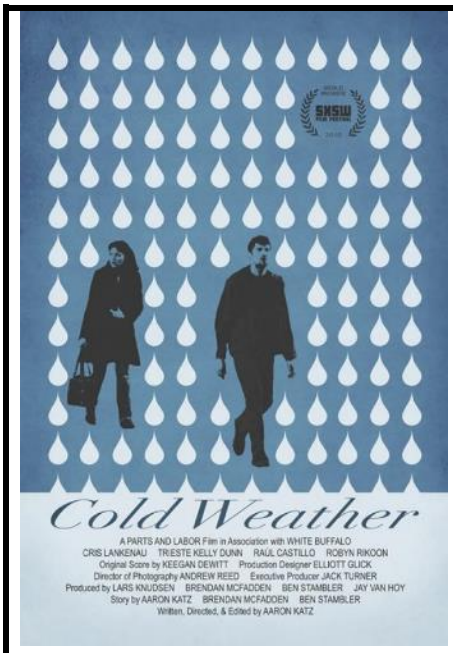


Figura 27: Cipher bureau – Análisis de frecuencias y doble transposición

4.14. Cold Weather



Duración: 96 minutos
País: Estados Unidos
Género: Drama
Año: 2010
Director: Aaron Katz

Una atípica historia de misterio en la que Doug, un estudiante de Ciencias Forenses fracasado, vuelve a su Portland natal para recuperarse, pero en lugar de eso se hunde en una espiral de desapariciones y pistas que no llevan a ninguna parte.
(FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
48:20	48:50	Al sombrear con lápiz en una hoja en blanco de una libreta, Doug ve cómo queda marcada una lista de números.
59:10	59:40	Doug le cuenta a su hermana que ha descubierto que significan los números. Son estadísticas de béisbol y usa los números como código en un libro sobre beisbol que tenía en la habitación
1:00:10	1:01:45	Doug y su hermana encuentran el libro en la biblioteca y buscan los jugadores a quien corresponden las estadísticas de la lista de números. Se dan cuenta que la primera letra de los apellidos les da el mensaje: T-H-R-E-E-P-M (3:00 pm); S-U-N (Sunday); S-E-B-R-O-O-K (SE (south east) Brooklyn St.).
1:04:25	1:04:42	Doug responde una llamada de teléfono de una cabina que es un mensaje automático que le dicta una nueva lista de números.
1:07:25	1:07:35	Doug le explica a Rachel que la llamada era para darle un nuevo código que indicaba donde quieren encontrarse con ella.

Concepto: Cifrado por libro

Esta película indie de presupuesto limitado utiliza un cifrado por libro para su trama dramática y de misterio. Es un cifrado original que emplea un libro con estadísticas de jugadores de beisbol para cifrar los mensajes.

Tiempo de representación	3min 2s (3,1%)	
Definición	Definido	Se explica el tipo de cifrado.
Funcionamiento y uso	Correcto	Se observa cómo se emplea.
Representación gráfica del concepto	Realista	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

4.15. Contact

Duración: 150 minutos
País: Estados Unidos
Género: Ciencia ficción
Año: 1997
Director: Robert Zemeckis

Tras la prematura muerte de sus padres siendo una niña, Eleanor Arroway perdió la fe en Dios. Como contrapartida, ha concentrado toda su fe en la investigación: trabaja con un grupo de científicos que analizan ondas de radio procedentes del espacio exterior con el fin de encontrar señales de inteligencia extraterrestre. Su trabajo se ve recompensado cuando detecta una señal desconocida. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
51:00	52:15	Localizan un mensaje cifrado como recepción de las imágenes de televisión que han recibido. Esas imágenes se enviaron a 25 fotogramas por segundo y las que han recibido son a 50 FPS. Al separar las imágenes entrelazadas contienen páginas de texto cifrado que son diferentes entre ellas.
56:40	56:55	Las páginas que han recibido tienen marcas en las esquinas que deberían servir para ordenarlas y descifrar su contenido. Ellie y su equipo no han encontrado ese orden.
01:03:10	01:05:20	Hadden le muestra a Ellie la clave para descifrar el mensaje. Le muestra que las páginas son tridimensionales y que así pueden conectarlas entre ellas y que cada página del mensaje está escondida la clave para resolverlo. Ellie le muestra a su equipo las páginas esconden ecuaciones elementales que son un glosario científico general que les da los símbolos de lo verdadero y lo falso. Al aplicarlo al resto del mensaje se muestran una especie de planos.

Concepto: Mensajes desde el espacio – cifrados de sustitución

Ya en “Aelita”, otra de las películas comentadas en este trabajo, encontrábamos la idea de recibir mensajes extraterrestres cifrados. “Contact” elabora mucho más esta idea y ofrece un cifrado que está explicado muy ligeramente pero que parece un cifrado de sustitución. La criptografía no es la trama principal de la película, pero sí que lanza la historia después de su primer tercio.

Tiempo de representación	2min 40s (1,8%)	
Definición	Parcial	
Funcionamiento y uso	Impreciso	No hay detalles claros respecto al cifrado empleado en los mensajes.
Representación gráfica del concepto	Neutra	La idea de las páginas que construyen un cubo para obtener el mensaje está bien representada, pero el cifrado no se muestra con detalle.
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

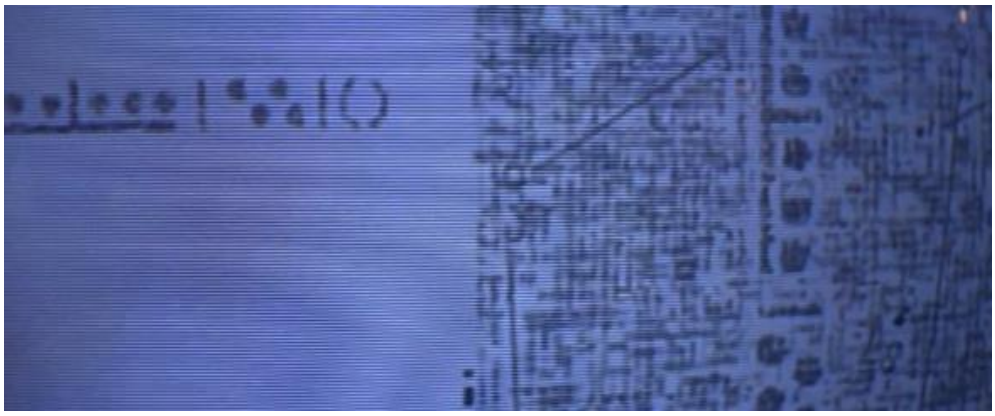


Figura 28: Contact – Los mensajes extraterrestres cifrados

4.16. From Russia With Love (Desde Rusia con amor)

Duración: 118 minutos
País: Reino Unido
Género: Thriller
Año: 1963
Director: Terence Young

El robo de un dispositivo capaz de descifrar complicadas comunicaciones está poniendo en peligro importantes investigaciones con respecto al gobierno ruso. James Bond, el agente 007 de los Servicios Secretos Británicos al servicio de Su Majestad, viajará hasta la Unión Soviética con el fin de encontrar a su objetivo. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
9:00	9:20	Spectra desvela su plan de robar a los rusos el nuevo modelo de su máquina descifradora Lektor.
19:45	20:30	Se asigna a James Bond la misión de ir a Estambul a contactar con la agente que puede recuperar la Lektor. Se explica que con la Lektor se podrán descifrar todos los códigos rusos.
52:30	53:15	Bond se encuentra con la espía rusa y hablan de la Lektor. Bond quiere un plano del consulado ruso para poder conseguirla.
58:50	1:00:30	La espía explica a Bond las características de la máquina: tamaño de una máquina de escribir, 10 kg, 24 signos y 16 cambios de claves, una cinta perforada con un mensaje cifrado se introduce en una ranura y el mensaje descifrado sale en papel continuo, en el interior tiene varios discos perforados. Desde la central de Inteligencia comunican a Bond que la descripción de la máquina corresponde a la realidad.
1:02:20	1:03:00	Robo de la Lektor.
1:45:15	1:46:00	Se vuelve a mostrar la Lektor en un hotel de Venecia en un último intento de robarla por parte de Spectra.

Concepto: Máquina Lektor (una versión ficticia de la Enigma)

El guion de esta película de James Bond, y de la novela original, gira alrededor de la recuperación de una máquina de descifrado, basada en la Enigma. En la película no se usa, pero se determina su importancia para la interceptación de mensajes durante la Guerra Fría en el universo de ficción, como réplica a lo ocurrido durante la Segunda Guerra Mundial.

Tiempo de representación	3min 25s (3%)	
Definición	Definido	Se nombra y se describe en varias ocasiones la máquina. Aunque se trata de una versión ficticia se encuentran paralelismos con la original.
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	Es una versión de ficción de la Enigma.
Avance de trama	Sí	Es el artefacto alrededor del cual gira la trama.
Reutilización	Sí	
Referencias en marketing	Sí	La máquina aparece nombrada en el tráiler y en la sinopsis https://www.youtube.com/watch?v=t9AeIdMQqR8

Figura 29: From Russia with Love – Máquina Lektor

4.17. Dope

Duración: 103 minutos
País: Estados Unidos
Género: Comedia
Año: 2015
Director: Rick Famuyiwa

Malcolm sobrevive en un barrio difícil de Los Angeles mientras manda solicitudes a universidades, realiza entrevistas académicas y se prepara para la selectividad. Pero una oportuna invitación a una fiesta clandestina le llevará a él y a sus amigos a una aventura que jamás imaginaron. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

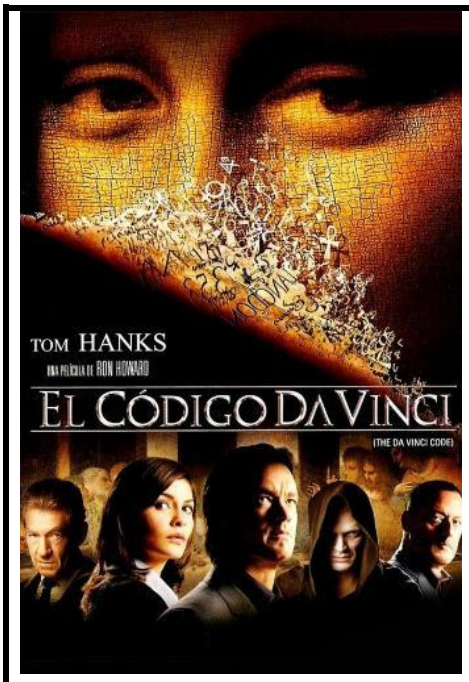
Inicio	Fin	Concepto
1:00:50	1:01:40	El grupo protagonista tiene que vender droga y decide hacerlo recibiendo el pago con bitcoins.
1:08:00	1:08:40	Ponen en marcha la web para la venta de droga y la cuenta de bitcoin para los pagos, explicando brevemente el funcionamiento.
1:20:30	1:22:05	Una vez vendida la droga necesitan recuperar el dinero. Le preguntan al experto que les ha ayudado a poner en marcha el negocio cómo hacerlo. Tienen que hacer una conversión de bitcoin a dólar. Para ello tienen que enlazar la cuenta bitcoin con una cuenta bancaria, pero habría una probabilidad de trazabilidad por parte de las autoridades. En caso de querer evitar la trazabilidad, hay que copiar los bitcoins en un disco duro y hacer el intercambio en el mercado negro.
1:27:40	1:29:00	Malcolm entrega el dinero al jefe de la operación, 10% en efectivo y el resto en la cuenta bitcoin. Le explica lo que es la cuenta de bitcoin repitiendo la explicación que les ha dado anteriormente el experto, respecto a cómo poner en marcha la cuenta y el proceso de conversión a dólares.

Concepto: Criptomonedas

Las criptomonedas son una divisa digital que emplea algoritmos criptográficos asimétricos para las transacciones. Está razonablemente explicado en una película de adolescentes más cómica que dramática. Nos encontramos frente a un ejemplo de uso de algoritmos criptográficos que, desde un punto de vista didáctico, facilita su explicación a diferente tipo de público.

Tiempo de representación	7min 10s (7%)	
Definición	Parcial	Se nombra y se define parcialmente.
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Neutra	Todo lo que tiene que ver con el proceso de cambio de bitcoins y venta de la droga está reflejado sin muchos detalles.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

4.18. The Da Vinci Code (El codigo Da Vinci)



Duración: 147 minutos
País: Estados Unidos
Género: Thriller
Año: 2006
Director: Ron Howard

Robert Langdon (Tom Hanks) acude al Museo del Louvre, cuando el asesinato de un restaurador deja tras de sí un misterioso rastro de símbolos. Con la ayuda de la criptógrafa Sophie Neveu (Audrey Tautou), descubre que la obra de Leonardo Da Vinci esconde una serie de misterios que apuntan a una sociedad secreta encargada de custodiar un antiguo secreto. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
12:20	14:00	Robert Langdon explica lo que significa la posición del cuerpo, los símbolos y marcas: el hombre de Vitruvio, el pentáculo en el pecho (icono religioso pagano, símbolo de Venus). También muestran con luz ultravioleta un mensaje escrito en el suelo (unos números y una frase: O. Dracoian Devil, Oh. Lane Saint!).
22:00	23:15	Sophie y Langdon vuelven a la sala donde está el cuerpo. Langdon se da cuenta que la serie Fibonacci esta desordenada y cree que es una pista que indica que las letras del mensaje también están desordenadas. Así se da cuenta que el mensaje escrito es un anagrama. El mensaje los lleva a otro cuadro: “Leonardo da vinci, the mona lisa”.
23:55	25:00	Sophie encuentra sangre en el suelo al lado del cuadro y hay otro mensaje que se con luz ultravioleta en la pared. Es otro anagrama que los lleva a otro cuadro: “so dark the con of man” / “Madonna of the rocks”. En el cuadro encuentran una especie de colgante de la flor de Lis
47:10	48:00	La caja fuerte contiene una pequeña caja de madera con un símbolo de una rosa. Esta contiene un criptex. Sophie explica que el criptex lo diseñó da Vinci para guardar secretos. Se escribe un mensaje en un rollo de papiro que se enrolla alrededor de un frasco de cristal que contiene vinagre y que si se intenta forzar el frasco se rompe y el vinagre deshace el papiro. La única forma de acceder es conocer la contraseña de los cinco discos cada uno con veintiséis letras (12 millones de combinaciones).
1:54:15	1:54:35	Langdon le explica a Sophie que en la tumba de Newton se veían todos los orbes imaginables menos uno, el que inspiro a Newton. La manzana. La palabra del criptex era: APPLE. Langdon había abierto el criptex antes de lanzarlo.

Concepto: Esteganografía y anagramas

La película incluye muchos enigmas, pero los que tienen relación con temas criptográficos son los ejemplos de tinta invisible y los anagramas. He añadido el criptex como curiosidad pues se trata de un artefacto para ocultar información sin cifrarla. No hay constancia que Da Vinci llegase a usarlo.

Tiempo de representación	4min 50s (3,2%)	
Definición	Definido	
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Realista	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparecen en el tráiler https://www.youtube.com/watch?v=5sU9MT8829k

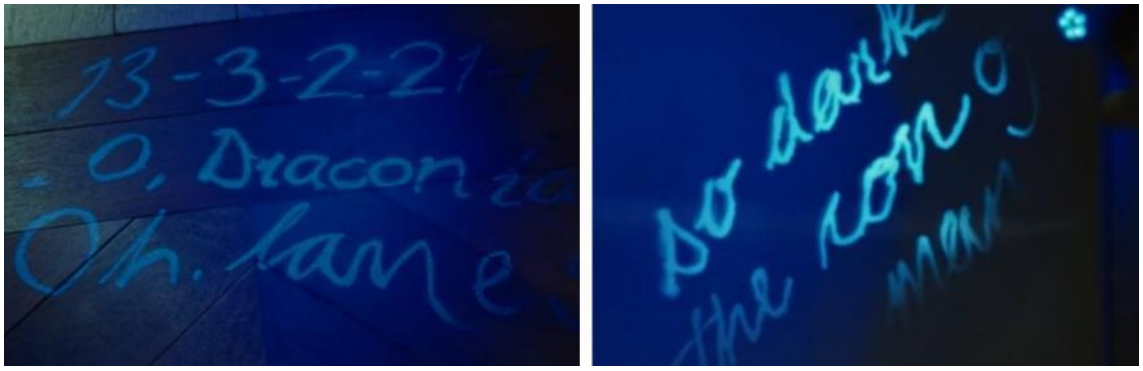


Figura 30: The Da Vinci Code – Tinta invisible

4.19. The Fourth Protocol (El cuarto protocolo)

Duración: 119 minutos
País: Reino Unido
Género: Thriller
Año: 1987
Director: John Mackenzie

El gobierno británico busca a un implacable y frío oficial del ejército ruso que llega a Inglaterra con una identidad falsa y se instala cerca de una base militar norteamericana. Se trata de averiguar cuál es su misión para impedir que la lleve a cabo. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:20:40	1:21:15	El espía ruso Petrofsky recibe un mensaje cifrado con rejilla. En la escena no se observa el descifrado, pero teniendo en cuenta los pocos orificios del papel parece una rejilla con transposición que hay que rotar.
1:23:30	1:23:40	La espía que está con Petrofsky ve la marca de la escritura del mensaje (“Kill Her”) que se ha obtenido del mensaje cifrado.

Concepto: Rejilla de Cardano

Tiempo de representación	45s (0,6%)	
Definición	Indefinido	
Funcionamiento y uso	Impreciso	Se muestra cuando coloca el papel con los orificios sobre el mensaje, pero no se precisa el funcionamiento.
Representación gráfica del concepto	Realista	El principio de funcionamiento es realista pero no se muestra completo.
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

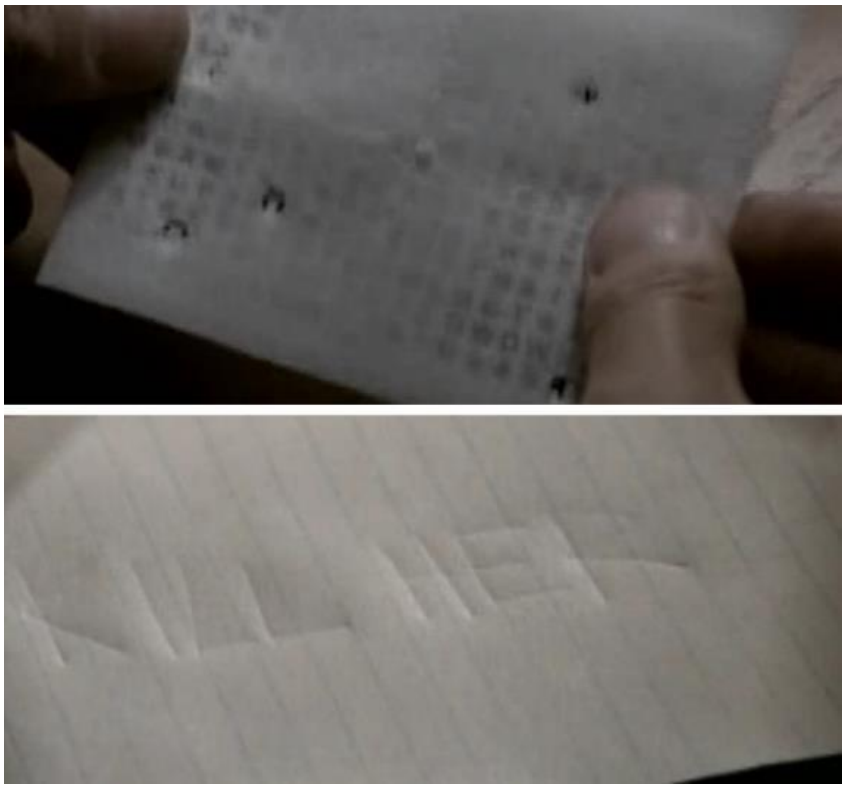


Figura 31: The fourth protocol – Rejilla de Cardano

4.20. El escarabajo de oro

Duración: 81 minutos
País: España
Género: Aventuras
Año: 1999
Director: Vicente J. Martín

Después de la muerte de su padre y que los acreedores se hicieran con su patrimonio, el joven William Legrand, acompañado de su fiel amigo Júpiter, decide irse a vivir a la única propiedad que le queda para dedicarse al estudio de los insectos y a la búsqueda de tesoros. Así es como descubren un escarabajo dorado con el lomo en forma de calavera junto a una bolsa que contiene un mensaje cifrado escrito con tinta invisible. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
25:00	25:30	Pergamino con un mensaje cifrado que se revela al calentarlo.
27:15	27:45	El protagonista escribe el mensaje en una pizarra para intentar descifrarlo.
35:40	37:00	Hablan de la tinta invisible: se comenta que a lo largo de la historia se han usado preparaciones incluyendo óxido de cobalto, azufre, zumo de limón para ocultar mensajes. Se explica que se consiguió descifrar el mensaje con la ayuda de un militar, pero no se dan detalles del descifrado.

Concepto: Esteganografía (tinta invisible)

Teniendo en cuenta que el cuento original de Poe contiene una detallada explicación de cómo usar análisis de frecuencias para descifrar un mensaje con un cifrado de sustitución monoalfabético es una lástima que la película no dedique ni un segundo de su metraje a ese tema y se quede en mostrar un mensaje escrito en tinta invisible que aparece al acercar el pergamino al fuego. Las explicaciones que da sobre la tinta invisible son más detalladas.

Tiempo de representación	2min 20s (2,9%)	
Definición	Definido	Se nombra la tinta invisible y se explican diferentes compuestos usados a lo largo de la historia.
Funcionamiento y uso	Impreciso	

Representación gráfica del concepto	Dramatizada	Se muestra el proceso de revelar la tinta de forma muy cinematográfica.
Avance de trama	Sí	El mensaje da inicio a la búsqueda del tesoro.
Reutilización	Sí	
Referencias en marketing	Si	Hay ciertas referencias al pergamino y al fuego en el cartel de la película.

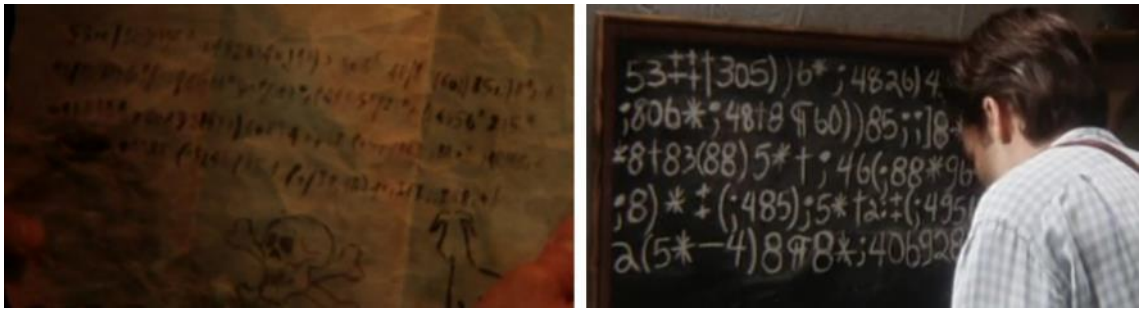


Figura 32: El escarabajo de oro – Mensaje en pergamino y copia en pizarra

4.21. The Goldbug TV Special (El escarabajo de oro Especial televisión)

Duración: 45 minutos
País: Estados Unidos
Género: Aventuras
Año: 1980
Director: Robert Fuest

Poco después de la Guerra Civil, mientras explora la isla de Sullivan, un niño se encuentra con dos excéntricos obsesionados que viven allí. Estos hombres lo ahuyentan y le advierten que nunca regrese ni que le cuente a nadie sobre ellos. Pronto, sin embargo, lo localizan y lo convocan de regreso, porque sin saberlo les ha dado una pista vital para su búsqueda y necesitan su ayuda para desentrañar el resto del misterio. (IMDB)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
14:00	14:25	Pergamino con un mensaje cifrado que se revela al calentarlo.
17:45	21:00	Se muestra el mensaje cifrado, se explica que es un código de sustitución simple (cada símbolo sustituye a una letra) y se emplea el análisis de frecuencias para descifrarlo. Se cuentan la letra con más apariciones y se hace corresponder a la e. Se describe que la palabra más usada en inglés es the y se busca en el pergamino.

Concepto: Cifrado de sustitución monoalfabético y análisis de frecuencias

Esta película corta, una adaptación juvenil de la historia de Poe, es mucho más respetuosa con el material original referente a la criptografía que la película española analizada anteriormente. Incluye de forma parcial el análisis que el autor hace en su cuento.

Tiempo de representación	3min 40s (8%)	
Definición	Definido	Se nombra el cifrado de sustitución y se explica su principio.
Funcionamiento y uso	Correcto	Se explica el descifrado usando un análisis de frecuencia.
Representación gráfica del concepto	Dramatizada	No hay una representación del proceso de descifrado, simplemente hay una explicación rápida.
Avance de trama	Sí	El mensaje da inicio a la búsqueda del tesoro.

Reutilización	No	
Referencias en marketing	No	

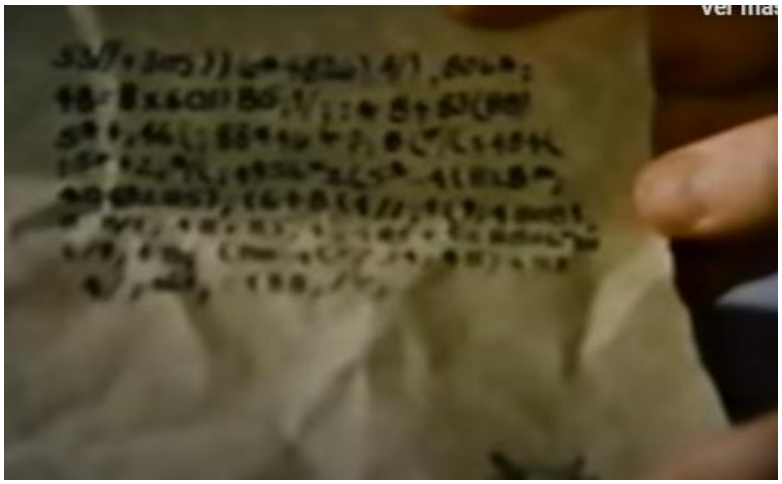


Figura 33: The goldbug tv special – Mensaje en pergamino

4.22. The Final Countdown (El final de la cuenta atrás)

Duración: 105 minutos
País: Estados Unidos
Género: Bélico
Año: 1985
Director: Don Taylor

En las costas de Hawái, un moderno y enorme portaviones de la marina americana se ve envuelto en una gigantesca y extraña tormenta que hace desparecer la nave. Pasada la tormenta, el capitán y la tripulación descubren que se han trasladado en el tiempo al día en que se produjo el bombardeo a Pearl Harbor. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
24:35	24:50	Después de pasar la extraña tormenta, el portaaviones recibe mensajes cifrados que les resultan extraños puesto que es un cifrado antiguo y en desuso.

Concepto: Códigos en desuso

La presencia de la criptografía es muy limitada en esta mezcla de ciencia ficción estilo "The Twilight zone" con cine bélico. Sin embargo, es interesante pensar en los códigos desde una perspectiva futura. La criptografía es una disciplina que cae en la idea de "código caducado" desde el momento en el que el criptoanálisis es capaz de descifrar un código. De ahí la carrera continua entre el criptoanálisis y crear nuevos cifrados.

Tiempo de representación	15s (0,23%)	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	
Avance de trama	No	
Reutilización	No	
Referencias en marketing	No	

4.23. The Falcon and the Snowman (El juego del halcón)

Duración: 131 minutos
País: Estados Unidos
Género: Thriller
Año: 1985
Director: John Schlesinger

Christopher Boyce (Timothy Hutton), un joven seminarista, y su amigo Daulton Lee (Sean Penn) son dos tipos normales, amigos desde la infancia, que sin querer se ven envueltos en una intriga de espionaje en plena guerra fría. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
22:00	24:30	Christopher trabaja en una oficina de comunicaciones cifradas y en esta escena se muestra como extrae de una carpeta la clave del día y empieza a recibir comunicaciones.
30:20	31:55	Decepcionado porque muchos de los mensajes que lee son operaciones encubiertas en otros países que en su opinión no tienen nada que ver con la seguridad nacional, Christopher roba una de las tarjetas con las claves del día que no se había destruido correctamente.
36:55	37:30	Con la ayuda de Daulton, Christopher redacta una carta para vender los mensajes a los que tiene acceso.
41:50	44:00	Daulton contacta con la embajada de la Unión Soviética, donde están dispuestos a pagar por la información. Les entrega la tarjeta con los códigos.
1:05:55	1:06:20	Christopher envía un mensaje cifrado a los rusos para evitar usar a Daulton. El tipo de cifrado no se muestra ni se explica; simplemente hay una imagen rápida del texto en claro y del mensaje cifrado.
1:15:50	1:17:00	Christopher devuelve las tarjetas de claves de los próximos días que ha estado enviando cuando reciben una visita de la NSA, que no descubre nada.

Concepto: Guerra Fría. Interceptar comunicaciones y claves.

La película retrata el conflicto entre Estados Unidos y la URSS a la hora de interceptar y descifrar comunicaciones ajenas. Las claves de un día sirven a los protagonistas para entrar en contacto con la URSS y vender los secretos.

Tiempo de representación	8min 25s (6,4%)	
Definición	Indefinido	No se nombre ni se define ningún tipo de cifrado.
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	Hay una representación dramatizada de los libros de claves y del mensaje enviado a los rusos. No se distingue el código usado ni se explica.
Avance de trama	Sí	Es el eje principal de la trama.
Reutilización	Sí	
Referencias en marketing	No	El tráiler presenta una idea general sobre los dos protagonistas siendo espías, pero no menciona la idea de las comunicaciones.

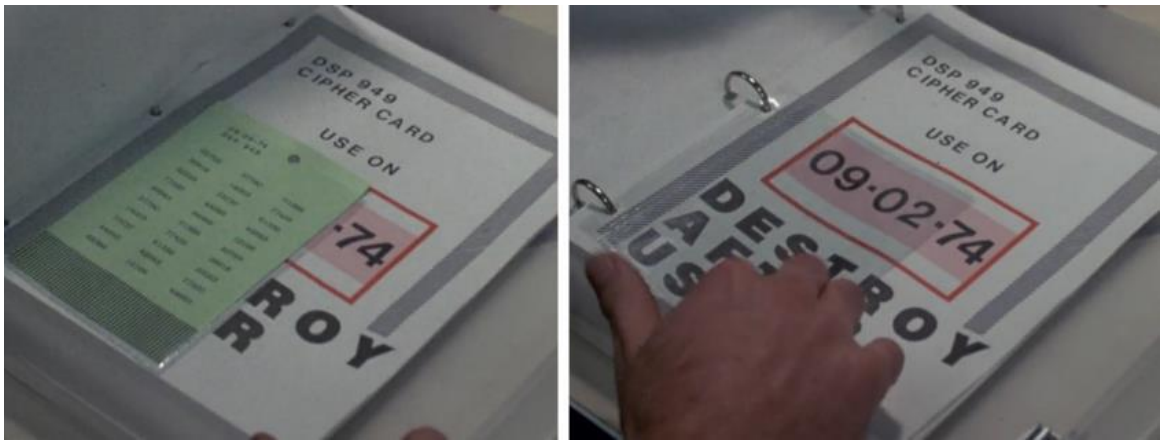


Figura 34: The falcon and the snowman – Clave del día

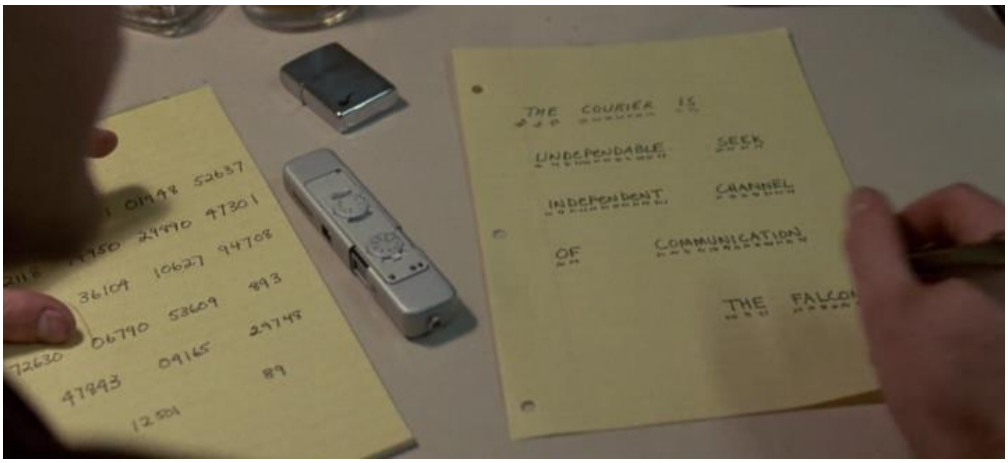


Figura 35: The falcon and the snowman – Mensaje cifrado

4.24. Enola Holmes

Duración: 123 minutos
País: Reino Unido
Género: Thriller
Año: 2020
Director: Harry Bradbeer

Cuando Enola, la hermana adolescente de Sherlock Holmes, descubre que su madre ha desaparecido, no duda en emprender su búsqueda. Tendrá que emplear todas sus dotes detectivescas para que su famoso hermano no dé con ella. Y para desentrañar la conspiración en torno a un misterioso y joven lord. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
0:45	1:20	Al principio Enola explica que su nombre al revés significa "Alone" y que su madre se lo puso porque le gustan los juegos de palabras.
3:49	4:00	La madre de Enola le ha dejado unos regalos antes de desaparecer. Entre ellos hay un libro llamado "el idioma de las flores", un disco con letras y números, una carta con letras y otra con un mensaje que dice: "usa estos regalos con cabeza".
18:25	19:10	Enola busca entre los regalos de su madre una pista que haya podido dejarle. En el envoltorio de los lápices encuentra un mensaje que dice Alone seguida de letras sin sentido. La frase está al revés y las palabras desordenadas. Enola utiliza unas fichas de abecedario para conseguir ordenar el mensaje: "Enola look on my chrisantemums"
40:55	41:40	Enola explica que para encontrar a su madre debe dejarle un mensaje cifrado para que sepa que quiere comunicarse con ella. Escribe lo siguiente: " Thank you my Chrysanthemum, are you blooming? Send iris, please". Iris es una flor que significa "tengo un mensaje para ti" según el pequeño libro que le dejó su madre, y por tanto iris significa mensaje en este contexto. Para ocultarlo, Enola mezcla las letras con un cifrado de transposición y lo publica en la sección de contactos de varias publicaciones que cree que su madre puede leer. El cifrado no se explica, pero hay que empezar a leer desde la T inferior derecha y saltar una línea hacia arriba y así sucesivamente en las columnas hacia la izquierda. Hay un error en una m y una y.
45:25	46:30	Enola descifra los anagramas de los lugares que había escuchado decir a su madre: - "The Bankmen met --> " The Embankment" - "Entangle herb" --> "Bethnal Green" - "Ellie Houseman" --> "Limehouse Lane"

1:48:20	1:49:00	Enola encuentra un mensaje extraño en la sección de contactos del periódico. Es una secuencia de números y cree que puede ser de su madre. Para descifrarlo utiliza el disco con letras y números que le dejó como regalo de cumpleaños. El mensaje dice: "meet me Royal academy five tonight mother". En realidad, no es un mensaje cifrado que se pueda descifrar con el disco, así que esta representación es incorrecta.

Concepto 1: Cifrado por transposición

Tiempo de representación	2min 05s (1,7%)	
Definición	Parcial	No se dice que es un cifrado por transposición, pero se explica brevemente su principio.
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Realista	Se usan las letras del Scrabble para montar los mensajes, pero es un recurso cinematográfico para mostrar más fácilmente lo que se haría con papel.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	https://www.youtube.com/watch?v=1d0Zf9sXlHk

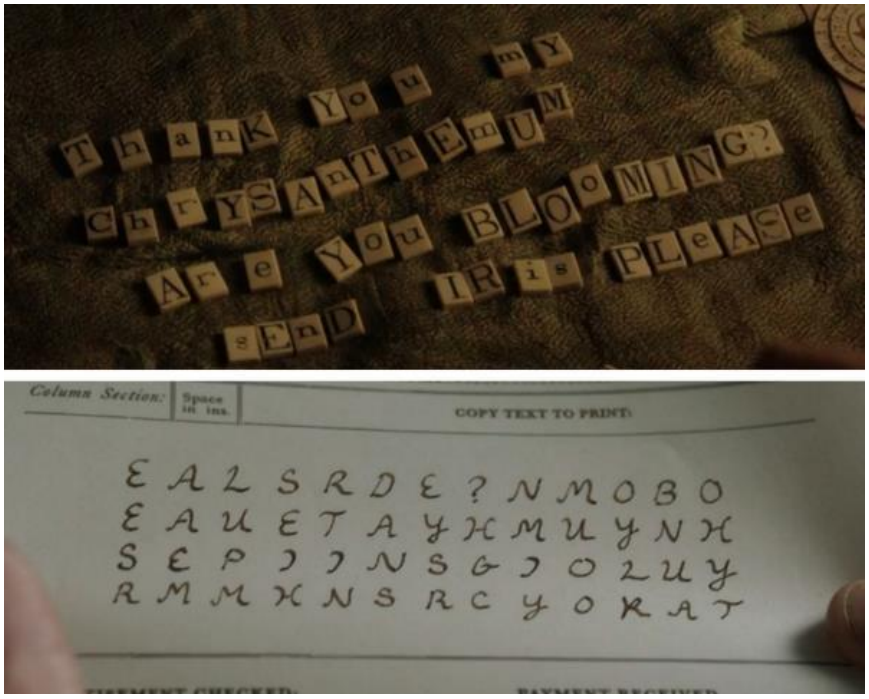


Figura 36: Enola Holmes – Cifrado por transposición

Concepto 2: Cifrado de sustitución – discos de cifrado

El mensaje que se descifra con el disco contiene probablemente un cifrado de sustitución, pero el uso del disco no es correcto.

Tiempo de representación	40s (0,5%)	
Definición	Indefinido	
Funcionamiento y uso	Incorrecto	El disco de cifrado no corresponde al mensaje que se está descifrando.
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	Sí	Aparece en el tráiler https://www.youtube.com/watch?v=1d0Zf9sXlHk

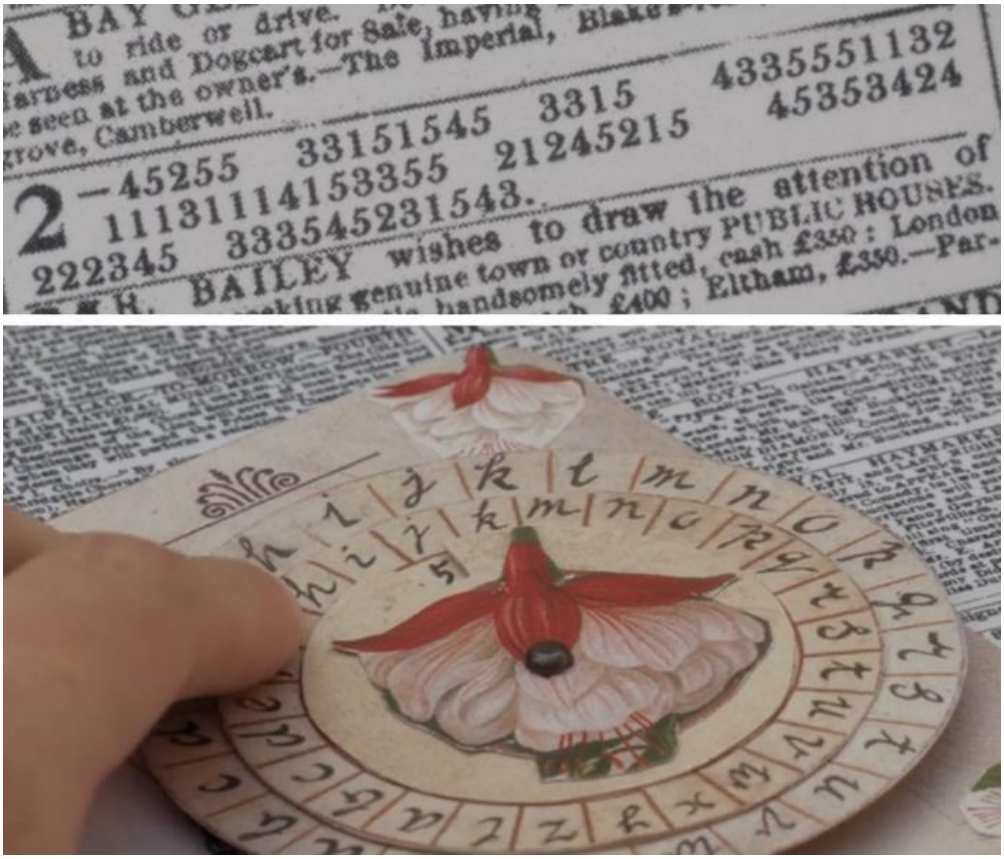


Figura 37: Enola Holmes – Cifrado de sustitución

4.25. Enola Holmes 2

Duración: 129 minutos
País: Reino Unido
Género: Thriller
Año: 2022
Director: Harry Bradbeer

Enola Holmes (Millie Bobby Brown) sigue los pasos de su popular hermano, Sherlock (Henry Cavill), abriendo su propia agencia, descubriendo que la vida como mujer detective a sueldo no es tan fácil como parece. A punto de cerrar el negocio cuando una joven cerillera sin dinero le ofrece a Enola su primer trabajo oficial: encontrar a su hermana desaparecida. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
30:45	31:20	Enola descifra el juego de palabras que se oculta en la carta que encontró en el tocador de Sarah Chapman El mensaje oculto es una dirección: “28 Bell Place, Whitechapel”. El mensaje se forma a partir de palabras homófonas y combinaciones de palabras dentro de una aparentemente inofensiva carta de amor. Es un ejemplo de esteganografía para ocultar un mensaje en otro totalmente inteligible.
51:50	52:52	Se ve a Sherlock mirando el mapa donde tiene conectado con hilos los diferentes puntos de las transacciones que se han hecho en los diferentes bancos para mover el dinero robado del caso que investiga. Se da cuenta que es un mensaje cifrado y que la secuencia de los puntos son diferentes bailes (27 bailes). Lo asocia con el libro “El lenguaje de la danza: 27 bailes”. Cada uno de los puntos es un baile y lo asocia a una letra que encuentra en el libro según la numeración de la transacción bancaria (no se aclara como se buscan los números en el cifrado por libro).
1:01:00	1:02:58	Sherlock sigue intentando descifrar el mensaje (las imágenes se alternan con las de Enola bailando y hablando con William). El mensaje es: “Good to meet you Sherlock Holmes” y firmado Moriarty (no hay explicación de cómo transforma los números de la transacción en el nombre de Moriarty).
1:48:57	1:49:02	Sherlock desenmascara a Mira Troy como MORIARTY. Se ve una reordenación de las letras del anagrama.

Concepto 1: Mensaje oculto (esteganografía)

Tiempo de representación	35s (0,4%)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Realista	Aunque la puesta en escena es cinematográfica, se muestra el funcionamiento.
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

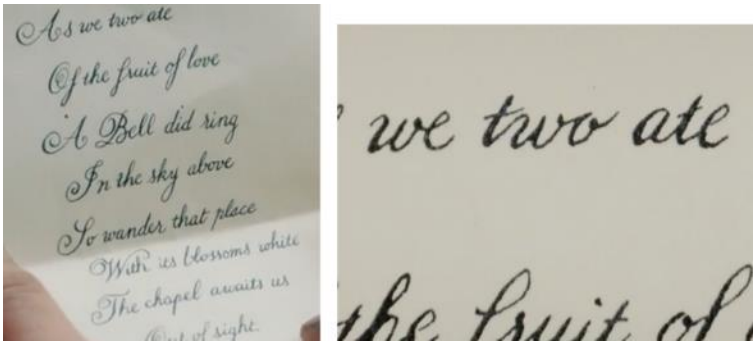


Figura 38: Enola Holmes 2 – Mensaje oculto

Concepto 2: Cifrado por libro

Tiempo de representación	3min (2,3%)	
Definición	Definido	
Funcionamiento y uso	Impreciso	
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

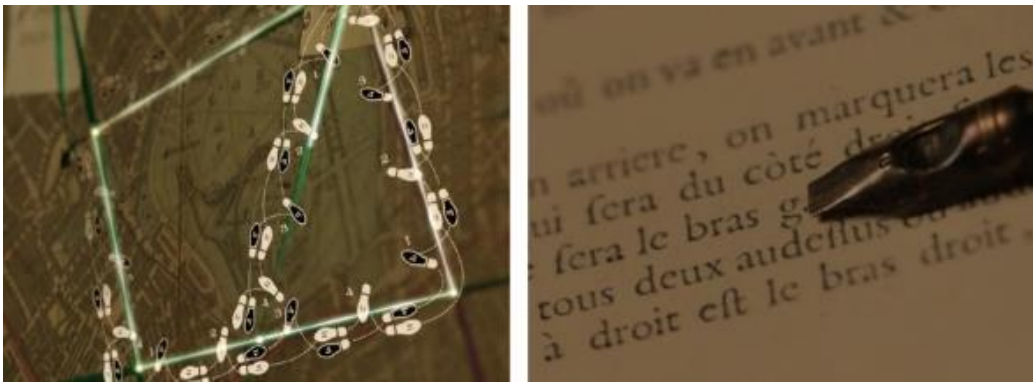


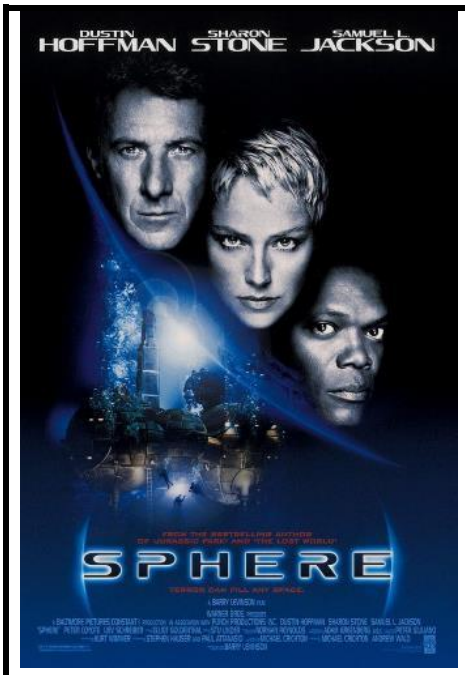
Figura 39: Enola Holmes 2 – Cifrado por libro

Concepto 3: Anagrama

Tiempo de representación	5s (0,07%)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Realista	Aunque la puesta en escena es cinematográfica, se muestra el funcionamiento.
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

Figura 40: Enola Holmes 2 – Anagrama

4.26. Sphere (Esfera)



Duración: 134 minutos
País: Estados Unidos
Género: Ciencia ficción
Año: 1998
Director: Barry Levinson

En las profundidades del Océano Pacífico se esconde uno de los secretos mejor guardados del gobierno americano y posiblemente el mayor descubrimiento de la historia de la humanidad: una nave aparentemente alienígena que se conserva intacta desde hace casi 300 años. Un equipo de científicos viaja al fondo marino con una inquietante misión: analizar la nave e investigar su origen. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
48:00	51:05	En las pantallas de la base submarina empieza a aparecer un código numérico y luego las pantallas vuelven a la normalidad. Un miembro de la tripulación muere. El código numérico vuelve a aparecer.
57:10	57:25	Aparecen mensajes cifrados en todas las pantallas de la nave.
58:30	1:01:30	Detectan que el mensaje no es aleatorio, tiene un patrón. Lo definen como un código. Lo convierten a binario y deducen que las letras del alfabeto están presentadas desde el punto de vista de la esfera, de la manera como la esfera ve un teclado, siguiendo una espiral. Aparece el primer mensaje “Hello. How are you? What is your name? My name is Jerry”. Con la reorganización del teclado son capaces de comunicarse.
1:37:20	1:38:40	El personaje interpretado por Dustin Hoffmann intenta rehacer la clave del cifrado porque es incorrecta. La frase inicial era “My name is Harry”
1:43:20	1:44:00	Reciben un mensaje cifrado de la superficie en grupos de tres letras que los propios algoritmos del sistema descifran.

Concepto: Cifrado de sustitución monoalfabético

La “esfera” de la película se comunica mediante una variación de un teclado QWERTY desde una perspectiva circular. Es decir, las letras están dispuestas en espiral y esa nueva disposición sustituye a la de un teclado original. Es importante añadir que en la cuarta escena en la que se habla de este código cuando el personaje interpretado por Dustin Hoffmann se da cuenta de que la clave es incorrecta, nos encontramos ante un momento de giro de guion sin demasiada lógica con respecto al cifrado puesto que la

única palabra incorrecta en el cifrado es el nombre que permite al protagonista entender la situación.

Tiempo de representación	7min 40s (5,7%)	
Definición	Parcial	No se dice el nombre, pero se define que es una sustitución del teclado
Funcionamiento y uso	Impreciso	Se muestra de una forma general cuál es la sustitución, pero el proceso no se hace visible de forma precisa.
Representación gráfica del concepto	Dramatizada	Es una representación claramente cinematográfica de un cifrado de sustitución, sin prestar atención a la lógica real.
Avance de trama	Sí	Permite comunicarse con la esfera.
Reutilización	Sí	
Referencias en marketing	No	

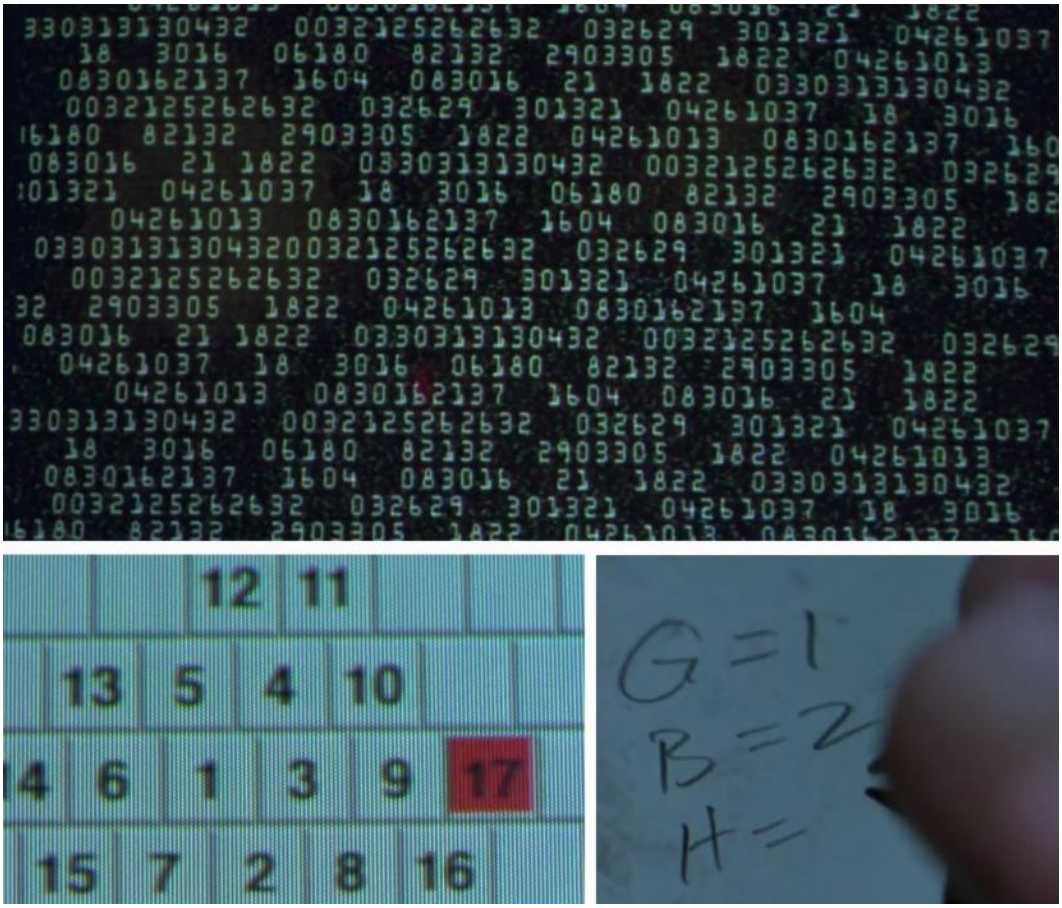


Figura 41: Sphere – Cifrado de sustitución monoalfabético

4.27. Gravity Falls

Duración: 22 minutos
País: Estados Unidos
Género: Animación
Año: 2012-2016
Creador: Alexander Robert Hirsh

Narra las aventuras de los mellizos de 12 años Dipper y Mabel Pines, que ven cómo se desvanecen sus planes para el verano cuando sus padres deciden mandarlos con su tío abuelo Stan, que vive en el corazón de Gravity Falls (Oregón). Pronto, Dipper y Mabel descubren que allí no todo es lo que parece. (FILMAFFINITY)

Antes de analizar esta serie, me gustaría aclarar que es una de las escasas excepciones que voy a añadir en este trabajo que incluye básicamente películas o episodios auto conclusivos de algunos productos televisivos que se pueden ver como si fuesen películas independientes. En este caso, voy a analizar una serie de televisión por dos razones: la primera, por tratarse de animación, un producto que se asocia más a los niños pero que puede establecer juegos que interesen a diferentes espectadores; la segunda, porque incluye variados ejemplos de cifrado en diferentes momentos de los episodios, desde los títulos de crédito (estableciendo un juego con el espectador) hasta momentos de la trama donde el cifrado es importante.

Voy a analizar el capítulo 1 de la segunda temporada: Scary-oke (Temible-oke).

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:15	1:18	Aparece la imagen de una celda y en la pared hay una llave con la palabra WIDDLE. Se trata de una clave para descifrar un mensaje que aparece al final del capítulo usando el cifrado de Vigenère.
11:55	12:00	Se muestran páginas de un diario que incluyen mensajes en los que las letras son inteligibles, pero no tienen sentido. Por un lado, ZDWFK RXW y por el otro, NLOO PH SOHDVH. En los dos casos se trata de un cifrado César, es decir, desplazando tres letras. De manera que el primer mensaje se convierte en Watch Out y el segundo Kill Me Please.
18:25	18:35	El protagonista tiene un diario que tiene mensajes escritos en tinta invisible que desvelan con luz ultravioleta.
22:27	22:30	Aparece el mensaje SMOFZQA JDPV. Si usamos una tabla de Vigenère con la

		palabra clave WIDDLE que aparecía al principio del episodio, obtenemos el mensaje WELCOME BACK.

Concepto: Varios cifrados (César, Vigenère) y esteganografía (tinta invisible) – uso didáctico

Es interesante que en estos casos los códigos están insertados como un juego con los espectadores. Forman parte de la trama, a veces para los personajes, a veces para el público estableciéndose un juego entre la producción y el espectador. Es un buen caso del uso de un producto de entretenimiento para enseñar una disciplina o hacer partícipe del público a ella.

Tiempo de representación	6s (0,45%) – Vigenère 5s (0,38%) – César	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	
Avance de trama	No	
Reutilización	No	
Referencias en marketing	No	

Tiempo de representación	10s (0,75%) – Tinta invisible	
Definición	Definido	
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Realista	
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

Figura 42: Gravity falls – Cifrado Vigènere (clave, mensaje)

Figura 43: Gravity falls – Mensajes cifrados (César)

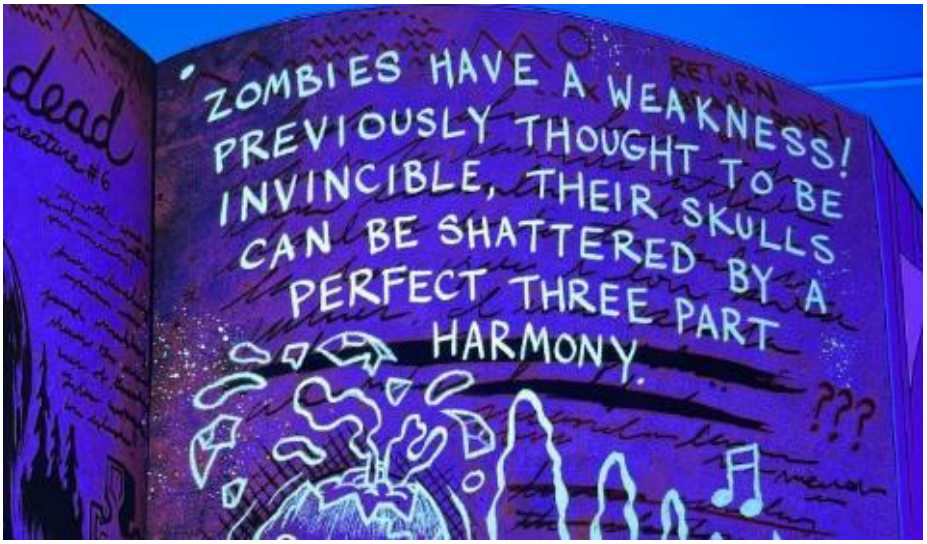
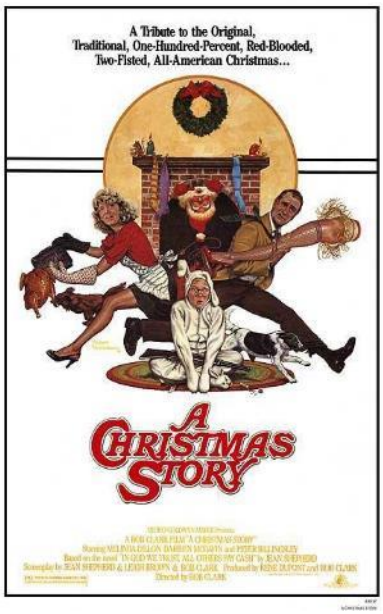


Figura 44: Gravity falls – Tinta invisible (forma parte de la trama)

4.28. A Christmas Story (Historias de Navidad)



Duración: 94 minutos
País: Estados Unidos
Género: Comedia
Año: 1983
Director: Bob Clark

En los años cuarenta, un niño quiere como regalo de navidad un rifle de aire comprimido. Claro está, los padres piensan que no es una buena idea. Comedia familiar extraordinariamente popular en Estados Unidos que se basa en las historias del humorista Jean Shepherd. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
48:05	51:05	El niño protagonista recibe el anillo decodificador que le permitirá descifrar los mensajes que dan en su programa de radio favorito. En el programa indican que se sitúe el anillo en una determinada posición y a partir de ahí emiten una serie de números. A partir de la posición del anillo que tiene los números en un disco y las letras en otro, el niño es capaz de descifrar el mensaje que resulta ser un anuncio, para su disgusto.

Concepto: Código de sustitución monoalfabético – anillo decodificador

La película incluye un código de sustitución monoalfabético representado por los anillos decodificadores, un juguete para niños. El cifrado de mensajes siempre ha estado presente en juegos infantiles y esta representación del mismo revela lo relevante que puede ser este proceso de juego para aprender más sobre las técnicas de criptografía.

Tiempo de representación	3min (3,2%)	
Definición	Indefinido	No se nombra ni se explica, es un juego infantil.
Funcionamiento y uso	Correcto	Se muestra el proceso de descifrado usando el anillo.
Representación gráfica del concepto	Realista	Se muestra un anillo decodificador realista y funciona para descifrar el mensaje.
Avance de trama	No	

Reutilización	No	
Referencias en marketing	No	

Figura 45: A Christmas story – Anillo decodificador

4.29. Hunt

Duración: 125 minutos
País: Corea del Sur
Género: Thriller
Año: 2022
Director: Lee Jung-jae

Corea del Sur, 1980. Tras el intento de asesinato del presidente Park por la agencia de inteligencia coreana, el ejército vuelve a hacerse con el poder. Corea del Norte lo ve como una oportunidad para una invasión futura y envía a uno de sus espías. Dos altos cargos de la seguridad surcoreana tienen la misión de perseguir al infiltrado. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
16:30	17:05	Aparece un papel camuflado como una factura de lavandería con una tabla con números y caracteres. En el puño de una camisa está bordado el mensaje como una serie de rayas verticales y horizontales. El receptor parece buscar la combinación de dos números en el puño de la camisa que dan el carácter en una tabla. En él se comunica una operación militar.
47:30	48:20	Un soldado que ha desertado desde Corea del Norte da a la inteligencia de Corea del Sur una copia de la tabla de cifrado.
48:55	49:30	Los agentes fotocopian la tabla de cifrado. Se empieza a usar para descifrar mensajes obtenidos en el pasado y mensajes que se interceptan.

Concepto: Cifrado con tabla

No hay mucha explicación sobre el tipo de cifrado usado, salvo que hay una tabla y combinaciones de números que proporcionan un carácter para obtener el mensaje en claro.

Tiempo de representación	2min (1,6%)	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	Forma parte de la representación que hace el guion de ese tipo de cifrado. No se muestra claramente el proceso de descifrado ni se dan muchos detalles salvo una tabla de cifrado.

Avance de trama	Sí	Sirve para empezar a encontrar al topo que hay infiltrado.
Reutilización	Sí	
Referencias en marketing	No	

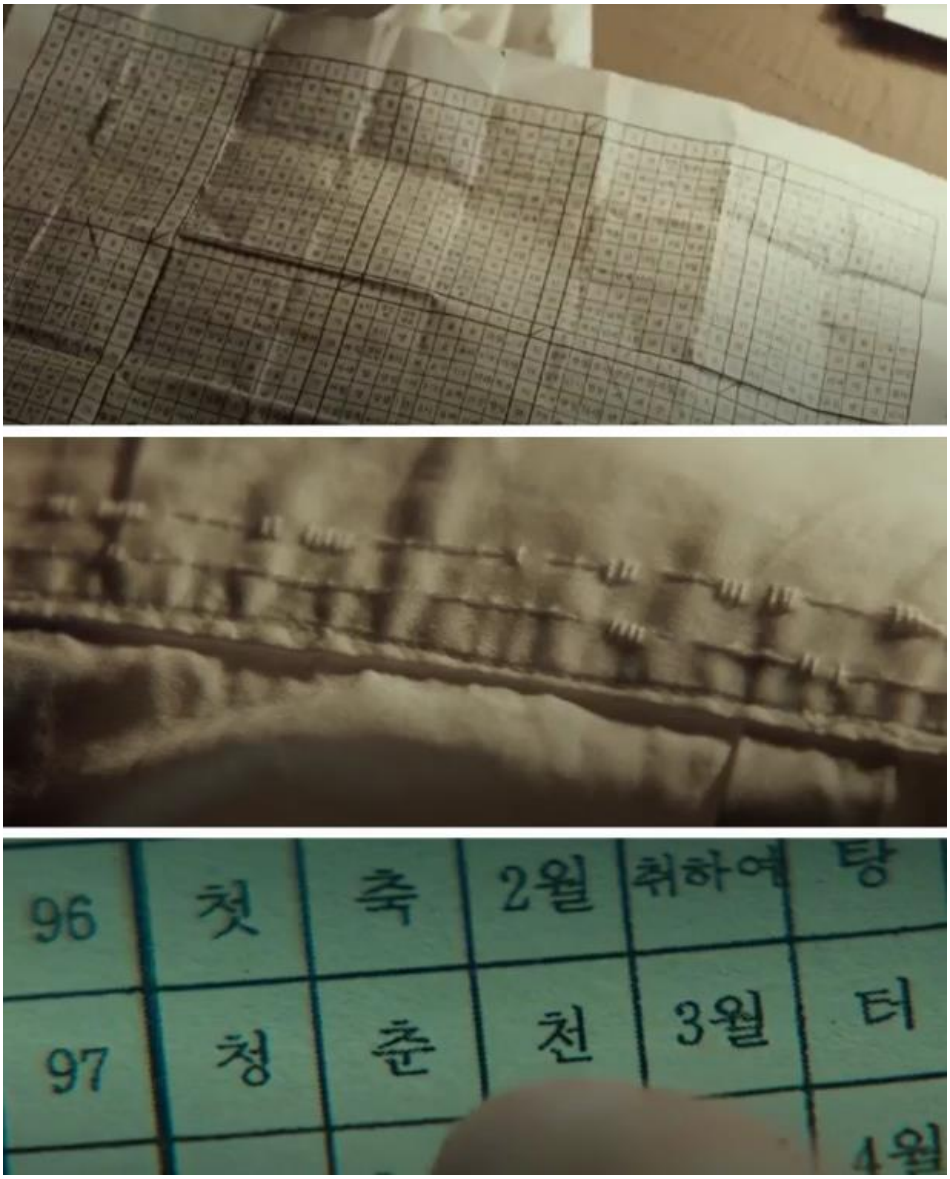


Figura 46: Hunt – Cifrado con tabla

4.30. Johnny Mnemonic

Duración: 96 minutos
País: Estados Unidos
Género: Ciencia ficción
Año: 1995
Director: Robert Long

Corre el año 2021 y la mitad de la población sufre de una enfermedad llamada "síndrome de atenuación de los nervios". Johnny (Keanu Reeves) es un mensajero de información, una persona que lleva los datos más importantes del siglo XXI, directamente implantados en su cerebro. Su información será muy valiosa para una corporación farmacéutica. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
9:30	15:30	Se inserta la información en el cerebro de Johnny y se encripta. Para encriptar, Johnny explica el procedimiento: el cliente hace click en 3 frames de la televisión, obteniendo tres imágenes que se usará para cifrar y que se deben enviar vía fax (en el mundo de la película conectados a través de internet y no a través del teléfono, que aportaría pérdidas) al receptor para el desencriptado. Johnny, el correo, no sabrá cuales son las imágenes y no puede acceder a la información. Unos asesinos de la yakuza interrumpen el proceso, la información se carga en el cerebro, pero las tres imágenes no se envían por fax. En la lucha, Johnny se queda una, los yakuza otra y la tercera desaparece.
36:20	36:35	Johnny explica brevemente a Jane, su guardaespaldas, que la información está cifrada con un código, haciendo referencia a las imágenes.
55:00	55:50	Intentan extraer la información de Johnny sin las imágenes usando algunos códigos usados normalmente. Teniendo en cuenta que se usaron imágenes aleatorias de la televisión, no es posible descifrarlo.
1:11:00	1:16:30	La resistencia tiene un descifrador que puede ayudar a Johnny. Se trata de un delfín con implantes que puede acceder a la información de Johnny utilizando una parte de los códigos y extrayendo el resto de su cerebro. La yakuza interrumpe el proceso.
1:21:20	1:21:30	Johnny consigue otra de las imágenes.
1:24:00	1:28:30	Se vuelve a conectar para que el delfín intervenga de nuevo teniendo más partes del código. Consiguen recuperar la tercera imagen y empiezan a desencriptar y enviar la información.

Concepto: Cifrado simétrico

Dentro de una trama de ciencia ficción basada en un relato de William Gibson, el cifrado que se utiliza para la información es una especie de cifrado simétrico en el que la clave debe ser enviada al receptor. No es ningún cifrado conocido pero el proceso sería el mismo que para otros cifrados de clave simétrica. El principal problema del sistema, tal y como se ve al final, es que la clave está almacenada con la información, práctica que no es segura.

Tiempo de representación	17min 15s (17,9%)	
Definición	Parcial	
Funcionamiento y uso	Impreciso	
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

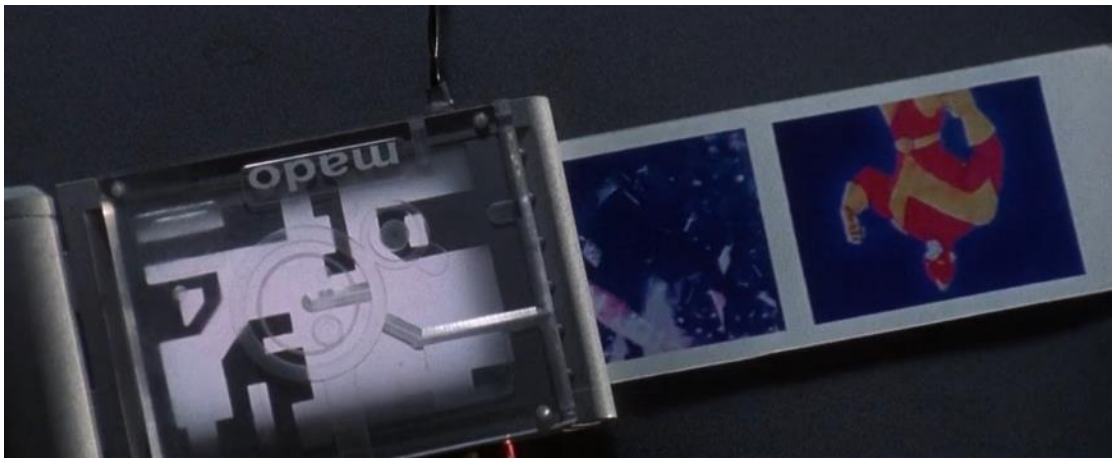
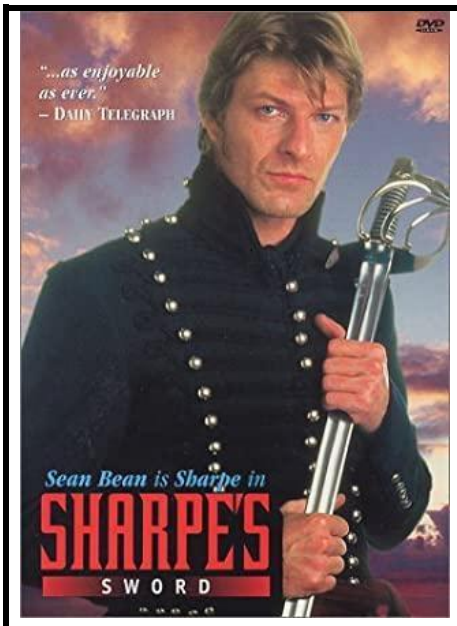


Figura 47: Johnny Mnemonic – Imágenes cifrado

4.31. Sharpe's Sword (La espada de Sharp)



Duración: 101 minutos
País: Reino Unido
Género: Bélico
Año: 1995
Director: Tom Clegg

Sharpe debe proteger al espía más importante de la red de Lord Wellington, pero ciertos asuntos domésticos, una joven traumatizada y la posibilidad de que haya espías franceses ponen en peligro el éxito de su misión. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
14:15	14:30	Se encuentra un papel con una serie de números que podrían ser un cifrado por libro.
25:10	25:30	Consiguen un libro que podría ayudar a descifrar el mensaje del que solo logran salvar unas cuantas páginas.
31:50	33:05	El libro es Candide de Voltaire y dado que es un libro bastante común podrían encontrar un ejemplar en la ciudad a la que viajan, a partir del cual descifrar el mensaje.
1:09:50	1:10:10	Consiguen Candide y empiezan a descifrar el mensaje. No se muestra en detalle el proceso, simplemente cómo buscan letras y palabras y las copian.
1:11:40	1:12:20	Una vez descifrado, explican cómo funcionaba esta cifra en particular: el primer número es la página, luego el número de la línea y de la palabra y al final la letra dentro de la palabra.

Concepto: Cifrado por libro

El único elemento de criptografía que aparece en la película es el cifrado por libro que utiliza "Candide" de Voltaire como clave. Aparece en diferentes momentos con un nivel limitado de detalle, pero se explica brevemente cómo funciona el cifrado. Un elemento interesante a considerar es que la época que se retrata, las Guerras Napoleónicas, no son un escenario habitual en el cine y en particular en el cine que incluye elementos criptográficos.

Tiempo de representación	2min 50s (2,9%)	
Definición	Definido	Se nombra y se explica el cifrado.
Funcionamiento y uso	Impreciso	
Representación gráfica del concepto	Neutra	No es una versión que muestre detalles sobre el proceso de descifrado.
Avance de trama	Sí	Permite descubrir quién es el espía.
Reutilización	Sí	
Referencias en marketing	No	

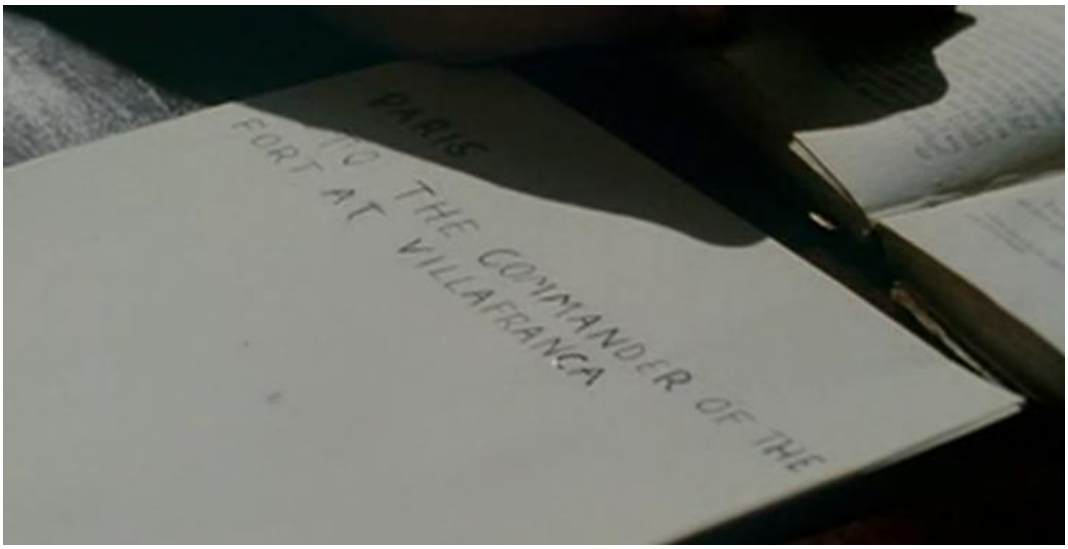
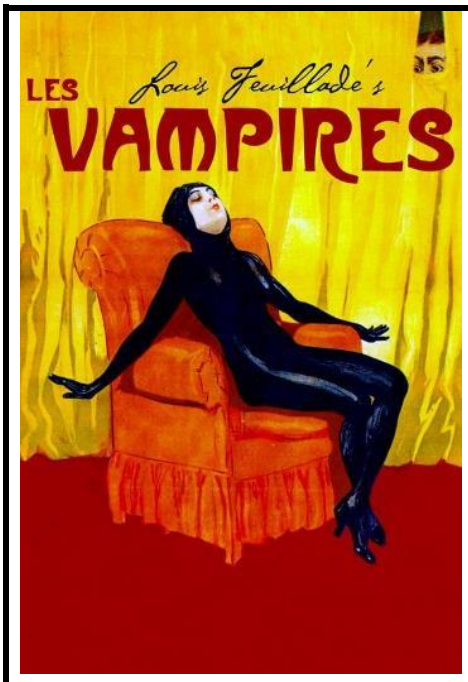


Figura 48: Sharpe's sword– Descifrado del mensaje usando "Candide"

4.32. Les Vampires



Duración: 421 minutos
País: Francia
Género: Thriller
Año: 1915
Director: Louis Feuillade

París es presa de un terror invisible y sin nombre contra el cual la policía no puede hacer nada. Una organización criminal conocida como "Los vampiros" siembra el caos con sus asesinatos, robos y secuestros. Poco se sabe acerca de esta banda de villanos, excepto que los dirige el Gran Vampiro y su seductora novia Irma Vep. Philippe Guerande es un periodista que, investigando el asesinato de un político, acaba encontrando a los vampiros. Se presentó dividida en 10 episodios. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
Tercer episodio (41 min)		
1:00	2:35	Guérande intenta descifrar un criptograma encontrado en el magistrado asesinado en el episodio anterior. Se muestra que es una transposición, primera la letra de la esquina superior izquierda, luego la de la esquina superior derecha, luego la esquina inferior izquierda y la inferior derecha. Y así sucesivamente. En el libro también se encuentra el nombre de un cabaret.
6:00	6:25	En dicho cabaret, actúa Irma Vep y el film nos muestra que es un anagrama de Vampire.
Octavo episodio (51 min)		
10:07	10:25	El Gran Vampiro le entrega un mensaje a Irma Vep cuando la mujer va a ser enviada a una cárcel en Argelia. El mensaje es un anagrama en el que le dice que salte del barco. Como en el caso anterior las letras reconstruyen el mensaje en pantalla.
Noveno episodio		
22:10	23:20	La familia de Guérande recibe un mensaje cifrado con una clave numérica. El ayudante de Guérande lo descifra con rapidez. Es un mensaje del mismo Guérande para que se reúnan con él. Es a priori un código de sustitución monoalfabético, pero no está desarrollado en el fragmento y no se puede saber con seguridad.

Concepto 1: Cifrado por transposición

Tiempo de representación	1min 35s (3,9%) Duración del capítulo: 41min (capítulo 3)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Realista	
Avance de trama	Sí	Permite a Guérande seguir investigando.
Reutilización	No	
Referencias en marketing	No	

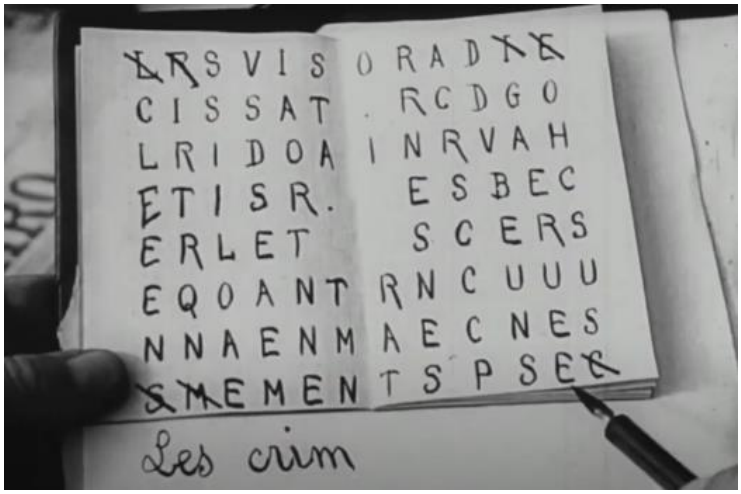


Figura 49: Les vampires – Código de transposición

Concepto 2: Anagrama

Tiempo de representación	35s (1,4%) Duración del capítulo: 41min (capítulo 3) 18s (0,7%) Duración del capítulo: 51min (capítulo 3)	
Definición	Indefinido	
Funcionamiento y uso	Correcto	
Representación gráfica del concepto	Dramatizada	Las letras se reconstruyen para el espectador.
Avance de trama	Sí	Permite a Guérande saber que Irma Vep pertenece a los vampiros.
Reutilización	Sí	
Referencias en marketing	No	

Figura 50: Les vampires - Anagrama

Concepto 3: Código numérico, probablemente un cifrado de sustitución monoalfabético

Tiempo de representación	1 min 20s (3%) Duración del capítulo: 49min (capítulo 9)	
Definición	Indefinido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Neutra	
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

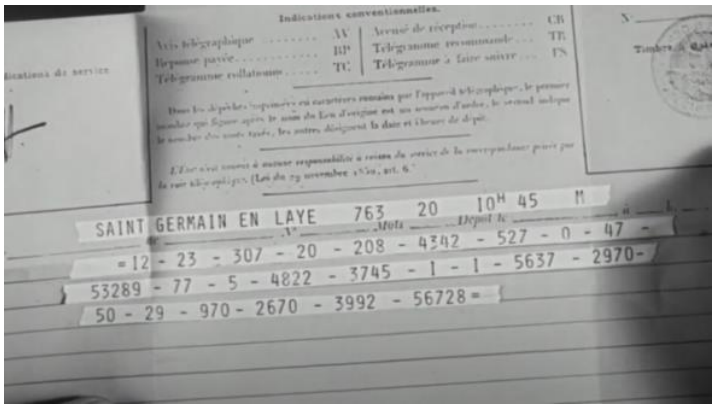


Figura 51: Les vampires – Código numérico

4.33. Manhunter (Hunter)

Duración: 118 minutos
País: Estados Unidos
Género: Thriller
Año: 1986
Director: Michael Mann

Will Graham (William Petersen) regresa como policía persuadido por un compañero. Encargado de la difícil tarea de dar caza a un escurridizo asesino que ataca sólo los días de luna llena, Graham decide emplear métodos poco convencionales. De este modo, recurre al doctor Hannibal Lecter (Brian Cox), otro asesino en serie, para entrar en la mente del asesino. (FILMAFFINITY)

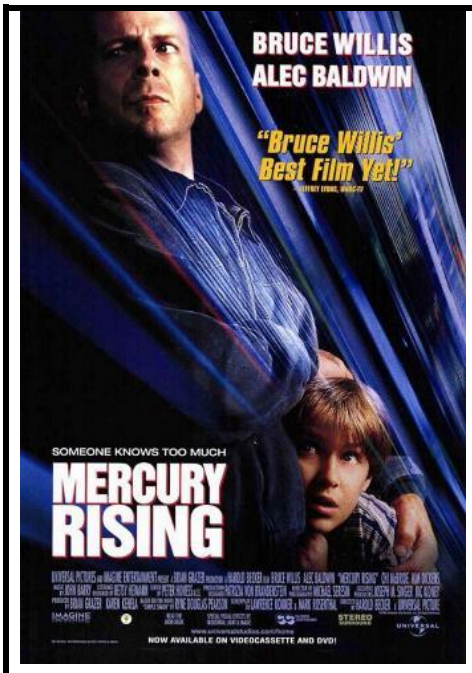
Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
45:05	47:00	Hannibal Lecter se pone en contacto con el asesino y le deja varias referencias a la Biblia: 100 plegarias y después Gálatas 6:11, 15:2, Actos 3:3, Apocalipsis 18:7, Jonás 6:8, Juan 6:22, Lucas 1:7. Buscan en la Biblia, pero no consiguen descifrar el código; debe referirse a otro libro que no conocen.
1:01:30	1:02:05	Encuentran que el código se podía descifrar con las Leyes del Estado de Maryland. El contenido del mensaje es la dirección de Will Graham y la frase "Sálvate y mátalos a todos".

Concepto: Cifrado por libro

Tiempo de representación	2min 30s (2,1%)	
Definición	Parcial	Se define parcialmente en la primera escena.
Funcionamiento y uso	Impreciso	
Representación gráfica del concepto	Dramatizada	Descifrado y búsqueda del libro se mantienen fuera de cámara.
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

4.34. Mercury Rising (Al rojo vivo)



Duración: 112 minutos
País: Estados Unidos
Género: Thriller
Año: 1998
Director: Harold Becker

Art Jeffries es un agente del FBI bastante insolente con sus superiores, razón por la cual le asignan las escuchas telefónicas. Por fin, un día, le encargan la investigación del caso de un niño desaparecido, cuyos padres han sido asesinados. Cuando lo encuentra, resulta ser un autista de nueve años que tiene una prodigiosa capacidad para interpretar códigos del gobierno teóricamente indescifrables. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
16:20	19:10	Simon, un niño autista, encuentra un pasatiempo en una revista que en realidad contiene un mensaje cifrado. Lo descifra con facilidad y llama al número de teléfono que aparece. En la llamada alerta a una oficina del gobierno de que ha sido capaz de descifrar el mensaje.
19:25	19:45	Se habla del código Mercury, un nuevo cifrado para las comunicaciones de Estados Unidos.
24:20	25:20	Se explican las pruebas a las que se ha sometido al Mercury, una de ellas es un mensaje cifrado en una sopa de letras por si alguien lo podía identificar.
1:00:40	1:01:05	El niño vuelve a descifrar el mensaje y vuelve a llamar al mismo número de teléfono.
1:04:05	1:05:15	El agente Jeffries recibe un correo electrónico con un mensaje cifrado. El niño lo descifra simplemente mirando la pantalla.

Concepto: Buscar descifradores usando pasatiempos en prensa y el código indescifrable

A lo largo de la historia se han usado en varias ocasiones pasatiempos en periódicos o revistas con el nivel de complicación suficiente como para encontrar personas que pudieran formar parte de equipos de criptoanálisis. La película lo lleva al terreno de la ficción al convertir a un niño autista en una máquina de leer cifrados, especialmente uno que se presenta como indescifrable.

Tiempo de representación	5min 45s (5%)	
Definición	Parcial	No se hace referencia al hecho del uso pasado de los pasatiempos, pero queda claro que la agencia del gobierno los usa para explorar las posibles debilidades del cifrado.
Funcionamiento y uso	Correcto	El niño descifra el mensaje (no se explica cómo) y llama al teléfono que en realidad es la agencia del gobierno.
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	Es la idea que pone en marcha la trama de la película.
Reutilización	Sí	
Referencias en marketing	Sí	Al ser el argumento principal de la película, aparece en el tráiler https://www.youtube.com/watch?v=Lodj3ZT4tOU

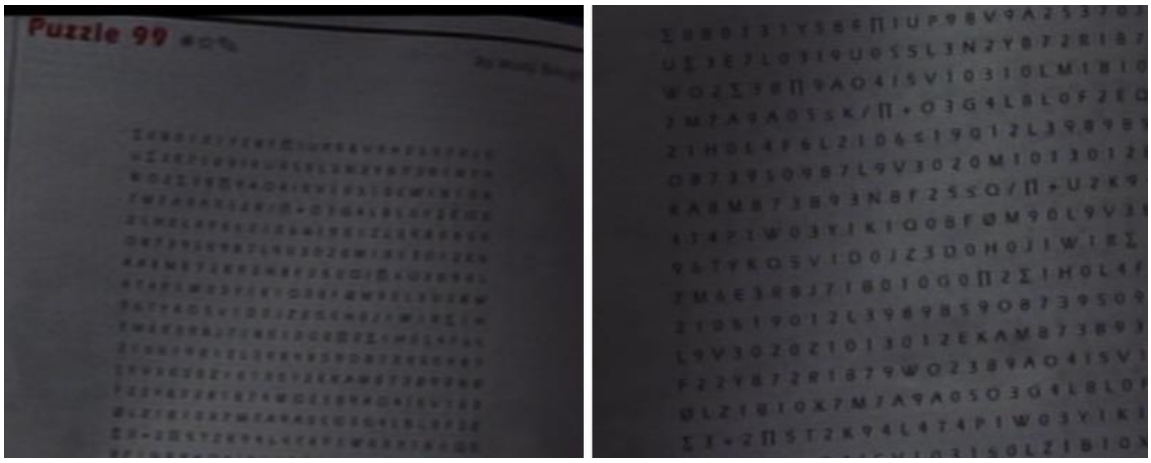


Figura 52: Mercury rising – Pasatiempo con cifrado

4.35. Midway

Duración: 138 minutos
País: Estados Unidos
Género: Bélico
Año: 2019
Director: Roland Emmerich

Año 1942, Segunda Guerra Mundial. Después del devastador ataque sorpresa que destruyó Pearl Harbor, la Armada Imperial Japonesa se prepara para un nuevo ataque. Pero el Almirante Nimitz y Dick Best, el mejor piloto de la armada estadounidense, preparan un contraataque al imponente ejército japonés. Todas las miradas se vuelcan hacia la remota isla de Midway, donde se pondrá a prueba y la fortaleza de ambas naciones. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

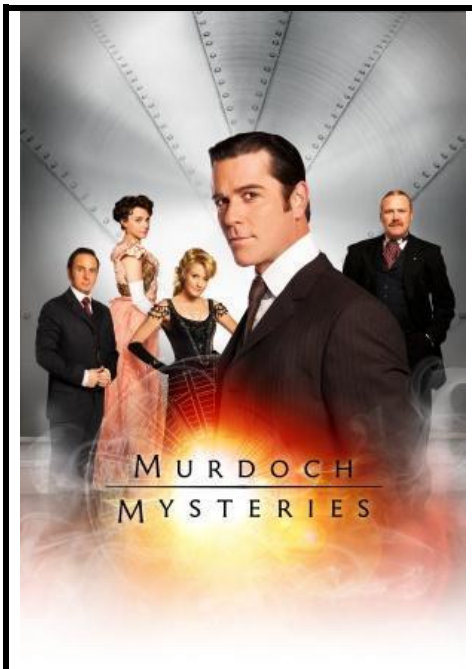
Inicio	Fin	Concepto
55:22	55:32	El almirante Chester Nimitz solicita que se envíe un mensaje cifrado al almirante Halsey para indicarle que el Enterprise se una a Yorktown y al Lexington en el mar del Coral.
55:35	56:05	Layton le explica a Nimitz que un oficial ha interceptado fragmentos de mensajes cifrados que les hace pensar que los japoneses tienen planeado un ataque mayor, pero aún no saben el objetivo
1:02:50	1:04:30	Nimitz y Layton acuden a la estación HYPO para hablar con los criptógrafos. Hablan con Rochefort y les explica cómo interceptan el 60% de los mensajes de radio japones y que han descifrado un 40%. Explica cómo se interpretan de manera diferente los mensajes que se reciben y como los interpretan y analizan ellos para llegar a determinadas conclusiones.
1:05:52	1:06:32	Nimitz le explica a Layton que Washington ha llamado para explicar que se han interceptado mensajes japoneses que indican que al objetivo de su próximo ataque no le queda agua potable. A su vez, Layton le indica que Midway ha enviado un mensaje sin codificar indicando que la depuradora no funciona. Según Layton ese mensaje demuestra que Midway es AF.
1:43:40	1:43:57	Layton le dice a Nimitz que Rochefort ha interceptado una señal japonesa y le dice que no han podido descifrar el mensaje. Le enseña el código a Nimitz y le dice que es del almirante Naguno y que no trasmite desde el Akagi sino desde un crucero.
2:02:26	2:03:26	Se recibe un mensaje en la estación (se ve como mecanografían: AF NO SENRYOU GA …). Se lo entregan a Rochefort y este a Layton, que se lo lleva a Nimitz y le dice que los japoneses se retiran.

Concepto: Captura de mensajes cifrados durante la Segunda Guerra Mundial

Esta nueva versión de “Midway” no se aparta en el uso de la criptografía de la película de 1976. No hay una presentación detallada de elementos criptográficos, pero se refleja la urgencia por descifrar mensajes enemigos y por usar esos mensajes para obtener ventajas tácticas.

Tiempo de representación	3min 17s (2,3%)	
Definición	Definido	Se da una idea clara de la ventaja táctica que supone conocer los cifrados enemigos, especialmente cuando se intenta conocer cuál es el lugar donde los japoneses van a atacar a partir de una suposición.
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	Es una versión de ficción de la captura de mensajes.
Avance de trama	Sí	La trama de la película gira alrededor de la captura de mensajes.
Reutilización	Sí	
Referencias en marketing	Sí	En el tráiler se observa cómo se descifran mensajes y las consecuencias de la batalla táctica. https://www.youtube.com/watch?v=BfTYY_pac8o

4.36. Murdoch Mysteries: The Prince and the Rebel



Duración: 48 minutos
País: Canadá
Género: Thriller
Año: 2008
Director: John L'Ecuyer

Con la visita del nieto de la reina Victoria, el príncipe Alfred, a Toronto, el detective Murdoch y el agente Crabtree quedan a cargo de la seguridad. El Príncipe es un bon vivant al que le gustan especialmente las fiestas y las chicas bonitas, pero su ayudante, David Jennings, es duro y exigente. Cuando la policía encuentra a una chica muerta en el parque, su anillo revela que pudo haber sido miembro de la Hermandad Republicana Irlandesa y, de hecho, puede haber un complot contra el Príncipe. (IMDB)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
19:05	19:40	Encuentran en el estómago de la chica asesinada un papel con unos agujeros recortados en una disposición particular.
19:40	20:05	Murdoch le explica a su superior que se trata de un cifrado y explica el principio de la rejilla y la clave es encontrar el libro o documento donde hay que ponerla para descifrar el mensaje.
26:10	27:22	Encuentra un libro en casa de la chica asesinada que se abre por una página como si hubiese sido forzado. Hay unas letras calcadas, los surcos del lápiz de haber escrito un papel encima, "Sic Semper tirannus" y la rejilla de Cardano permite obtener las letras del mensaje.

Concepto: Rejilla de Cardano

Tiempo de representación	2 min 7s (4,3%)	
Definición	Definido	Se nombra y se explica el concepto.
Funcionamiento y uso	Correcto	Se hace un uso correcto mientras se explica de la rejilla.
Representación gráfica del concepto	Realista	
Avance de trama	Sí	Se descubren los lugares donde se puede producir el atentado.
Reutilización	Sí	

Referencias en marketing	No	

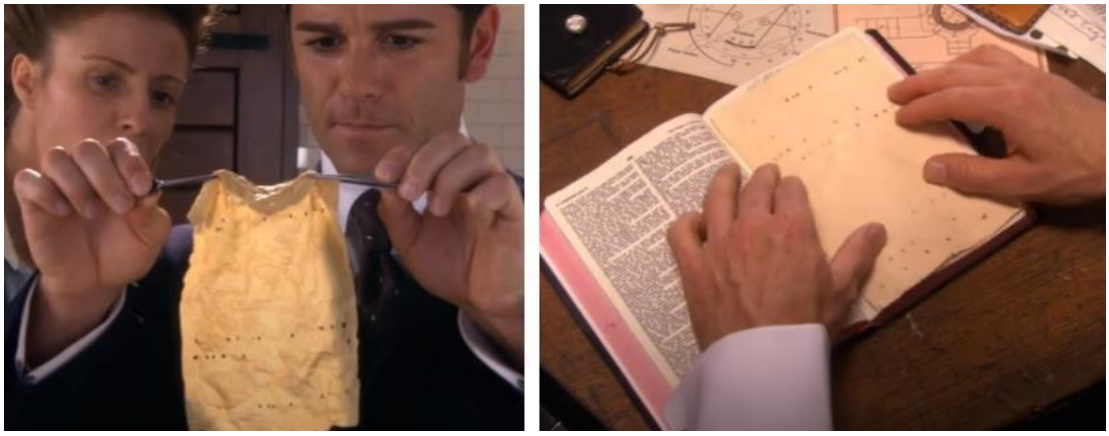


Figura 53: Murdoch Mysteries – Rejilla de Cardano

4.37. Paycheck

Duración: 114 minutos
País: Estados Unidos
Género: Thriller
Año: 2003
Director: John Woo

Michael Jennings es un ingeniero que realiza proyectos para una empresa de alta tecnología. Cada vez que termina un trabajo se lo borran de la memoria para que no pueda divulgarlo. Jennings espera ganar 90 millones de dólares por su último proyecto, en el que ha invertido tres años de trabajo. Sin embargo, en esta ocasión ni siquiera le pagan, aunque vuelven a borrarle la memoria. Con la ayuda de su compañera y amante Rachel, tratará de averiguar qué ha sucedido durante todo ese tiempo del que no recuerda nada. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:22:35	1:24:00	En uno de los sellos del sobre que el protagonista transporta hay un micropunto. Lo lleva a un laboratorio de un instituto y lo mira por el microscopio. En el micropunto hay varias imágenes de periódicos con previsiones sobre el futuro que les ayudan a entender lo que tienen que hacer.

Concepto: Micropunto

El uso del micropunto para ocultar información está mostrado de forma interesante en esta película. Dentro de un contexto de ciencia ficción, el micropunto no se usa para nada sofisticado, simplemente para ocultar unas imágenes que ayudan al protagonista a recordar el reto al que se enfrenta.

Tiempo de representación	1min 25s (1,3%)	
Definición	Indefinido	No se nombra el concepto de micropunto ni se define.
Funcionamiento y uso	Correcto	Se muestra como ampliando un pequeño fragmento de otra imagen aparecen informaciones no reconocibles a simple vista.
Representación gráfica del concepto	Realista	No se buscan formas sofisticadas para revelar la información, simplemente un microscopio electrónico.

Avance de trama	Sí	Es importante para que el protagonista sepa qué es lo que tiene que resolver.
Reutilización	No	
Referencias en marketing	No	

Figura 54: Paycheck - Micropunto

4.38. Rendezvous

Duración: 94 minutos
País: Estados Unidos
Género: Bélico
Año: 1935
Director: William K. Howard, Sam Wood

Bill, un periodista que trabaja en la sección de pasatiempos de un periódico, llega a convertirse en teniente con la idea de participar en el conflicto europeo. Antes de embarcarse entrará en contacto con las altas esferas del departamento de Guerra y conocerá a una atractiva mujer. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
2:10	3:00	Se va a enviar la posición de unos barcos usando un código nuevo. Pero antes se va a hacer una prueba para determinar que el código es seguro.
12:00	16:00	El código es descifrado por los alemanes que no interceptan el barco para hacer creer a los americanos que el código es seguro. Se muestra cómo se revela un mensaje escrito con tinta invisible pero el proceso de descifrado no aparece. El mensaje descifrado llega primero a San Diego y luego a México antes de ser transmitido a Alemania.
23:10	25:00	El protagonista William Gordon es en realidad experto en cifrado y es reclutado para trabajar en el Departamento de Guerra en lugar de irse al frente en Europa.
28:50	32:30	William va a la oficina de código, una oficina donde se envían y reciben diferentes mensajes cifrados. Le piden que analice un mensaje determinando las frecuencias de aparición de las letras. William demuestra sus conocimientos en la disciplina.
35:00	35:50	Con uno de los mensajes recibidos empiezan a hacer pruebas de cifrado por desplazamiento para obtener el texto en claro.
38:10	40:00	Siguen haciendo pruebas de desplazamiento con el mensaje y con un desplazamiento de 5 consiguen descifrar la primera palabra FIRST pero no las siguientes. Gordon sospecha que esa primera palabra es la clave de un cifrado polialfabético. Aplican esa clave a 5 discos de cifrado para poder hacer el descifrado en paralelo, equiparando la A con la F en la primera, la A con la I en la segunda y así sucesivamente. A partir de ahí descifran el mensaje.
40:00	41:40	Con la certeza de que el código no es seguro, el alto mando tiene el dilema de transmitir la posición de los barcos sabiendo que lo van a descifrar. Se proponen encontrar a la persona que robó el libro de códigos.
50:40	52:45	Gordon intercepta una carta con un anuncio que tiene un mensaje oculto con tinta invisible. Encontrar el reactivo no es un proceso obvio. Gordon quiere

		encontrar el reactivo en la espía que ha asesinado al comandante Brennan.
1:15:00	1:16:30	El espía que robó el libro de códigos es descubierto.

Concepto: Primera Guerra Mundial – descifrado de mensajes como ventaja militar

El guion de la película se centra en los esfuerzos del Departamento de Guerra, y en concreto de la oficina de comunicaciones y códigos, una oficina de cifrados, para enviar mensajes sin que sean interceptados y descifrar aquellos que provienen del enemigo. El objetivo principal de los americanos es poder transmitir la posición de encuentro con los británicos y ese es el eje sobre el que gira esta película bélica de espías. Se muestran diferentes escenas en la oficina de cifrado, diferentes ejemplos de tinta invisible y el proceso de descifrado de un mensaje con un cifrado de sustitución polialfabético. Es un proceso simplificado, pero es interesante porque dedica unos cuantos minutos de la película a desgranar la técnica.

Tiempo de representación	17min 15s (18,5%)	
Definición	Definido	El propósito de la oficina de cifrado se explica, al igual que se dan explicaciones generales de procesos de ocultación de la información.
Funcionamiento y uso	Impreciso	No todos los procesos de descifrado se muestran con el mismo detalle. Hay explicaciones detalladas en algunos, aunque con un componente cinematográfico importante.
Representación gráfica del concepto	Neutra	
Avance de trama	Sí	Es el centro de la trama.
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler https://www.youtube.com/watch?v=fnnYFjPzcMc

Figura 55: Rendezvous – Oficina de cifrado y disco de cifrado

4.39. Sebastian

Duración: 100 minutos
País: Reino Unido
Género: Drama
Año: 1968
Director: David Greene

Un matemático británico, que está trabajando en descifrar un código, de forma inesperada se enamora de otra descifradora. Esto lleva a una intriga complicada entre los descifradores de códigos. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
2:30	2:40	El protagonista pide a una chica con la que coincide que deletree su nombre al revés en lugar de dárselo directamente.
4:15	4:55	Se encuentra con la misma mujer y le pide cuantas palabras puede formar a partir de unas cuantas letras. Después de su respuesta, Sebastian le da un número de teléfono y le ofrece un trabajo. Ella le pregunta su nombre, él se lo deletrea.
16:30	18:55	La chica (Rebecca) llega a la oficina acompañada de otras. En el lugar de trabajo sólo hay mujeres. Unas están tecleando unos números en la pantalla y unas letras como equivalente. Sebastian empieza a explicarles a las chicas que el mensaje es importante y que se refiere a un fugitivo. Empieza a comentar que se enfrentan a una mezcla de cifrado de sustitución y transposición. Les da varias instrucciones: haciendo referencia a unas letras t les pide que las alineen en columnas, que hagan un test digrámico (es decir que analicen grupos de letras relacionadas), que busquen grupos que se repiten (Sebastien considera las t parte de un grupo). Las anima a que se pongan con ello. Sebastian es el responsable de esa oficina de cifrado donde sólo trabajan mujeres.
20:30	20:40	Sebastian indica a sus empleadas que los grupos 5 y 10 son dos digramas comunes como base de sus análisis de frecuencias.
20:10	23:20	Sebastien y su equipo trabajan en el descifrado. Se observa cómo se analizan diferentes combinaciones de números, ordenados en columnas, se van buscando patrones de digramas, muchos intentos sin éxito.
23:40	25:25	Sebastien pide al equipo que se concentren en las columnas 4 y 7. Consiguen descifrarlo y arman un gran escándalo, como si fuese una fiesta o una buena noticia. No se da el contenido del mensaje. Una de las chicas le dije a Rebecca: “No los leemos, simplemente los desciframos”.
30:50	33:00	Rebecca sube al despacho de Sebastian con lo que ella define como un código

		indescifrable. Él lo descifra en pocos segundos, dejando a la mujer en ridículo. No hay explicación sobre el código ni sobre el método de descifrado.
54:10	55:50	Sebastian llega con un mensaje a descifrar, en principio debería ser una sustitución simple. El mensaje es descifrado sin dar detalles sobre el método, pero el contenido versa sobre las necesidades de equipo en procesos revolucionarios en América del Sur.
1:14:45	1:21:10	Sebastian recibe el encargo de identificar el código que está insertado en las transmisiones que hace un satélite ruso. En la estación que capta las transmisiones, Sebastian es capaz de identificar los fragmentos que tienen código insertado. Sebastien lleva esos fragmentos a la oficina de cifrado. Reducen la velocidad de esos fragmentos para descubrir un código como Morse que no es Morse y del que las chicas tienen que encontrar los patrones para poder descifrarlo. Se ven varios intentos de descifrado, que no se explican ni quedan nada claros puesto que utilizan gráficos con muy poco significado, sin éxito.
1:36:15	1:39:00	El sonido de un sonajero permite a Sebastian obtener una pista sobre cómo decodificar el mensaje. La película termina sin llegar a una solución.

Concepto: Oficina de cifrado

La película gira alrededor de una oficina de cifrado bastante particular: ambientada en los años 60 en el Reino Unido, Sebastian dirige una oficina en la que todas las empleadas son mujeres relativamente jóvenes. La película es una mezcla de drama, comedia y un punto de thriller, relativamente inclasificable. Le dedica muchos momentos a descifrar códigos, aunque los procesos no están definidos ni se muestran los procesos de descifrado. Además, se muestran esquemas y dibujos complejos, pero con poco significado. Se mencionan cifrados de sustitución, de transposición y se habla de la importancia de descifrar mensajes para obtener ventajas sobre la URSS durante la Guerra Fría. Incluso hay una agente que filtra informaciones al enemigo.

Tiempo de representación	21min 10s (21%)	
Definición	Definido	Se nombra y se describe el propósito de la organización.
Funcionamiento y uso	Impreciso	Se muestra cómo funciona la oficina, pero no cómo se descifran los mensajes. Hay una acumulación de términos sin llegar a profundizar.
Representación gráfica del concepto	Dramatizada	Tanto la concepción como el funcionamiento de la oficina son hijas de un tipo de cine propio de la época.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	

Figura 56: Sebastian – Algunos de los extraños esquemas usados

4.40. Sherlock Holmes The Secret Weapon

Duración: 68 minutos
País: Estados Unidos
Género: Thriller
Año: 1943
Director: Roy William Neill

El detective Sherlock Holmes (Basil Rathbone) y su fiel ayudante el doctor Watson (Nigel Bruce) se enfrentan al colaboracionista nazi Profesor Moriarty. Moriarty tiene entre sus planes secuestrar a un científico británico que ha creado una nueva mira de bombardero para atacar al ejército alemán. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
16:55	17:20	El doctor Tobel escribe un mensaje usando unos dibujos de unos hombres en diferentes posiciones (cifrado extraído del cuento de Conan Doyle “Sherlock Holmes and the Dancing men”).
31:05	32:00	La novia del doctor Tobel entrega la carta con el mensaje cifrado a Holmes. Pero donde se supone que debería estar el mensaje hay otro totalmente distinto porque alguien se ha encargado de manipular el sobre. La mujer explica a Holmes que en el mensaje de Tobel había unos hombres danzantes.
45:30	49:00	Holmes logra recuperar el mensaje a partir de la impresión en la siguiente página del bloc donde fue escrito. Aparecen los hombres danzantes. Watson rápidamente identifica el cifrado por sustitución explicando su funcionamiento y el análisis de frecuencias de forma breve y muy imprecisa (aunque sí que explica que las letras más frecuentes son E, T, A, O, lo que sí es cierto). Pero el mensaje obtenido no tiene ningún sentido. Holmes entonces deduce que los elementos en forma de pirámide encima del mensaje introducen una variación en el cifrado para hacerlo más seguro. En esa pirámide hay 1, 2 y 3 hombres de lo que Holmes deduce que se van saltando letras en ese orden. Es decir, si la primera letra es una “i” en realidad es una “j”, si la segunda es una “y” en realidad es un “a”. Consiguen descifrar así las tres primeras líneas del mensaje, pero la única tiene una variación que por el momento les resulta imposible de romper.
51:30	55:00	Revisando el mensaje, Holmes descubre que la última línea está escrita en espejo y utilizando las mismas reglas que con el resto del mensaje consigue descifrarlo. En paralelo se muestra que Moriarty también lo descifra haciendo la misma deducción.

Conceptos: Cifrado de sustitución monoalfabético (análisis de frecuencias) / Cifrados por desplazamiento / Esteganografía

El cifrado principal de esta película es un cifrado de sustitución monoalfabético utilizando los hombres danzantes de la historia original de Conan Doyle. Se aplican al mensaje cifrado algunas otras variaciones, como un pequeño cifrado por desplazamiento siguiendo el código en la parte superior del mensaje, o cifrar el mensaje en espejo (una forma de desplazamiento). También hay elementos de esteganografía cuando Holmes recupera el mensaje de la hoja del bloc a partir del calco generado por el lápiz, empleando sales fluorescentes y fotografiando con luz ultravioleta.

Tiempo de representación	7min 20s (10,8%)	
Definición	Definido	Se nombra el cifrado de sustitución y se explican sus principios y el análisis de frecuencias brevemente. Se explican de forma breve también los principios de los cifrados por desplazamiento.
Funcionamiento y uso	Impreciso	Se muestra el proceso de descifrado sin detalles.
Representación gráfica del concepto	Neutra	No hay una representación clara de cómo se descifra el mensaje: la explicación es breve y la representación es poco detallada.
Avance de trama	Sí	El mensaje permite a Holmes resolver parte del caso.
Reutilización	Sí	
Referencias en marketing	Sí	El tráiler (https://www.youtube.com/watch?v=qeABjmW3DdM) comienza con la imagen de los hombres danzantes y la siguiente pregunta: “What those dancing men mean?”.

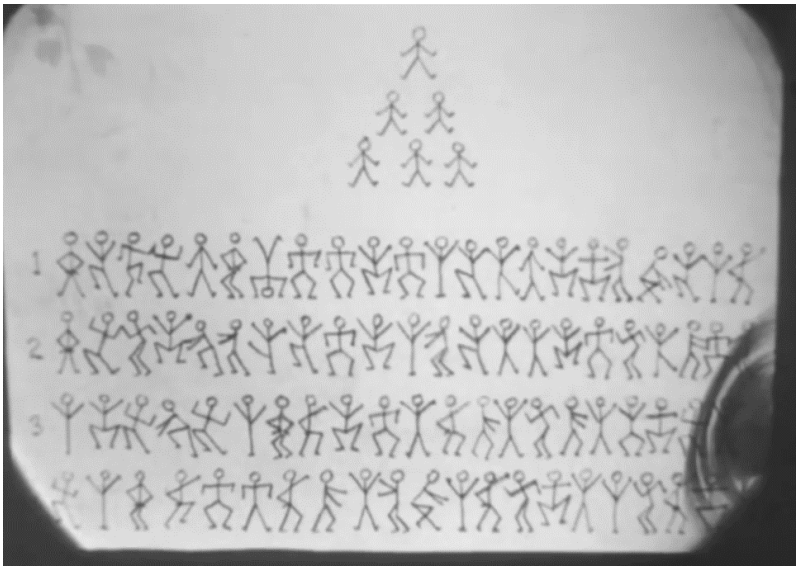
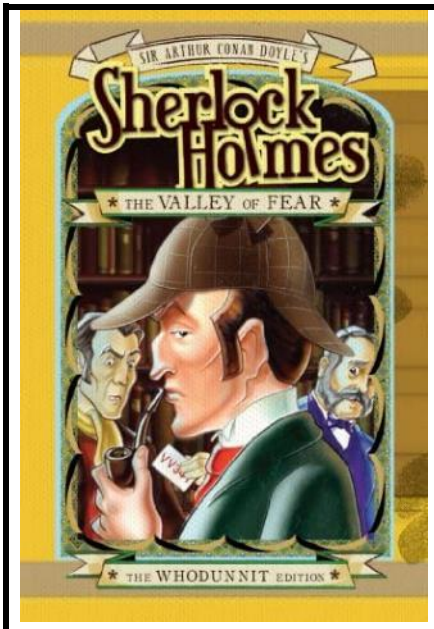


Figura 57: The secret weapon – Cifrado monoalfabético

4.41. Sherlock Holmes and the Valley of Fear



Duración: 50 minutos
País: Australia
Género: Animación
Año: 1983
Director: Norma Green

Basada en la novela de Arthur Conan Doyle, Sherlock Holmes recibe un mensaje que le pone en la pista de un complot contra el señor Douglas, y del que Moriarty podría estar detrás. (WIKIPEDIA)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
0:20	3:30	Sherlock recibe una carta con un listado de números y algunas palabras. Después de revisarla deduce que es un código de libro, aunque no sabe exactamente a qué libro se está refiriendo. Watson le pregunta por qué la persona no ha enviado el libro y Sherlock le explica que un mensaje codificado que contuviera la clave no sería demasiado útil. Sherlock recibe una segunda carta en la que el remitente le informa que no puede enviar la clave.
4:00	7:20	Holmes y Watson empiezan a discutir sobre el mensaje. Sherlock deduce algunos datos del libro, como es largo porque el primer número 534 indicaría la página del libro. El siguiente elemento es C2 que para Sherlock indicaría que el libro tiene dos columnas. Para Sherlock el libro tiene que ser bastante común sino la persona se lo habría enviado. Watson le sugiere que podría ser la Biblia, pero Sherlock le contesta que hay demasiadas ediciones, y que eso dificultaría la decodificación del mensaje. Watson propone el Almanaque Whitaker, por la estructura de un almanaque y lo habitual que es su uso. Empiezan a decodificar el mensaje y tiene sentido, ya que explica que una persona llamada Douglas. Llega un inspector de policía que les informa que John Douglas ha sido asesinado.

Concepto: Cifrado por libro

Esta historia de Holmes incluye un caso muy claro de cifrado por libro, que además lanza la acción de la película. Además, está bien definido durante los primeros minutos de la película, con algunos elementos que permiten a Holmes deducir el tipo de libro, aunque la deducción sea muy rápida.

Tiempo de representación	6min 30s (13%)	
Definición	Definido	Se nombra y se describe el cifrado por libro; lo mismo ocurre con el proceso de descifrado.
Funcionamiento y uso	Impreciso	Se describe el proceso de descifrado y se establece entre los dos protagonistas un proceso de deducción sobre el libro. No se representa el proceso de descifrado detallado.
Representación gráfica del concepto	Dramatizada	No se muestra una versión realista. Se hace una simplificación del descifrado.
Avance de trama	Sí	El mensaje descifrado lanza parte de la trama.
Reutilización	Sí	
Referencias en marketing	No	

Figura 58: Sherlock Holmes and the valley of fear – Cifrado por libro

4.42. Sherlock Holmes: A Game of Shadows (Sherlock Holmes: Juego de sombras)

Duración: 129 minutos
País: Estados Unidos
Género: Thriller
Año: 2011
Director: Guy Ritchie

En todo el mundo se están produciendo llamativas noticias: un escándalo acaba con un potentado del algodón de la India, un comerciante de opio chino fallece de una aparente sobredosis, estallan bombas en Estrasburgo y Viena, ... Nadie ve ninguna conexión entre estos acontecimientos aparentemente aleatorios, excepto el famoso detective Sherlock Holmes, que ha adivinado una red deliberada de muerte y destrucción. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
56:00	00:56:48	Watson envía un telegrama sin sentido a su mujer. El hermano de Holmes le explica que es un menaje cifrado. Es un código que tiene con su hermano. Si la primera letra del mensaje es una consonante el resto de la frase significa justo lo contrario.
35:25	35:40	Holmes ve en la pizarra de Moriarty el triángulo de Pascal escrito con sumas de sus diagonales. También ve el título de un libro sobre horticultura y una planta muerta.
1:47:50	1:48:54	Holmes le dice a Moriarty que al robarle la libreta sabía que estaba codificada. Deduce que el código se encuentra en el libro "El arte de la horticultura doméstica" porque cuando estuvo en su casa vio el libro, pero se dio cuenta que no cuidaba sus plantas. Se ve como la mujer de Watson tiene el libro con el mensaje resuelto.

Concepto: Cifrado por libro

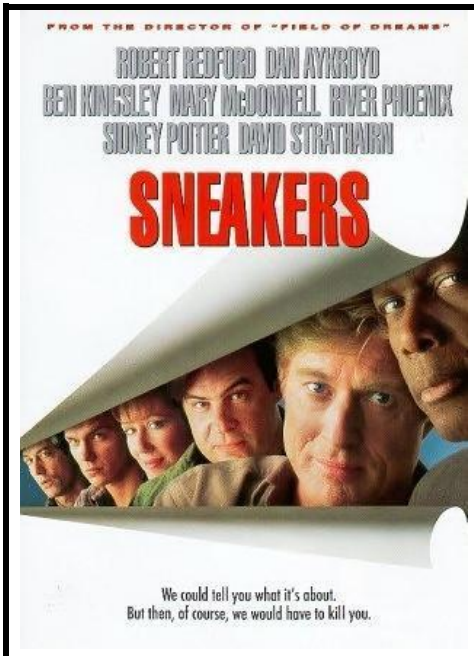
Estamos frente a un caso interesante de cifrado por libro complejo que no llegó en pantalla. "Aventuras matemáticas en el cine" **(Sorando, 2015)** da una extensa explicación sobre el uso del triángulo de Pascal para cifrar la secuencia página-línea-letra correspondiente. Para ello usaba las sumas de las diagonales del triángulo siguiendo una clave pública que Moriarty daba en sus conferencias, en una versión particular de la idea de clave pública y clave privada. Todo esto quedó fuera del montaje final salvo la breve imagen que se presenta complementando la tabla. La

explicación es larga y seguramente no encajaba demasiado en el clímax final de la película.

Tiempo de representación	1min 19s (0,9%)	
Definición	Parcial	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	Se consigue incautar la fortuna de Moriarty.
Reutilización	No	
Referencias en marketing	No	

Figura 59: Sherlock Holmes: A game of shadows – Cifrado por libro

4.43. Sneakers (Los fisgones)



Duración: 126 minutos
País: Estados Unidos
Género: Thriller
Año: 1992
Director: Phil Alden Robinson

Martin Bishop es el líder de un grupo especializado en el mantenimiento de los sistemas de seguridad de grandes empresas. Un día se ve obligado a trabajar para una agencia secreta que le encarga el robo de una caja negra. Pronto averigua que esa caja tiene la capacidad de decodificar cualquier sistema de encriptación y que la agencia que lo ha contratado no es estatal. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
12:55	13:20	Aparecen miembros de la NSA que detallan su función como los que "decodifican los códigos ajenos".
14:40	15:35	La NSA está siguiendo a un matemático especializado en criptografía que recibe dinero de Rusia. El matemático está desarrollando una "caja negra" cuya función no se conoce. La NSA pide al equipo liderado por Martin Bishop hacerlo.
20:40	21:50	Van a la conferencia del matemático que habla de métodos matemáticos para factorizar números grandes y la posible construcción de un decodificador universal.
31:00	31:25	En la oficina del matemático, Martin Bishop encuentra la máquina.
38:00	44:30	Mientras están analizando la máquina, el nombre de la compañía SETEC ASTRONOMY es un anagrama de TOO MANY SECRETS (lo descubren utilizando letras de Scrabble). Siguen investigando la máquina y descubre que es un decodificador, la máquina que lo descifra todo y permite desencriptar cifrados RSA permitiéndoles el acceso a los sistemas de la Reserva Federal o el sistema de control de tráfico aéreo.

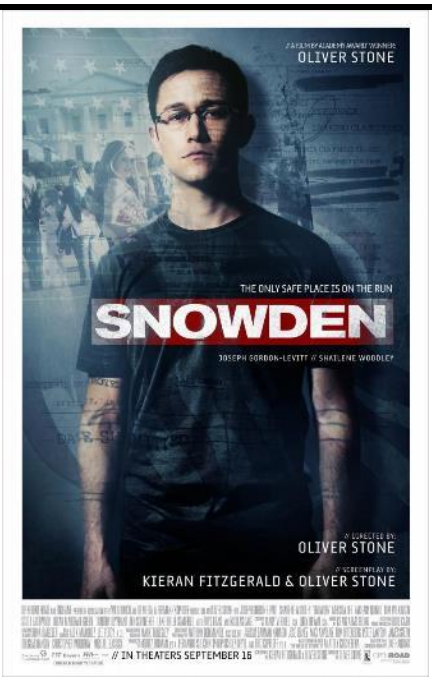
Concepto: La máquina de descifrado universal – cifrado RSA

"Sneakers" se tomó desde el principio su premisa en serio. Iba a hablar de criptografía y para ello contrató como consultor a Leonard Adelman, la A detrás de RSA, para aportar credibilidad a la conferencia del matemático o discutir sobre su algoritmo. La película no deja de ser ficción y los momentos de la charla son breves y no directamente comprensibles si uno no empieza a analizar y buscar información sobre cómo se construyó su discurso. De la misma manera, el decodificador universal es un

dispositivo inexistente pero que permite explorar la idea de que los algoritmos de cifrado moderno se basan en problemas irresolubles (en la práctica y con el poder de computación actual). La película también tiene sus buenas dosis de técnicas de infiltración y de ingeniería social realistas como cuando graban la voz del empleado que les permite tener acceso a las instalaciones del villano.

Tiempo de representación	9min 25s (7,5%)	
Definición	Definido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	La máquina no existe, así que es todo producto de la puesta en escena cinematográfica.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	En el tráiler (https://www.youtube.com/watch?v=8X_yiqK_sUs) y en la sinopsis.

4.44. Snowden



Duración: 134 minutos
País: Estados Unidos
Género: Drama
Año: 2016
Director: Oliver Stone

Narra los acontecimientos que siguieron a la publicación por parte del diario 'The Guardian' de los documentos clasificados que aportó el joven analista de la Agencia de Seguridad Nacional (NSA) Edward Snowden sobre el programa secreto de vigilancia mundial de la Agencia en el 2013, unos documentos que revelaban que espiaban a miles de millones de personas de todo el planeta. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
11:14	12:22	Snowden llega al centro de entrenamiento de la CIA. Entra en una habitación y se encuentra a un hombre que le indica dónde ir. Snowden se interesa por la máquina en la que está trabajando y le pregunta si es una Enigma. El hombre le dice que es una Sigaba, “la mejor máquina de cifrado de la guerra fría”. Snowden le dice que siempre ha querido aprender criptografía y pregunta por otra de las máquinas. El hombre le explica que es la Hot Line, la primera conexión directa entre Washington y Moscú. Se presentan y Snowden se interesa en otra de las máquinas preguntando si es una Cray 1. Hank Forrester le explica que es el primer superordenador.
21:50	23:15	Forrester le explica a Snowden que cuando trabajó en NSA creó un programa que diferenciaba lo extranjero y lo nacional y que encriptaba el resto de señales que no se estuvieran analizando para que siguiesen siendo privadas. Cuenta que no lo usaron, pero que luego utilizaron otro programa basado en el suyo, pero que no tenía filtros o automatizaciones, que analizaba toda la información.
33:53	35:20	Snowden ve como Gabriel Sol utiliza el programa XKeyscore para localizar amenazas a Bush desde el 3 de febrero y le explica cómo recopila la información. La información se recoge de todo el mundo tanto pública como privada desde emails a chats o SMS (Upstream, Muscular, Tempora, Prism).
38:40	39:33	Gabriel está investigando a Marwan Al-kirmani, un banquero del que quiere tener información Snowden. Buscan alguna debilidad e investigan a su cuñada. Snowden se sorprende porque Gabriel accede en directo a la cámara y micro del ordenador utilizando un programa, Optic Nerve.
39:58	41:42	Snowden no está cómodo con espiar a la cuñada. Le pide investigar el Facebook de la hija. Utilizan el programa XKeyscore. Snowden le pregunta si

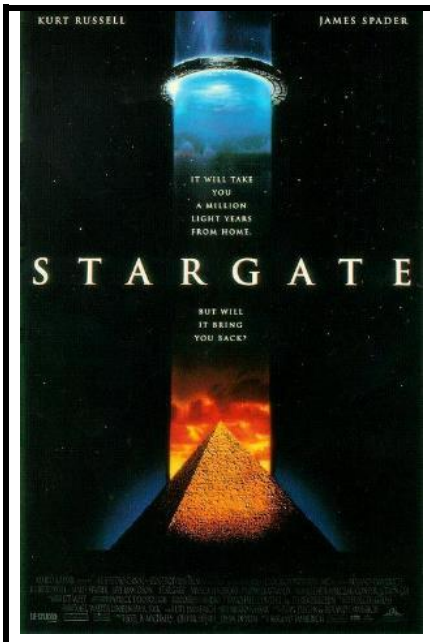
		no hace falta una orden judicial y si sería necesaria en objetivos estadounidenses. Descubren información del novio y la madre de la hija a partir de redes sociales como Facebook.
56:00	58:30	Snowden le explica a la periodista todo lo que hizo en Japón: crear un sistema de backup, espiar a la población japonesa, atacar a infraestructuras. También habla de implantar malware en México, Alemania, Brasil, Venezuela, Austria. De la misma manera vigilar a líderes mundiales.
59:20	1:01:10	Snowden explica que en vigilancia antiterrorista hacia búsquedas en SIGINT. Explica que no solo sigue la información esa persona sino la de todos los números de teléfono con los que están en contacto. Explica la red de conexiones acaba siendo muy extensa y que la información de cualquiera puede ser observada.
1:24:09	1:25:00	Snowden propone la creación de una base de datos centralizada, Heartbeart.
1:28:52	1:29:52	Snowden les muestra a unos compañeros los datos que ha encontrado mientras desarrolla el programa Heartbeat sobre la recolección de datos del mes de marzo del mundo entero de emails y llamadas por Skype. Les enseña que el país sobre el que se recolectan más datos es Estados Unidos.

Concepto: Cifrado versus Privacidad

Me alejo ligeramente del tema del trabajo con esta propuesta. Snowden es un personaje muy conocido y este biopic lleva al cine su vida y sobre todo el proceso de revelación de las estrategias de vigilancia de la NSA. No creo que sea casualidad que la película empiece hablando de una máquina de cifrado y de la Hot Line entre Washington y Moscú, elementos de protección de la información y por tanto que garantizan la privacidad. A partir de ahí se suceden múltiples escenas que hablan de la tecnología empleada para recopilar datos, públicos y privados, de objetivos militares y de población en general, muchos de ellos protegidos por la ley y supuestamente encriptados. No hay en esta película referencias a métodos de cifrado pero el fondo de la cuestión está ahí y entronca con la criptografía moderna y la sensación de protección que subjetivamente puede generar. Desde un punto de vista didáctico, un objetivo que persigue en parte este trabajo, es un tema de actualidad y creo que necesario.

Tiempo de representación	12min 48s (9,5%)	
Definición	Definido	
Funcionamiento y uso	Impreciso	No se muestran detalles del funcionamiento.
Representación gráfica del concepto	Neutra	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler https://www.youtube.com/watch?v=QlSAiI3xMh4) y en la sinopsis.

4.45. Stargate (Stargate, puerta a las estrellas)



Duración: 121 minutos
País: Estados Unidos
Género: Ciencia ficción
Año: 1994
Director: Roland Emmerich

Un coronel y un científico, movidos por distintos intereses, investigan el misterioso hallazgo en unas excavaciones de un extraño artefacto al que llaman "Puerta de las Estrellas". Acompañados de un equipo de reconocimiento, atraviesan la Puerta y son transportados a un lejano planeta. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
3:20	5:10	Meseta de Guiza, 1928. Se ve como muestran un hallazgo arqueológico al Dr. Langford y su nieta Catherine Langford. Son unas piedras cubiertas de símbolos jeroglíficos y un aro gigante con símbolos.
11:30	13:25	El Dr. Jackson acude a unas instalaciones militares. Allí le muestran unas estructuras de piedra cubiertas de jeroglíficos. Son las mismas que las de la primera escena. El Dr. Gary Meyers le explica que se pueden ver dos líneas de jeroglíficos y que hay una que no es conocida. El Dr. Jackson le dice que no son jeroglíficos, que quizá sea escritura hierática o cuneiforme. Jackson se pone a corregir una traducción de una pizarra. Entre otras palabras traduce “Stargate”.
14:45	15:05	Se escucha una grabación de Jackson diciendo que no es capaz de descifrar los símbolos de la figura oval y que no existen similitudes con escrituras conocidas.
16:55	19:00	El Dr. Jackson les explica a los militares sus hallazgos. Les dice que esos símbolos que pensaban que eran palabras en realidad representan constelaciones estelares y que están colocadas formando un mapa o señalando una dirección. Cree que los siete puntos podrían definir unas coordenadas. Explica cómo interpretar los puntos para determinar la localización.
19:35	23:00	La Dra. Langford le muestran al Dr. Jackson otro hallazgo que tenían escondido (un aro gigante), también cubierto de símbolos (el mismo que aparecía en la primera escena). Ese aro tiene diferentes grabados en la parte central de la circunferencia y se ve como esa parte gira. La tienen monitorizada y le muestran los diferentes símbolos a Jackson en una pantalla. Este detiene el vídeo cuando aparece en la imagen un símbolo que él había descrito y ellos no habían sabido interpretar. Gracias a eso programan una secuencia de combinación de siete símbolos girando el aro central y posicionando cada símbolo en un lugar concreto de la estructura. Al finalizar la secuencia se abre una especie de portal en el centro del aro.

34:05	35:15	Una vez atravesado el portal y ver que este se encuentra en el interior de una especie de pirámide, el coronel O'Neill le pide a Jackson que trabaje en la interpretación de la puerta rápidamente para poder volver. Jackson le dice que no puede porque necesita investigar si existen otras construcciones o huellas de civilización para poder encontrar el código de alineación de la puerta.
1:03:30	1:04:30	Una de las personas del "otro lado" muestra a Jackson el interior de un edificio donde hay muchos grabados jeroglíficos. Ella pronuncia (lee) alguno de los símbolos y él intenta aprender por imitación.

Concepto: Jeroglíficos

Aunque no podemos considerarlos parte de la criptografía, por el hecho de que no se crearon para ocultar mensajes en origen, el hecho de que desde un punto de vista actual nos resulten desconocidos implica un estudio muy similar al necesario para descifrar mensajes. Resulta, por tanto, una disciplina interesante puesto que permite reflejar en el cine muchos de los desafíos a los que se enfrentan los criptoanalistas y esta película, en el contexto de la ciencia ficción, refleja esos desafíos: la apertura del portal, el retorno…

Tiempo de representación	11min 45s (9,75%)	
Definición	Definido	
Funcionamiento y uso	Impreciso	Se muestran algunos momentos en los que se leen jeroglíficos o se utilizan en la trama sin detallar el proceso.
Representación gráfica del concepto	Neutra	El uso de los jeroglíficos se realiza en el contexto de la trama de ciencia ficción, sin la precisión que representaría una lectura real.
Avance de trama	Sí	Es un elemento principal para desarrollar la trama.
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler: https://www.youtube.com/watch?v=DPnWKHkziak

Figura 60: Stargate – Jeroglíficos

4.46. Summer Wars

Duración: 114 minutos
País: Japón
Género: Animación
Año: 2009
Director: Mamoru Hosoda

Conectándose a través de un ordenador, una televisión o un teléfono, millones de personas se introducen en el mundo virtual OZ y adoptan la forma de avatares. Kenji es un estudiante superdotado en matemáticas que trabaja como técnico de mantenimiento de OZ. Natsuki, la chica de sus sueños, le invita a pasar el verano junto a su familia en Nagano. Pero cuando un virus ataca OZ desencadenando una catástrofe, Kenji y todo el clan inician una verdadera cruzada familiar para salvar al mundo virtual. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
23:15	24:35	Kenji recibe un mensaje con una serie muy larga de números y el título "Resuélveme". Kenji se pasa toda la noche intentando descifrar los números y al final consigue llegar a una solución que envía de vuelta. No se observa el proceso. El único mensaje que se observa como solución es "The magic words are squeamish ossifrage".
25:25	29:00	A la mañana siguiente, Kenji aparece en la televisión como el responsable de un ataque a OZ. Kenji no tiene acceso al sistema y su amigo Takashi le explica que la noche anterior un correo electrónico con un código llegó por correo a un gran número de gente con el título "Resuélveme". Kenji le explica que fue él quien lo resolvió.
42:45	49:05	Se explica que el hacker (una inteligencia artificial llamada Love Machine) está robando cuentas dentro de OZ, pero dado que este mundo virtual se ha convertido en un reflejo del real donde todas las empresas y servicios públicos tienen su equivalente, las cuentas de personas tienen privilegios de acceso a sistemas de control.
45:30	47:05	Kenji intenta acceder al sistema central repitiendo el proceso de desencriptar una clave con papel y lápiz. En el proceso se dan cuenta de que no fue el único que consiguió desencriptar el código enviado por la IA.
1:42:10	1:44:30	Para salvar a la familia de la caída de un satélite que la IA ha programado, Kenji debe descifrar varios códigos cifrados. Primero lo hace con papel y lápiz y finalmente es capaz de hacerlo de memoria.

Concepto: RSA – desencriptado de clave de acceso

No es la primera película en la que Mamoru Hosoda trata el tema de los mundos virtuales, los metaversos y las inteligencias artificiales. Es un creador de anime conectado con la actualidad y preocupado por cómo la tecnología puede afectar al mundo real y a la tradición, tan importante en Japón. Es, por tanto, un tipo de cine que conecta con muchos tipos de público y en particular con un público joven y que puede servir de origen de múltiples debates: desde el tiempo que pasamos en mundos virtuales hasta la privacidad y seguridad de nuestras comunicaciones. En cuanto a la criptografía, la película parte de una premisa irrealizable tal y como se plantea. El protagonista y otras personas reciben un número que desencriptado permite el acceso con privilegios al sistema OZ. Kenji lo descifra con papel y lápiz, lo que es imposible pues haría falta potencia computacional. La película hace referencia en su resolución a "The magic words are squeamish ossifrage", la solución a un reto de factorización que los creadores de RSA propusieron en 1977[9].

Tiempo de representación	15min 10s (13,2%)	
Definición	Indefinido	No se explica cómo funciona el encriptado.
Funcionamiento y uso	Impreciso	Se muestra el descifrado los accesos de forma gráfica sin precisar en los detalles.
Representación gráfica del concepto	Dramatizada	La película utiliza todos los recursos de animación a su disposición para dar una visión comprensible de algoritmos de difícil representación.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	No	

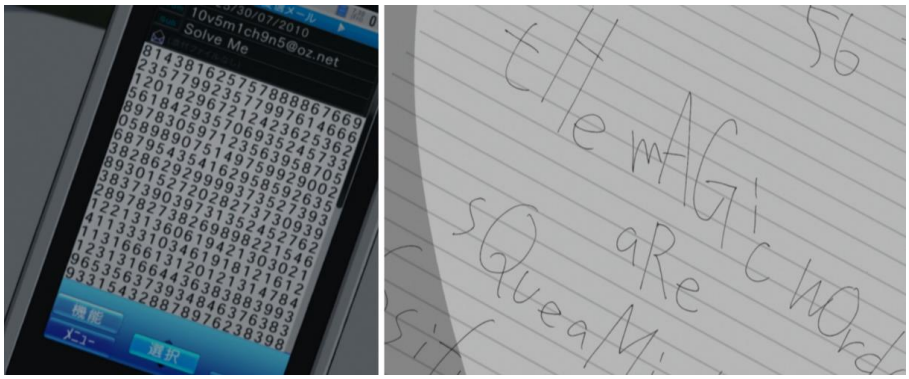
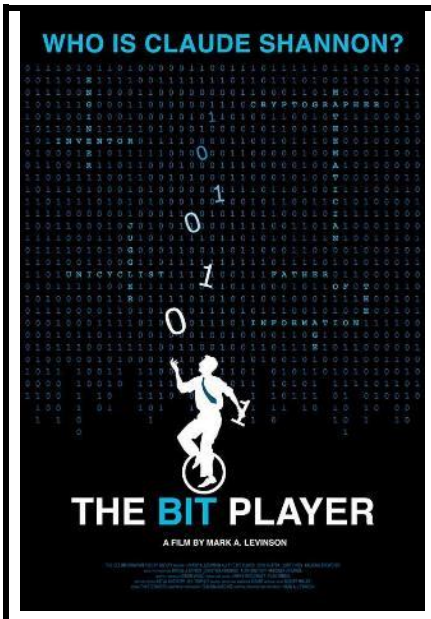


Figura 61: Summer Wars – Mensaje y descifrado

[9] Atkins, D., Graff, M. y Lenstra A. K. (1994). *The magic words are squeamish ossifrage*. Advances in Cryptology - ASIACRYPT '94, 4th International Conference on the Theory and Applications of Cryptology, Wollongong, Australia, November 28 - December 1, 1994

4.47. The Bit Player



Duración: 90 minutos
País: Estados Unidos
Género: Documental
Año: 2018
Director: Mark Levinson

The Bit Player cuenta la historia de un genio pasado por alto, Claude Shannon (el "Padre de la teoría de la información"), que revolucionó el mundo, pero nunca perdió su curiosidad infantil. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
5:45	7:30	Mediante una secuencia animada se explican los principios de la teoría de la comunicación de Shannon.
11:00	12:15	El documental explica que de pequeño a Shannon le gustaban los códigos. Lo relaciona con Poe que tenía la misma afición y habla de “The Gold-Bug” y el pergamino con el mensaje en tinta invisible. Comenta a continuación como Poe explica el análisis de frecuencias para descifrar el mensaje. Sigue conectando esta idea de búsqueda de patrones con el trabajo de Alan Turing durante la Segunda Guerra Mundial para romper la Enigma. Eso lleva a Shannon a pensar que la clave está en encontrar patrones.
31:25	32:15	Entra a trabajar en los laboratorios Bell y pide participar en los grupos de trabajo relacionados con la criptografía, que estaban buscando una manera segura de cifrar las comunicaciones entre Roosevelt y Churchill. Pero Shannon se interesó también por la parte más teórica de esas comunicaciones: ¿Cuántos mensajes se debían interceptar para poder encontrar una solución a un cifrado? ¿Se podía crear un código indescifrable?
35:30	38:45	Shannon trabaja en su teoría de la comunicación durante diez años en paralelo a todo su trabajo en criptografía. Shannon quería encontrar una manera de medir la información como algo físico, que se pudiera medir. De ahí empieza a relacionar la información con la resolución de la incertidumbre. Y de esa idea de convertir la información en algo medible deriva la idea de convertir la información, cualquier tipo de información, en bits. El problema se reduce a dos preguntas: ¿Cómo convertir la información en ceros y unos? ¿Cómo asegurarse que esos ceros y unos se transmitan a través del canal con precisión?
40:00	42:10	Shannon parte de la idea de la redundancia (estudiando la redundancia en la lengua inglesa) para determinar su siguiente avance: comprimir la información, eliminar la redundancia y sólo enviar lo que no se puede predecir. Descubrió que

		hay un tamaño mínimo al que se puede reducir la información y no perder nada esencial. Shannon mostró como calcularlo de una manera que tiene que ver con las probabilidades dentro del mensaje y toma una forma similar al cálculo físico de la entropía. Shannon deriva de ahí el concepto de entropía de la información, siendo ésta el mínimo de tamaño de compresión de la información.
43:20	44:15	Shannon se concentró también en el canal y en el ruido que podía aportar. Y Shannon se preguntó si podía calcular la máxima velocidad a la que se podía transmitir la información a través de un canal. Y también que se podrían encontrar códigos que permitirían transformar la información de manera que se pudiera llegar a esa velocidad máxima.
47:05	47:35	Shannon publica en 1948 su artículo “A mathematical theory of communications”.

Concepto: Claude Shannon

Este documental con reconstrucciones dramatizadas es un interesante repaso a la vida de Shannon y a sus conceptos principales sobre comunicación y algunas ideas sobre criptografía. He seleccionado de todo el metraje los elementos más relevantes con el tema, pero hay otras partes que lo tocan tangencialmente o que suponen desarrollos a partir de las ideas iniciales.

Tiempo de representación	11min 40s (12,9%)	
Definición	Definido	Se explican de forma detallada las teorías de Shannon.
Funcionamiento y uso	Correcto	Se muestran los procesos resumidos de cómo Shannon llegó a sus ideas.
Representación gráfica del concepto	Realista	Se usan imágenes reales con reconstrucciones gráficas detalladas.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler: https://www.youtube.com/watch?v=QizwJLoIkuo

4.48. The Imitation Game (Descifrando Enigma)

Duración: 114 minutos
País: Reino Unido
Género: Drama
Año: 2015
Director: Morten Tyldum

Biopic sobre el matemático británico Alan Turing, famoso por haber descifrado los códigos secretos nazis contenidos en la máquina Enigma, lo cual determinó el devenir de la II Guerra Mundial (1939-1945) en favor de los Aliados. Lejos de ser admirado como un héroe, Turing fue acusado y juzgado por su condición de homosexual en 1952. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
7:40	7:50	Turing llega a Bletchley cuyo cartel principal es Bletchley Radio Manufacturing
10:50	13:40	Turing discute con el comandante Denniston sobre el proyecto secreto de Bletchley: el análisis y descifrado de la máquina Enigma. El comandante lo lleva a una sala donde tienen una Enigma junto a otros matemáticos y criptoanalistas. Es una máquina interceptada por Polonia con 5 rotores y dos cables en el panel de conexión. Se deja claro que los mensajes alemanes son indescifrables y que solo tener la máquina no es la solución, porque no se conoce la configuración de la máquina.
18:30	18:45	Mientras el resto del equipo intenta descifrar algunos mensajes utilizando análisis de frecuencias para encontrar patrones, Alan afirma que está construyendo una máquina que podrá descifrar cualquiera de los mensajes.
19:00	20:10	Alan trabaja construyendo esquemas de la máquina, a partir del funcionamiento de las conexiones y los rotores.
26:40	27:00	Turing propone utilizar un crucigrama muy complejo para obtener personal para Bletchley.
38:35	39:00	Después de superar una prueba, Joan Clarke es contratada en Bletchley.
44:00	45:10	Joan y Alan hablan sobre el artículo de Turing que hablaba sobre la máquina reprogramable.
51:30	53:00	Hacen una primera prueba con la máquina de Turing que debería descifrar la configuración del día, sin éxito.
1:14:30	1:17:45	Alan se plantea que la máquina busque configuraciones a partir de mensajes predecibles. Cada día los alemanes envían un informe sobre el tiempo y hay palabras que se repiten. La máquina consigue replicar la configuración. La prueban con la Enigma.

Concepto: Descifrado de la Enigma - Alan Turing

La película simplifica y transforma muchos hechos de la vida de Turing. Hay que celebrar que una producción importante se centre en la vida de una figura con tanta relevancia, pero Bletchley Park descifró más códigos alemanes además de la Enigma y se construyeron más de doscientas máquinas para descifrar (British Bombes). Aspectos de la vida de Turing se tratan también con incorrecciones como la extensión de la relación con Joan Clarke, la investigación en 1950 acusándole de espía o los detalles de su muerte. Licencias aparte, esta película es un buen elemento didáctico para explicar los aspectos reales de la vida de Alan Turing, la carrera por descifrar la Enigma o el trabajo en Bletchley Park.

Tiempo de representación	11min 15s (9,8%) – he considerado las escenas más relevantes ya que toda la película es un biopic de Turing.	
Definición	Definido	
Funcionamiento y uso	Correcto	Sin muchos detalles se muestra el funcionamiento de la Enigma.
Representación gráfica del concepto	Dramatizada	Hay grandes diferencias entre la realidad y el guion de la película.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler (https://www.youtube.com/watch?v=j2jRs4EAvWM) y en la sinopsis.

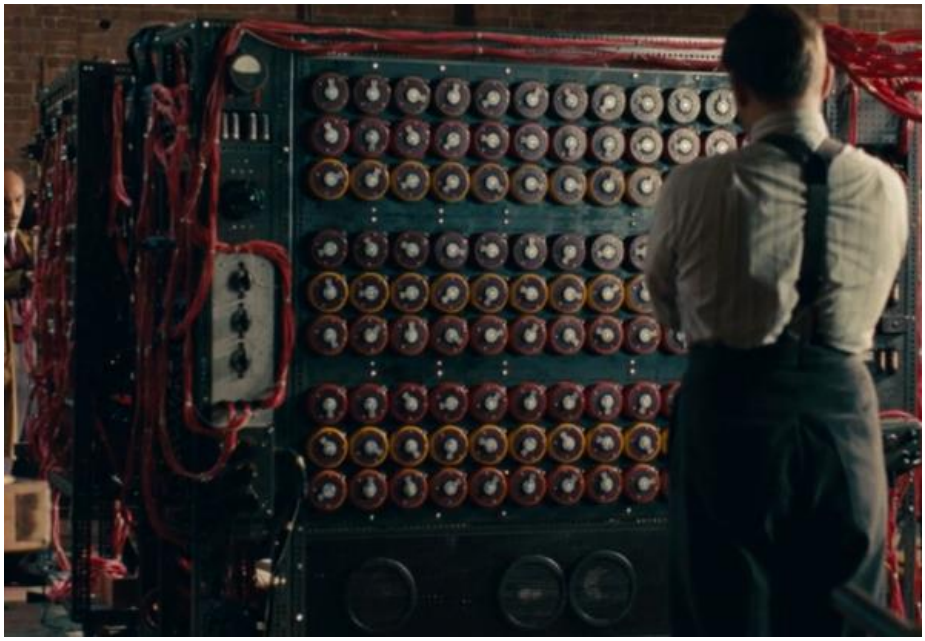


Figura 62: The imitation game – Máquina de Turing

4.49. Feng sheng. The Message

Duración: 117 minutos
País: China
Género: Thriller
Año: 2009
Director: Chen Kuo-fu, Gao Qunshu

En 1942 tras una serie de intentos de asesinato contra funcionarios del gobierno japonés, el jefe de inteligencia de Japon reúne a un grupo de sospechosos en una mansión para ser interrogados. Ahi comienza un juego tenso del "gato y el ratón". (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
19:30	21:20	Un grupo de personas que trabaja en la parte china afín a la fuerza invasora japonesa durante la Segunda Guerra Mundial es reunido para descifrar un mensaje cifrado, necesario para evitar el asesinato de funcionarios del gobierno japonés (aunque esto es realmente una excusa para encontrar al espía traidor). El mensaje son una serie de números y es presentado como una lotería: 3 6 4 4 5 6 0 2…. La única experta del grupo, Li, explica que en total el mensaje codifica 18 caracteres pero que sin el libro de códigos no van a poder descifrarlos.
22:00	23:50	Un alto oficial japonés llega con el libro de claves. Con él empiezan a descifrar. Se explica que el chino para transmitirlo en Morse se codifica con 4 números. En el mensaje hay 72 dígitos, por tanto 18 caracteres como había mencionado Li. El problema es que los números están mezclados o cifrados y no se pueden buscar los caracteres tal y como aparecen en el mensaje. Li consigue obtener los caracteres y los reordena para obtener el mensaje. No está clara la explicación del reordenamiento de caracteres.

Concepto: El uso del chino en Morse y el cifrado

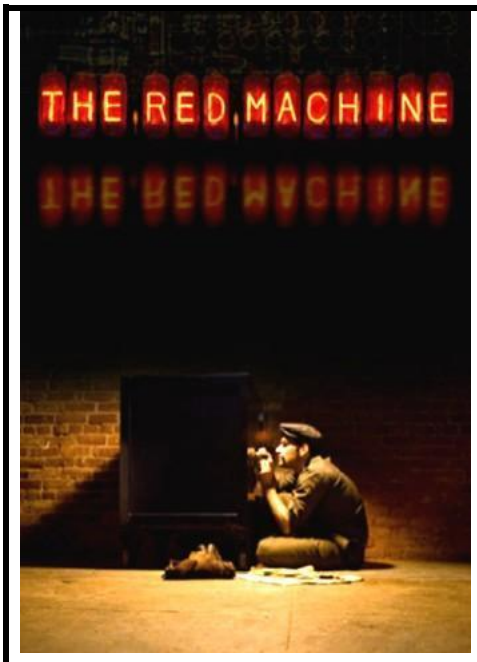
El punto de arranque del argumento central de esta película es un cifrado. No está explicado ni tenemos constancia por las imágenes de qué tipo de cifrado tenemos delante. Sin embargo, hay dos elementos interesantes: el primero, es cómo se usa la lengua china con código Morse y es que cada carácter se codifica con cuatro números; el segundo, es que además esos números se han reordenado para complicar el descifrado. Los personajes necesitan el libro de códigos para ver esa relación entre carácter y números, que en el caso particular de la película no se trata de ningún

estándar. Por otro lado, esos caracteres están reordenados a priori antes de la codificación en morse ya que en un momento del descifrado Li nombra seguidos los números 781 que formarían parte de un carácter que se puede ver en una de las fotos inferiores. He intentado recuperar partes del mensaje, pero se enseña muy poco en la escena y me ha sido imposible recuperar un fragmento de los caracteres chinos relevante. Resulta por tanto inconfirmable el tipo de cifrado usado, pero en este caso podemos considerar la forma en la que se codifica el Morse como un cifrado de sustitución.

Tiempo de representación	2min 40s (2,2%)	
Definición	Definido	Se explica cómo se codifican los caracteres en Morse y la necesidad de un libro de códigos.
Funcionamiento y uso	Impreciso	Se muestra de forma superficial el proceso de descifrado.
Representación gráfica del concepto	Neutra	
Avance de trama	Sí	Es el punto de giro que la historia necesita para llegar a la siguiente parte de la trama.
Reutilización	No	
Referencias en marketing	Sí	Aparece en el tráiler (https://www.dailymotion.com/video/x24cbob) y en la sinopsis.

Figura 63: The message – Código Morse y cifrado de sustitución

4.50. The Red Machine



Duración: 84 minutos
País: Estados Unidos
Género: Bélico
Año: 2009
Director: Stephanie Argy, Alec Boehm

Washington, DC, 1935: En el punto álgido de la Gran Depresión, un joven ladrón se ve obligado a ayudar a un espía de la Marina de los Estados Unidos a robar un nuevo dispositivo que el ejército japonés está usando para codificar sus mensajes ultrasecretos. Durante la misión, que se complica por el oscuro pasado del espía en Tokio, los dos descubren que son peones en un juego más grande. (IMDB)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:10	2:30	La película comienza en la división de descifrado de códigos en Washington. Se dedican a descifrar mensajes japoneses (en la pared se ve el código morse japonés, no se habla del cifrado de los mensajes). Llega un mensaje distinto a los habituales, no son capaces de descifrarlo.
13:45	14:30	Se informa al teniente Ellis y a Eddie Doyle, el ladrón, que los japoneses están usando un nuevo código, empleando una máquina que está en manos del embajador japonés Shimada. Y necesitan conseguirla.
49:15	55:00	Encuentran la máquina Red en casa del emperador. El objetivo es obtener fotografías y aprender del funcionamiento. Desmontan la máquina para estudiar y tener fotos de cada uno de los componentes.
58:06	58:50	Presentan el informe sobre la máquina con fotos: tiene un teclado con alfabeto japonés, hay unos indicadores iluminados en el panel superior, tiene tres rotores cada uno con una rueda que tiene 87 slots, el cableado interno…
1:00:19	1:01:28	Ellis discute con la responsable de la operación. Van a construir un duplicado de la máquina, pero no tienen el libro con el set up diario.
1:09:25	1:10:30	Ellis le cuenta al embajador que saben que están usando la máquina como una forma de entretenerlo mientras el ladrón roba el libro de códigos. Le dice que “tiene una idea bastante aproximada de la máquina”, lo que provoca un gesto de condescendencia por parte del embajador enfatizando que con esa máquina “no es suficiente tener una buena idea”.
1:11:50	1:12:20	Eddie Doyle fotografía el libro de códigos mientras Ellis y el embajador hablan.

Concepto: Máquina Red

Esta producción de bajo presupuesto pero elegante, bien construida y muy entretenida tiene como elemento central el conseguir información sobre una máquina Red. Cuando los criptoanalistas americanos se encuentran con cifrados imposibles de romper, acuden a un militar y a un ladrón para obtener la descripción más detallada posible. Lo consiguen y la película da una descripción detallada basada en las informaciones sobre la máquina. La película muestra también en las primeras escenas las consecuencias de ese paso, cuando los criptoanalistas, acostumbrados al cifrado manual de una libreta de un solo uso u otro método, se enfrentan a las complejidades de los códigos generados por máquinas.

Tiempo de representación	13min 28s (16%)	
Definición	Definido	
Funcionamiento y uso	Impreciso	Se muestra la máquina por dentro pero no se usa en la película.
Representación gráfica del concepto	Realista	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler (https://www.youtube.com/watch?v=BQalz_VOFac) y en la sinopsis.

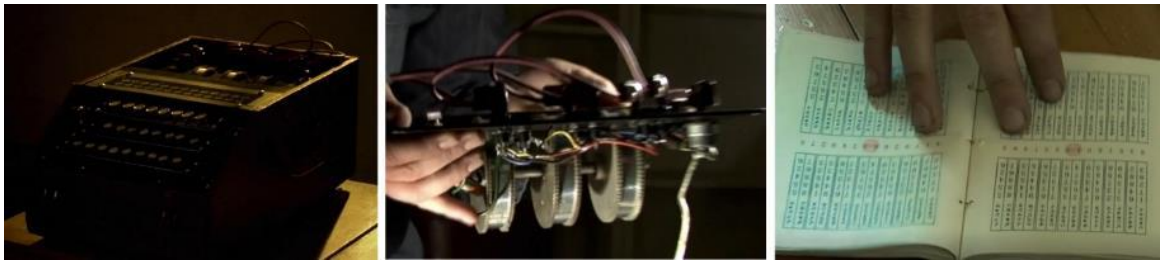


Figura 64: The red machine – Máquina Red

4.51. The Silent War

Duración: 120 minutos
País: Hong Kong
Género: Thriller
Año: 2012
Director: Felix Chong, Alan Mak

Un thriller de espionaje ambientado en los años 1950 que adapta la novela "Year Suan/Plot Against" de May Jia. Tony Leung Chiu Wai interpreta a un hombre ciego que trabaja para un afinador de pianos. Jake ha sido reclutado para una misión de espionaje debido a su sentido de la audición. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
1:00	2:30	La película comienza con una sala de intercepción de comunicaciones, con mensajes cifrados y como estos se descifran y retransmiten. No hay más detalles.
11:00	12:50	La agente Zhang recibe la información de que un mes antes la sala de intercepción de comunicaciones perdió todos los canales enemigos, del Kuomingtan, ya que la película retrata la Guerra Civil china. Estos volvieron, pero solo transmitiendo informaciones de poca importancia. La agente pregunta si el cifrado ha cambiado. Pero no es ese el problema, sino un probable cambio de frecuencias. La agente recibe la misión de traer a la persona que puede recuperar esas frecuencias.
42:50	44:10	He Bing es capaz de encontrar las nuevas frecuencias gracias a su sentido del oído desarrollado.
58:00	1:04:00	Tras un ataque, la agencia del gobierno es consciente que hay una o varias emisoras que no han sido encontradas puesto que hay mensajes que no se han logrado obtener y descifrar. Encuentra esos canales e incluso es capaz de describir cómo actúan las personas que envían el código morse. Son cifrados distintos que no son capaces de desencriptar, pero suponen que están dirigidos al espía enemigo más importante.

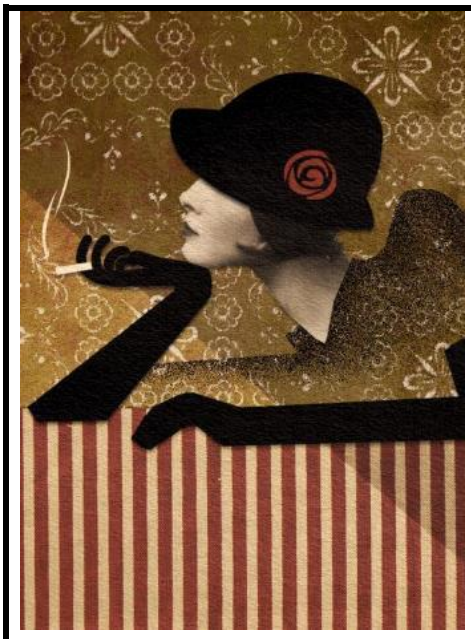
Concepto: Frecuencias de transmisión de mensajes

Nos encontramos con un concepto interesante que no es exactamente criptográfico pero que tiene mucho que ver con la aplicación de la criptografía en el mundo militar. En la gran mayoría de películas el foco está puesto en los métodos de descifrado y en cómo usar la ventaja competitiva que implica tener acceso a los mensajes del

enemigo. Sin embargo, un mensaje no se puede descifrar si no se ha recibido y esta película centra su atención en eso. En un momento determinado, las frecuencias de transmisión habituales del enemigo se quedan en silencio o retransmiten mensajes cifrados casuales. Los métodos de descifrado funcionan, pero la fuente de información no. Esto genera un tipo distinto de problema, que esta película en particular resuelve de manera bastante irreal.

Tiempo de representación	10min 40s (9,8%)	
Definición	Definido	
Funcionamiento y uso	Impreciso	
Representación gráfica del concepto	Dramatizada	Todo el proceso de volver a encontrar las frecuencias correctas es un artificio cinematográfico poco realista.
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler: https://www.youtube.com/watch?v=ZrbTKRgAU7M

4.52. The Thomas Beale Cipher



Duración: 10 minutos
País: Estados Unidos
Género: Thriller
Año: 2010
Director: Andy Allen

El profesor White, criptógrafo extraordinario, está tras la pista del cifrado de Thomas Beale notoriamente imposible de descifrar, un acertijo de un siglo de antigüedad que oculta la ubicación de una fortuna en oro. Pero White no está solo: fuerzas sombrías lo siguen de cerca. (IMDB)
https://www.youtube.com/watch?v=xMdFfWVoI-o

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
0:35	0:40	El corto abre con una serie de noticias del protagonista y acaba esta secuencia con una portada de un periódico en el que se le acusa de espía. Junto a ellas otras noticias que hablan de los esfuerzos de Alan Turing por decodificar la Enigma.
0:55	1:10	Explica que lo persiguen los federales por haber descifrado el mayor reto de su tiempo, en referencia a los Beale Papers.
1:35	1:40	Se muestra una toma de la maleta del profesor White, que incluye en su interior una máquina de cifrar, lo que se intuye es muy próximo a una Enigma.
2:20	3:35	Se explica la historia de Thomas Beale, de cómo se supone que enterró un tesoro y escribió tres mensajes cifrados para establecer su localización. Y que este misterio no ha sido resuelto todavía tras muchos intentos.

Concepto: El misterio de los Beale Papers – cifrado por libro

La inclusión de este corto viene motivada por dos razones principales: en primer lugar, porque se basa en una historia fascinante relacionada con la criptografía, los papeles Beale; en segundo lugar y es algo bastante más subjetivo, por la calidad del corto y el juego con los espectadores pues incluye algunos cifrados para mantener el entretenimiento. Se trata de una curiosidad, pero una de aquellas que puede dar origen a explicar varios conceptos y que resulta muy coherente con el proyecto divulgativo.

El corto explica brevemente la historia de Thomas Beale y los mensajes cifrados que supuestamente marcan el tesoro escondido y a partir de ahí construye un pequeño thriller de gran riqueza teniendo en cuenta que son 10 minutos. No hay detalles sobre el tipo de cifrado de los papeles de Beale, aunque, como juego, el corto incluye algunos mensajes cifrados como el que se puede ver en una imagen que se presenta abajo.

Tiempo de representación	1min 40s (16,6%)	
Definición	Definido	Se nombran y explican los papeles de Beale.
Funcionamiento y uso	No mostrado	No se muestra el cifrado.
Representación gráfica del concepto	Dramatizada	Es una versión animada y libre del concepto sin explicación o reflejo real.
Avance de trama	Sí	Es el elemento alrededor del que gira la trama.
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler: https://www.youtube.com/watch?v=QdgJ4ilz3-w

Figura 65: The Thomas Beale Cipher – Noticias

Figura 66: The Thomas Beale Cipher – La máquina "Enigma"

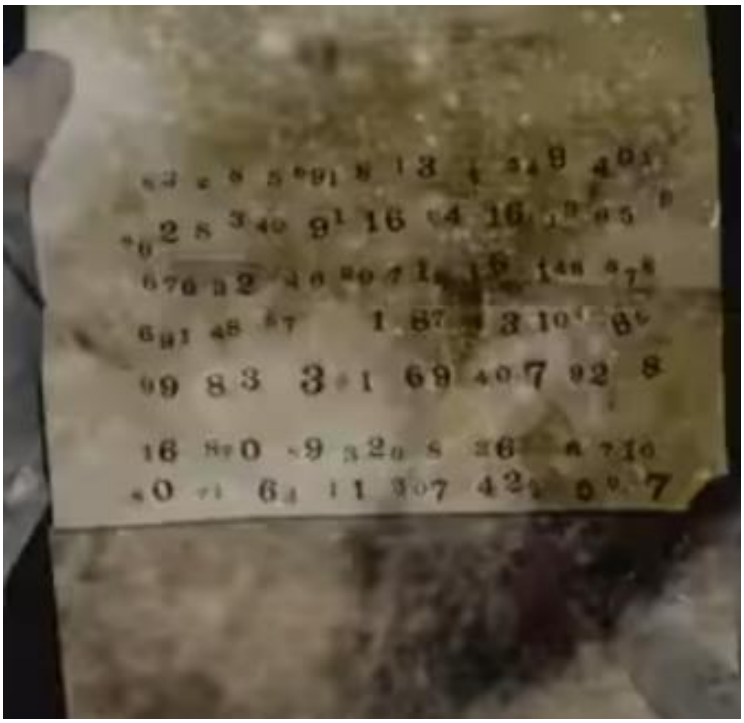


Figura 67: The Thomas Beale Cipher – Papeles de Beale

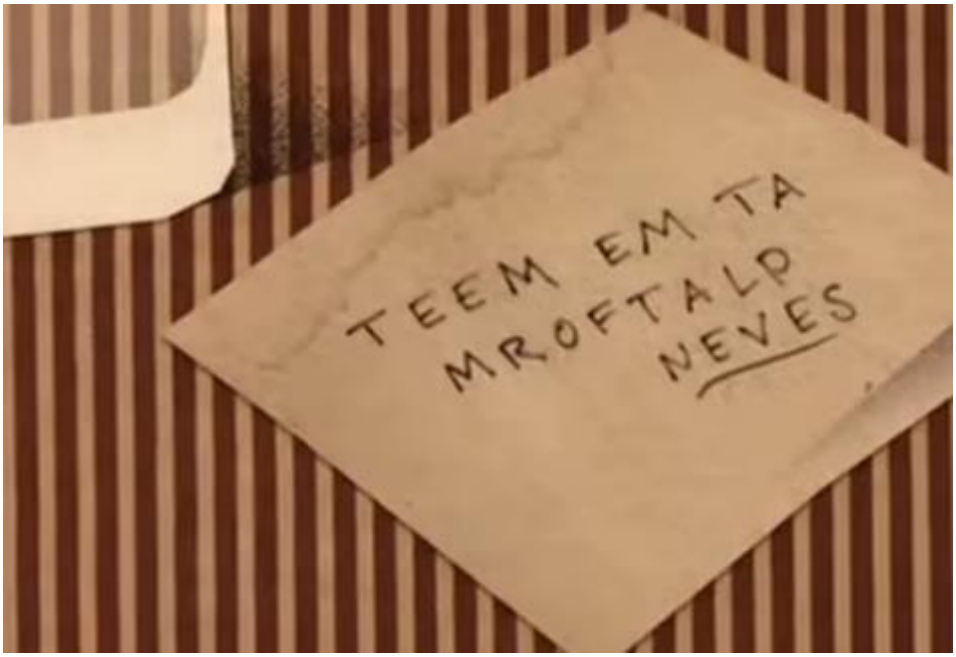
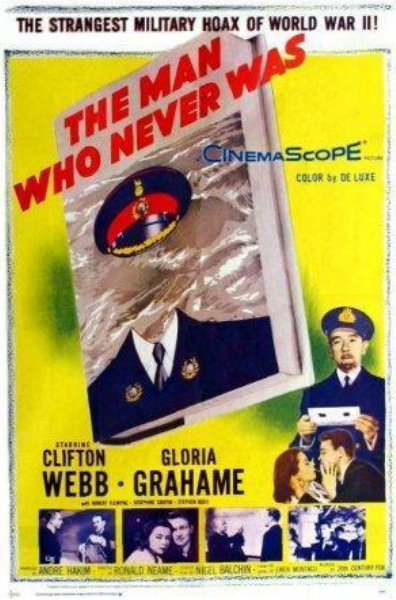


Figura 68: The Thomas Beale Cipher – Juego "Meet me at platform seven"

4.53. The Man Who Never Was (El hombre que nunca existió)



Duración: 103 minutos
País: Reino Unido
Género: Bélico
Año: 1956
Director: Ronald Neame

En la primavera de 1943, un vecino de Punta Umbría descubrió, mientras pescaba en ”El Portil”, el cuerpo sin vida de un militar inglés junto con los restos de una balsa neumática. Sin saberlo, aquel pescador, acababa de encontrar al hombre que nunca existió: la operación “Mincemeat” había comenzado.
(FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
59:50	1:00:55	El Comandante Montagu recibe una llama de su superior. Le pide que perturbe las comunicaciones telefónicas. El Mayor Montagu acciona un botón en el teléfono (secráfono) etiquetado como “Secret”. En la conversación hablan como la operación Mincemeat sigue su curso correctamente y el cadáver del falso militar portador de los papeles con los que se intenta que los alemanes dividan sus fuerzas en el Mediterráneo ha llegado a Huelva.

Concepto: Secráfono

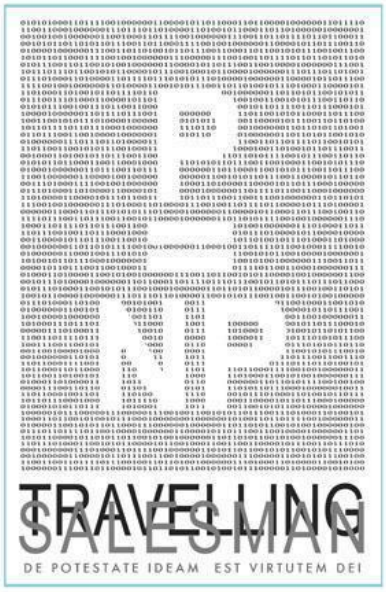
Esta película es una muy buena adaptación de la historia real, la que hubo detrás de la operación Mincemeat. Aunque incluye algunos elementos de ficción para darle un toque más cercano al thriller, en el fondo es un ejemplo muy bien realizado de una operación de ocultación y modificación de información propia de toda la Segunda Guerra Mundial. En el film se emplea un secráfono para ciertas comunicaciones que no debían ser interceptadas.

Tiempo de representación	1min 5s (0,98%)	
Definición	Parcial	
Funcionamiento y uso	Impreciso	Se muestra cómo se acciona el botón Secret del secráfono, pero no el proceso subyacente.
Representación gráfica del	Realista	

concepto		
Avance de trama	Sí	
Reutilización	No	
Referencias en marketing	No	

Figura 69: The man who never was – Secráfono

4.54. Travelling Salesman



Duración: 80 minutos
País: Estados Unidos
Género: Ciencia ficción
Año: 2012
Director: Timothy Lanzone

Definida como un "thriller intelectual", "Travelling Salesman" plantea qué sucedería si cuatro inteligentes matemáticos hubieran conseguido resolver uno de los grandes enigmas de la historia de la ciencia: P = NP. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
9:30	9:50	Presentan a un ponente (Tim Morton) que fue laureado con un premio por haber descubierto la no existencia de las funciones unidireccionales (como las empleadas para los algoritmos criptográficos actuales). Es una de las cuatro personas que están discutiendo el proyecto secreto.
19:30	20:28	Primera referencia a un procesador y unos algoritmos que demuestran la resolución del problema P vs NP. En la película se explica que casi todas las áreas del conocimiento se basan en la idea de que las búsquedas por fuerza bruta son difíciles y conllevan mucho tiempo. Han demostrado una manera para facilitar el proceso y eso lo cambia todo.
35:45	37:55	Se determina que una de las implicaciones de la solución del problema es que los algoritmos de encriptado pueden ser rápidamente descifrados, y la necesidad de que se aparezcan nuevos algoritmos.

Concepto: El problema P vs NP

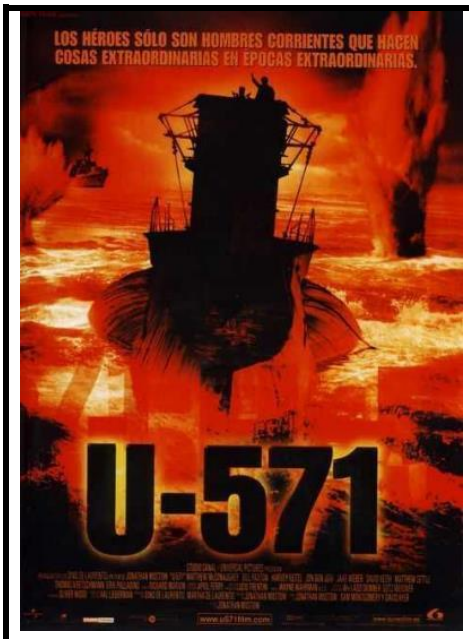
Este es uno de los grandes problemas de la teoría computacional que tiene que ver con la complejidad. Hay problemas que pueden ser resueltos por un ordenador en un tiempo P mientras que otros, los NP, son tan complejos que el tiempo es infinito. Resolver este problema sería demostrar que los problemas NP pueden ser reducidos mediante “atajos matemáticos” a problemas P. Esto afectaría a algoritmos de encriptación que se basan en la descomposición de números primos grandes, por ejemplo. De ahí de interés de esta película que en muchas de sus secuencias habla

de esta implicación de la resolución del problema, por ser una de las que mayores consecuencias podría tener a nivel mundial.

“Travelling Salesman” reflexiona sobre este tema sin entrar en las ecuaciones, pero sí adentrándose en el territorio matemático teórico. He destacado las secuencias que tienen que ver con la criptografía de una manera u otra, aunque se podría subrayar el 60% de la película. El film en general es muy interesante salvo cuando entra en la parte de la conspiración y el interés se desplaza en otras direcciones.

Tiempo de representación	3min 28s (4,3%)	
Definición	Definido	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Neutra	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	

4.55. U-571



Duración: 116 minutos
País: Estados Unidos
Género: Bélico
Año: 2000
Director: Jonathan Mostow

En 1942, en plena Segunda Guerra Mundial, la flota alemana está causándole a los Aliados un gran número de bajas gracias a un sistema de comunicaciones llamado "enigma". Un capitán norteamericano ha conseguido, sin embargo, detectar que las señales del codificador "enigma" proceden de un submarino alemán averiado, el U-571, que se encuentra en mitad del Atlántico Norte. Un grupo de oficiales aliados es enviado para reducir a la tripulación del U-571 y apoderarse del codificador. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
00:00	01:00	Se describe en la película que los submarinos alemanes están causando grandes bajas en los aliados y que éstos son incapaces de descifrar sus comunicaciones.
23:10	24:20	Un submarino aliado quiere interceptar un submarino alemán averiado que transporta la Enigma. Se hará pasar por un submarino alemán que va a abastecerles y a ayudarles con la reparación de la avería. El objetivo es capturar la Enigma. Se determina que los alemanes están ganando la guerra gracias a la Enigma. Es una misión tipo “caballo de Troya”.
41:32	41:40	Se muestra la Enigma dentro del submarino alemán.
44:30	44:40	Los soldados aliados recogen la Enigma y se preparan para llevarla a su submarino.
1:21:20	1:21:40	Los militares americanos discuten que no pueden ser capturas porque los alemanes les torturarían para saber qué conocimientos tienen de sus códigos, entre otras cosas. Se establece la importancia de que los alemanes no sepan cuánto sabe el ejercito aliado de sus sistemas de cifrado.

Concepto: Obtención de la máquina Enigma por parte de los aliados

La Enigma y su importancia en la Segunda Guerra Mundial se refleja en esta película bélica en la que el objetivo de unos soldados es capturar una máquina dentro de un submarino. La captura de una Enigma era primordial para poder hacer ingeniería

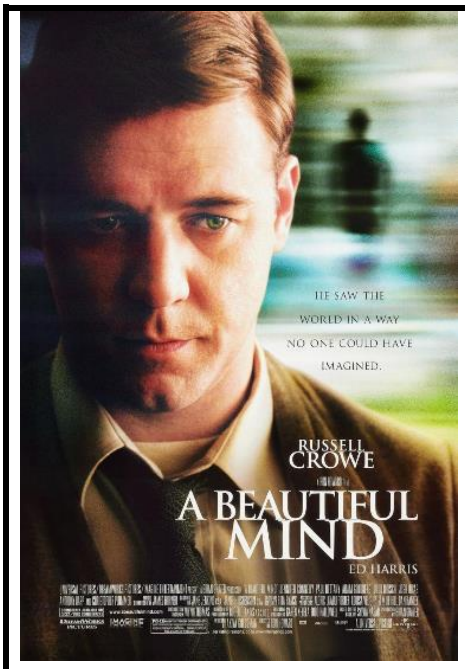
inversa y descifrar las comunicaciones interceptadas. Estos esfuerzos quedan claros en esta película que, sin embargo, no retrata hechos reales. La primera máquina Enigma naval fue capturada por marineros ingleses del HSM Bulldog del submarino alemán U-110 en mayo de 1941, meses antes de la implicación de los norteamericanos y años antes de que éstos capturasen una Enigma.

Tiempo de representación	2min 48s (2,4%)	
Definición	Parcial	Se nombra la Enigma sin explicar para qué sirve. Sólo hay vagas referencias a que parece una máquina de escribir.
Funcionamiento y uso	No mostrado	No se muestra el funcionamiento de la Enigma.
Representación gráfica del concepto	Neutra	Todo el proceso de capturar una maquina Enigma es una dramatización que no es precisa en cuanto a los hechos históricos, aunque parte de algunos reales.
Avance de trama	Sí	La captura de la Enigma es el origen de toda la trama.
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler (https://www.youtube.com/watch?v=aFdmp8ZIDGM) y en la sinopsis.

Figura 70: U-571 – Máquina Enigma a capturar

Figura 71: U-571 – Máquina Enigma dentro del submarino alemán

4.56. A Beautiful Mind (Una mente maravillosa)



Duración: 130 minutos
País: Estados Unidos
Género: Drama
Año: 2001
Director: Ron Howard

Obsesionado con la búsqueda de una idea matemática original, el brillante estudiante John Forbes Nash llega a Princeton en 1947 para realizar sus estudios de postgrado. Por fin, Nash esboza una revolucionaria teoría y consigue una plaza de profesor en el MIT. Gracias a su prodigiosa habilidad para descifrar códigos es reclutado por Parcher William, del departamento de Defensa, para ayudar a los Estados Unidos en la Guerra Fría contra la Unión Soviética. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
25:20	27:50	El profesor John Nash llega al Pentágono. Le explican que han interceptado trasmisiones de radio de Moscú pero que el ordenador no detecta ningún patrón, pero ellos creen que es una clave. Son secuencias de números. John Nash observa los mensajes y mentalmente los analiza (lo representan destacando diferentes secuencias de números) y descubre que son latitudes y longitudes que pertenecen a diferentes puntos de EE. UU marcando una ruta.
35:10	37:11	William Parcher del Departamento de Defensa se reúne con Nash para pedirle que trabaje con ellos en una operación secreta relacionada con una bomba atómica que robaron los soviéticos a los nazis. Una parte del ejército soviético, Nueva Libertad, pretende detonarla en EE. UU. Nueva Libertad se comunica con los agentes mediante códigos insertados en revistas y periódicos y necesitan que Nash los descifre. Para ellos le hace memorizar una serie de revistas y periódicos.
44:46	46:15	Nash observa y analiza diferentes recortes de periódicos y revistas. De repente descubre un patrón que podrían ser mensajes (lo muestran de la misma manera, destacando diferentes letras y números). Se ve a Nash escribiendo una serie de letras y números y señalando localizaciones en un mapa.
49:13	49:35	Se ve a Nash marcando con lápiz diferentes palabras de una revista. Una niña le pregunta que qué está haciendo y él le explica que está buscando patrones en publicaciones periódicas.
1:31:00	1:31:30	Nash vuelve a tener alucinaciones y cree ver un nuevo mensaje en un periódico (se ve otra vez como se destacan palabras). Empieza a marcar diferentes palabras con lápiz hasta que alguien lanza una piedra a su ventana.

Concepto: Guerra Fría y criptografía – John Nash

Este biopic de John Forbes Nash se centra en su vida desde su periodo de estudios hasta la obtención del premio Nobel. La aparición de elementos criptográficos está principalmente relacionada con la enfermedad mental de Nash, diagnosticado de esquizofrenia, que le hacía creer que trabajaba para el Departamento de Defensa descifrando códigos. En el ambiente de Guerra Fría, esa obsesión con ser perseguido por rusos formaba parte de una cierta realidad, aunque no la de Nash. En la película muestran la esquizofrenia con las alucinaciones visuales que incluyen otras personas con las que se comunica. En la realidad Nash tenía alucinaciones auditivas pero los temas eran similares.

Tiempo de representación	6min 52s (5,3%)	
Definición	Parcial	
Funcionamiento y uso	No mostrado	
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler (https://www.youtube.com/watch?v=aS_d0Ayjw4o) y en la sinopsis.

4.57. Lemony Snicket's a Series of Unfortunate Events (Una serie de catastróficas desdichas de Lemony Snicket)

Duración: 103 minutos
País: Estados Unidos
Género: Aventuras
Año: 2004
Director: Brad Silberling

Violet, Klaus y Sunny Baudelaire, tres niños huérfanos, son adoptados primero por unos extraños parientes y después por Lemony Snicket (el narrador de la historia). También se hace cargo de los Baudelaire el astuto y ambicioso Conde Olaf cuyo objetivo es arrebatarles la herencia. Violet, la mayor, tiene catorce años y es la más valiente de los tres. Klaus, de doce años, es muy inteligente y vive obsesionado con el mundo de las palabras. Sunny, la pequeña, habla un lenguaje que solo sus hermanos pueden entender. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
40:25	40:55	Klaus usa una serpiente que ha visto varias veces enrollada en el brazo de su tío para dejarle un mensaje. La serpiente funciona como una escítala, los caracteres escritos verticalmente al enrollarse en la muñeca del tío de Klaus forman la palabra impostor, referida al ayudante que acaba de llegar que no es otro que el Conde Olaf.
59:30	1:01:05	Encuentran una nota de suicidio escrita por su tía Joe. Se trata de una nota con muchísimas faltas de ortografía, que no serían normales en su tía pues le obsesionaba la gramática. Klaus deduce que hay un mensaje escondido dentro. Se muestran imágenes de algunos de los libros que Klaus ha leído sobre criptografía. El niño deduce que cada error en una palabra da una letra correcta que forma parte del verdadero mensaje que su tía les quería dejar. Así, la palabra ike debe ser ice, por tanto una c; inbearable debe ser unbearable y por tanto u… El resultado del mensaje es Curdle Cave y suponen que su tía está escondida.

Concepto: Escítala

Tiempo de representación	30s (0,5%)	
Definición	Indefinido	No se define ni se nombra.

Funcionamiento y uso	Impreciso	Se muestra el funcionamiento parcial.
Representación gráfica del concepto	Dramatizada	La escítala es una serpiente, es una representación dramatizada.
Avance de trama	Sí	Con el mensaje descubren que el impostor es el Conde Olaf.
Reutilización	No	
Referencias en marketing	No	

Figura 72: Lemony Snicket – Escítala serpiente

Concepto: Código de sustitución

Tiempo de representación	1min 35s (1,5%)	
Definición	Parcial	Se define sin nombrarlo.
Funcionamiento y uso	Correcto	Klaus describe el proceso para obtener el mensaje oculto. No es un proceso completo, pero está correctamente mostrado.
Representación gráfica del concepto	Realista	
Avance de trama	Sí	Les permite encontrar a su tía que se ha escondido.
Reutilización	No	
Referencias en marketing	No	

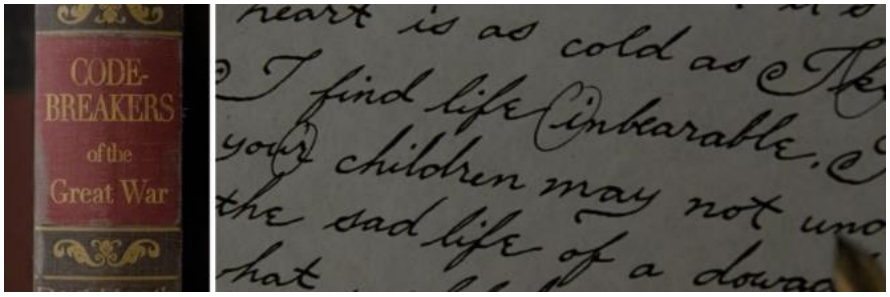


Figura 73: Lemony Snicket – Mensaje escondido (sustitución simple)

4.58. Viaje al centro de la Tierra

Duración: 90 minutos
País: España
Género: Aventuras
Año: 1976
Director: Juan Piquer Simón

Un científico organiza una fabulosa expedición para llegar al centro geográfico de la Tierra. Acompañado de una pareja de novios y un pastor, durante el viaje tendrá que vérselas con seres extraordinarios y diversos peligros. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
5:30	8:40	Encuentran un mensaje en un libro que relata una supuesta expedición al centro de la Tierra. Después de varios intentos consiguen descifrarlo encontrando que es un cifrado de transposición doble. En primer lugar, el mensaje se ha escrito en espejo y luego organizado en columnas que se han transpuesto. Es una versión simplificada de la explicación más detallada que hace Jules Verne en la novela, pero para descifrarlo utilizan dos elementos interesantes: un proyector de diapositivas para trasladar las columnas y hacer más visible esa traslación y un espejo, para poder leer el mensaje al revés.

Concepto: Cifrado por transposición

Hay varias versiones de la novela de Jules Verne, en la que el autor dedica varios capítulos a descifrar el mensaje que da inicio a la aventura. Esta versión española de Juan Piquer Simón es la que representa con cierto detalle algunos de los elementos presentes en la novela y creo que es destacable el cuidado que puso en explicar, aunque sea parcialmente, el proceso de descifrado del mensaje recibido.

Tiempo de representación	3 min 10s (3,5%)	
Definición	Indefinido	No se define ni se nombra.
Funcionamiento y uso	Impreciso	Se muestra con el juego del proyector y el espejo una ligera idea del cifrado.
Representación gráfica del	Neutra	Se usan elementos muy cinematográficos para enseñar el cifrado, pero son efectivos y se puede entender en general cómo

concepto		funciona.
Avance de trama	Sí	Es el inicio del viaje al centro de la Tierra.
Reutilización	No	
Referencias en marketing	No	

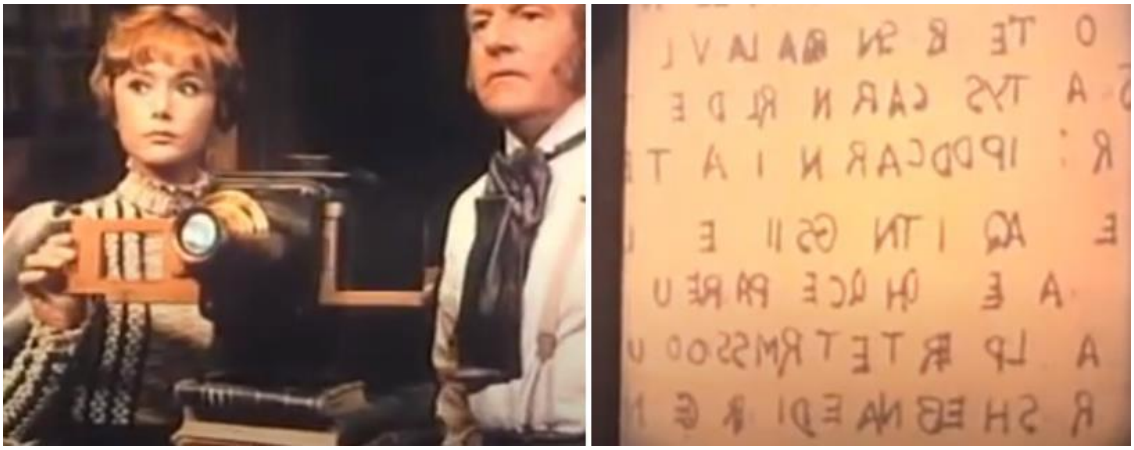


Figura 74: Viaje al centro de la tierra – Cifrado por transposición

4.59. Windtalkers

Duración: 133 minutos
País: Estados Unidos
Género: Bélico
Año: 2002
Director: John Woo

Durante la Segunda Guerra Mundial el avance de las tropas estadounidenses en la campaña del Pacífico se ve seriamente obstaculizado por la capacidad de los servicios de inteligencia japoneses para descifrar mensajes. A finales de 1942, son entrenados varios centenares de indios navajos para emplear un código secreto basado en su lengua materna. Los protagonistas son dos oficiales cuya misión es proteger a dos indios navajos enrolados en la Marina. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
9:00	10:10	Los indios navajos son entrenados para ser code talkers.
14:30	15:20	Siguen haciendo pruebas para mejorar sus habilidades a la hora de recibir y descifrar mensajes.
17:00	18:40	El Sargento Enders recibe una nueva asignación. Le explican que el ejército estadounidense ha desarrollado un nuevo código basado en la lengua de los navajos que los japoneses no pueden descifrar y hay que proteger dicho código. Enders tiene como misión acompañar a un soldado navajo para protegerlo, pero sobre todo para proteger el código que no puede caer en manos enemigas.
43:00	44:20	Yahzee, el code talker de Anders, transmite un mensaje usando el código navajo. Los japoneses interceptan, pero son incapaces de descifrar.
1:38:40	1:41:20	Anders se ve obligado a matar a uno de los code talkers que iba a ser capturado. El código es más importante que los code talkers.

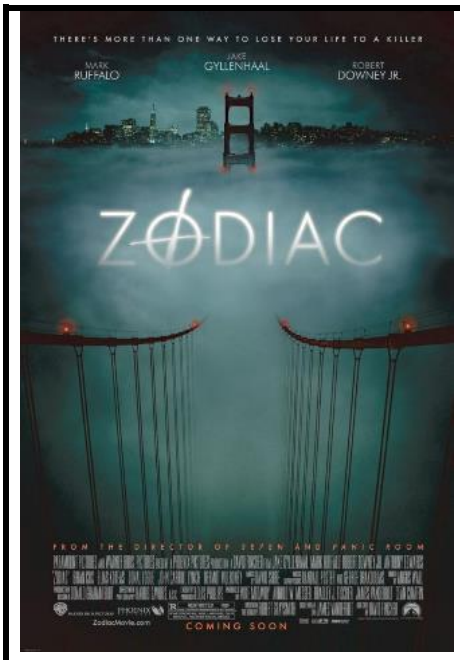
Concepto: Segunda Guerra Mudial – Code Talkers

La película retrata la importancia del código basado en la lengua de los navajos que se desarrolló para asegurar las comunicaciones y que los japoneses no las interceptaran. Se muestran unas breves escenas del proceso de aprendizaje y de su intervención en misiones.

Tiempo de representación	6min 40s (4,9%)	
Definición	Definido	Se explica la necesidad del código y de los cifradores navajos.
Funcionamiento y uso	No mostrado	Los procesos de cifrado y descifrado no se muestran.
Representación gráfica del concepto	Dramatizada	
Avance de trama	Sí	Los code talkers son el centro de la trama.
Reutilización	Sí	
Referencias en marketing	Sí	Aparece en el tráiler (https://www.youtube.com/watch?v=KOmH0_F8_XI) y en la sinopsis.

Figura 75: Windtalkers – Código navajo

4.60. Zodiac



Duración: 158 minutos
País: Estados Unidos
Género: Thriller
Año: 2007
Director: David Fincher

Thriller sobre el famoso "Asesino del Zodiaco", un asesino en serie que, entre 1966 y 1978, mató a numerosas personas en San Francisco, al tiempo que enviaba a los medios de comunicación cartas con pistas. La acción se centra en las largas pesquisas de dos detectives que intentaron darle caza y en las investigaciones de dos periodistas que trataron de averiguar su identidad. (FILMAFFINITY)

Apariciones de elementos relacionados con la criptografía:

Inicio	Fin	Concepto
10:30	11:55	Asesino del zodiaco envía una carta al periódico que contiene un texto cifrado (se muestra en 11:06). El asesino quiere que el código se publique en prensa.
11:12	14:40	Se describe como está construido el mensaje: el texto cifrado se divide en tres secciones (cada una enviada a un periódico), cada una con 8 líneas y 17 símbolos. No hay espacios entre los símbolos que provienen de 7 fuentes diferentes: griego, código morse, señalización naval, …
14:50	16:30	Los mensajes son descifrados (no hay explicación sobre cómo se hace) por dos aficionados. La última línea del mensaje no tiene sentido, son letras desordenadas y en el periódico empiezan a ver si podría ser un anagrama.
48:05	48:15	Llega una nueva carta del asesino con otro mensaje cifrado.
49:20	50:50	Hablan de los mensajes cifrados explicando que es un código de sustitución simple (monoalfabético), explicando brevemente cómo funciona. Se explica el principio del análisis de frecuencias aplicado al mensaje de zodiac: la consonante doble más habitual es la ll y en una carta de ese estilo debería aparecer la palabra Kill al menos una vez, eso se une al resto del análisis de frecuencias. Se muestra “The code breakers” de David Kahn, que presenta un código de sustitución en el prefacio del que el asesino extrajo 8 símbolos. Hay símbolos que parecen medievales que pertenecen a un cifrado usado en la Edad Media, el alfabeto zodiaco (imagen del libro “Codes and Ciphers” de John Laffin).

Concepto: Código de sustitución homofónico – el asesino del zodiaco

Nos encontramos ante una de las representaciones de uno de los casos criminales más célebres en los que estuvieran incluidos elementos de criptografía. Aunque la película muestra los mensajes encriptados y es fiel a la realidad cuando indica que fueron resueltos por dos aficionados, simplifica (pienso que por razones de no complicar la explicación para el público) al explicar que el cifrado era de sustitución monoalfabético. La complejidad del mensaje, con 54 símbolos, hacía imposible que fuera ese tipo de cifrado. Se puede considerar como un cifrado de sustitución homofónico, que parte del monoalfabético y que añade símbolos para las letras más comunes **(Bauer, 2019)**. Algunos de los mensajes descifrados por el protagonista (Robert Graysmith) se basan en el libro que él mismo escribió y en el que se basa la película, pero han sido discutidos por otros autores **(Bauer, 2019)**. Aun así, la representación gráfica que la película hace del caso, aunque simplificada, se acerca a la realidad de lo que se vivió desde un punto de vista del descifrado de dichos mensajes.

Figura 76: Zodiac – Mensaje cifrado real enviado por el asesino del zodiaco

Tiempo de representación	8min 13s (5,2%)	
Definición	Parcial	Se nombra y se explica del cifrado de sustitución monoalfabético, aunque no sea exactamente el presentado por los mensajes del asesino del zodiaco.
Funcionamiento y uso	Impreciso	Se explica parcialmente el análisis de frecuencias y cómo se utilizaría para descifrar el mensaje.
Representación gráfica del concepto	Realista	La representación de los mensajes, quién los descifró y parte del proceso se basa en la realidad explicada por Robert Graysmith.
Avance de trama	Sí	Es un elemento principal en el desarrollo de la trama.
Reutilización	Sí	
Referencias en marketing	Sí	Se muestran los mensajes cifrados y su importancia https://www.youtube.com/watch?v=yNncHPl1UXg

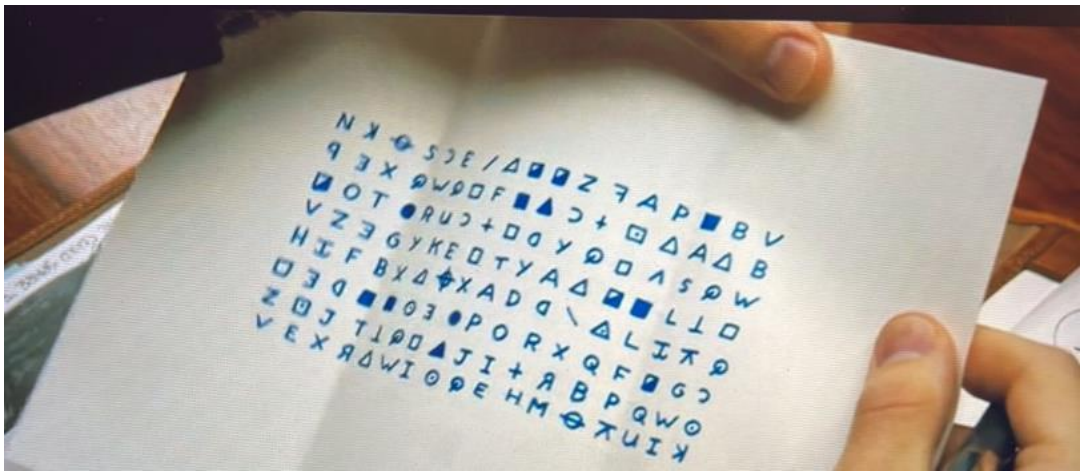


Figura 77: Zodiac – Mensaje recibido tal y como se muestra en la película

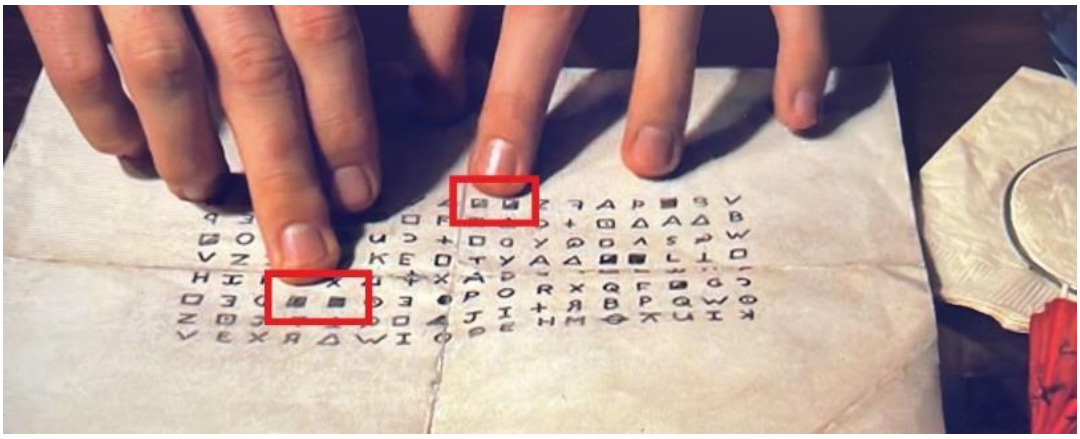


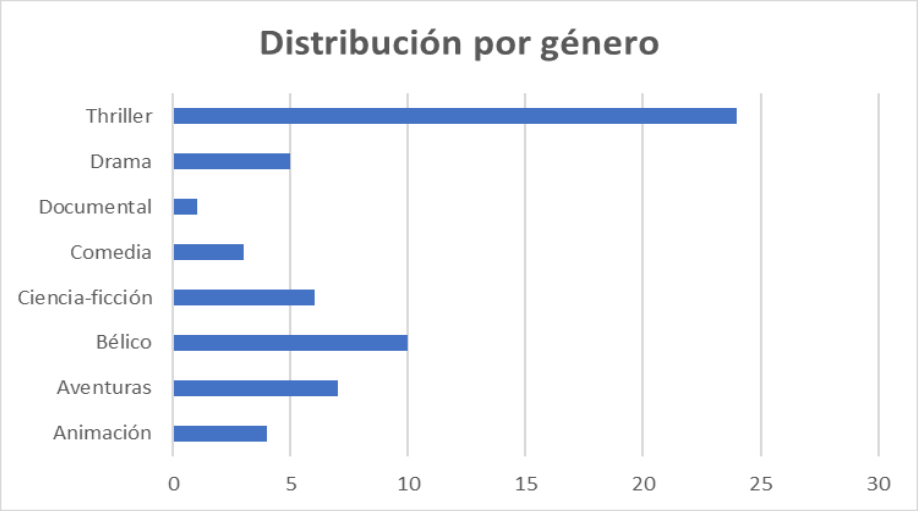
Figura 78: Zodiac – Analisis de frecuencias (símbolos dobles reemplazando la doble ll – se señalan dos pares)

5. EVALUACIÓN GLOBAL Y LÍNEAS DE TIEMPO

Para realizar este trabajo se han visto 76 películas y, de ellas, evaluado 60, que son las que contenían elementos relevantes. A partir de dichas evaluaciones he construido una tabla Excel que se puede encontrar en el Anexo II con la que he hecho un análisis de los diferentes resultados.

5.1. Distribuciones por género y década

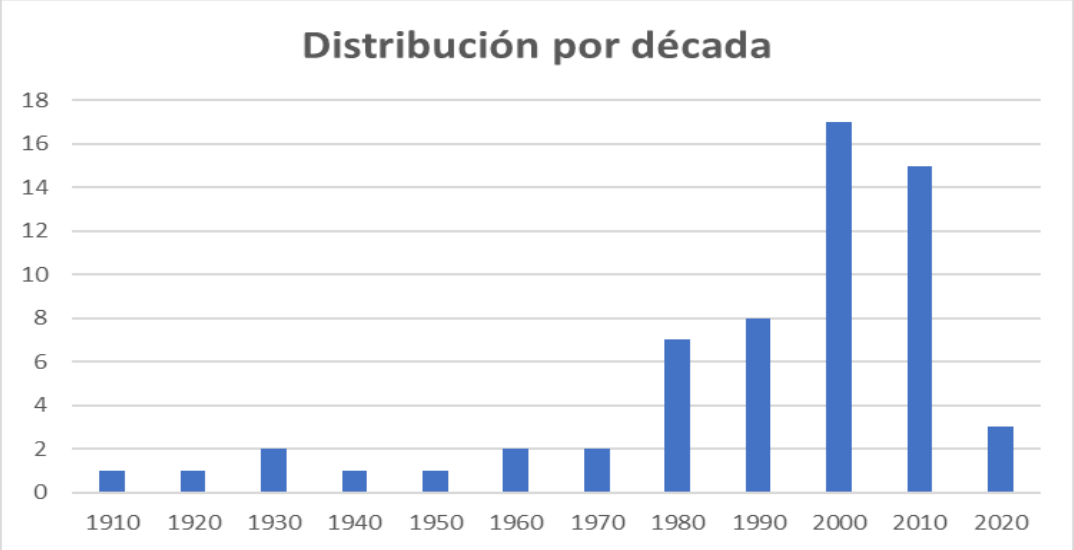
Género	Recuento películas
Animación	4
Aventuras	7
Bélico	10
Ciencia ficción	6
Comedia	3
Documental	1
Drama	5
Thriller	24
Total general	**60**



El género más analizado es el thriller y dentro de este hay muchas películas de espías. A continuación, ténemos películas bélicas y de aventuras. Estos tres géneros son bastante lógicos si tenemos en cuenta las asociaciones directas que se suelen hacer entre la criptografía, los códigos y los tipos de situaciones en los que podemos encontrarlos. El cine enfatiza estos tópicos y construye producciones a partir de estos escenarios más habituales. Sin embargo, creo que he encontrado films interesantes en una amplia distribución de géneros, incluída la comedia, que añaden variedad a los principales.

En cuanto a la distribución por décadas, el número más alto de películas se concentra entre las producciones realizadas a partir del 2000. Creo que es interesante considerar el esfuerzo hecho por encontrar producciones del inicio del cine y queda pendiente para un trabajo futuro el profundizar en las primeras décadas, hasta los años 70, con el fin de encontrar más producciones que incluyan elementos criptográficos.

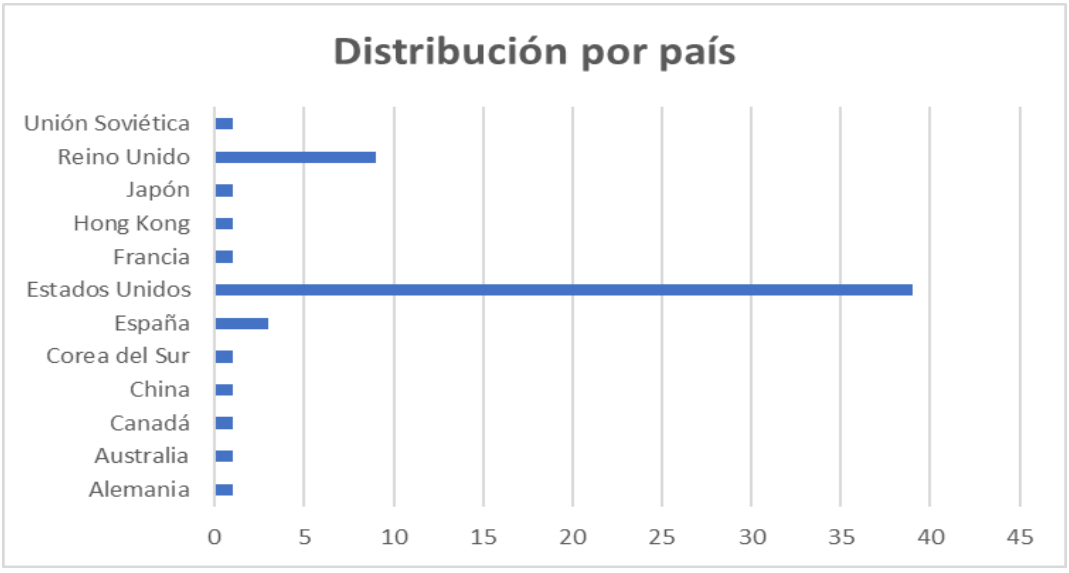
Década	Recuento películas
1910	1
1920	1
1930	2
1940	1
1950	1
1960	2
1970	2
1980	7
1990	8
2000	17
2010	15
2020	3
Total general	**60**



5.2. Distribución por país

La amplia mayoría de películas analizadas provienen de Estados Unidos, siendo el Reino Unido y España los países que le siguen. Era uno de los objetivos del trabajo buscar la mayor diversidad posible en cuanto a la procedencia de las producciones, pero claramente esto se ha convertido en un ejercicio muy difícil. La menor información y conocimiento de las filmografías no estadounidense dificultó la búsqueda, y la limitación de tiempo, teniendo en cuenta todo el que se ha dedicado a ver cada una de las películas, no ha facilitado este proceso. Sin embargo, estoy satisfecho por haber analizado películas de 12 países diferentes, por conseguir que 21 de ellas no sean de Estados Unidos y por haber dedicado un tiempo adecuado y razonable a la búsqueda.

País	Recuento películas
Alemania	1
Australia	1
Canadá	1
China	1
Corea del Sur	1
España	3
Estados Unidos	39
Francia	1
Hong Kong	1
Japón	1
Reino Unido	9
Unión Soviética	1
Total general	**60**



5.3. Evaluación de los conceptos según definición, funcionamiento y representación

A la hora de evaluar los conceptos, en la tabla Excel del Anexo II se puede comprobar que he ido agrupando los diferentes conceptos más detallados dentro los análisis en familias e ideas generales, variadas, pero que permitían realizar análisis agregados, obteniendo un total de 34 conceptos, que se pueden ver a continuación.

Conceptos	Apariciones
Sustitución monoalfabético	10
Cifrado por libro	8
Tinta invisible	6
Cifrado por transposición	4
Máquina Enigma	4
Anagrama	3
Segunda Guerra Mundial	3
Códigos espaciales	2
Escítala	2
Guerra Fría. Interceptar comunicaciones y claves	2
Jeroglíficos	2
Máquina de desencriptado universal	2
Mensaje oculto	2
Oficinas de cifrado	2
Rejilla de Cardano	2
Sustitución polialfabético	2
Buscar criptoanalistas con pasatiempos en prensa	1
Cifrado Playfair	1
Cifrado simétrico	1
Cifrado vs Privacidad	1
Claude Shannon	1
Code Talkers	1
Código Morse y la lengua china	1
Códigos en desuso	1
Criptomonedas	1
Estación de números	1
Frecuencias de transmisión	1
Máquina Red	1
Micropunto	1
Primera Guerra Mundial	1
Problema P vs NP	1
RSA	1
Secráfono	1
Sustitución homofónico	1

Se trata de conceptos variados que cubran gran parte de la historia de la criptografía. Los elementos propios de la critografía moderna, los que dependen mucho más de algoritmos y ordenadores, son mucho más difíciles de encontrar pues su representación en pantalla es menos obvia. De la misma forma, técnicas de cifrado clásicas pero complejas como el cifrado de sustitución polialfabético también tiene apariciones limitadas dado que es complejo de explicar y exige un gran tiempo de pantalla que los guiones no suelen dedicar.

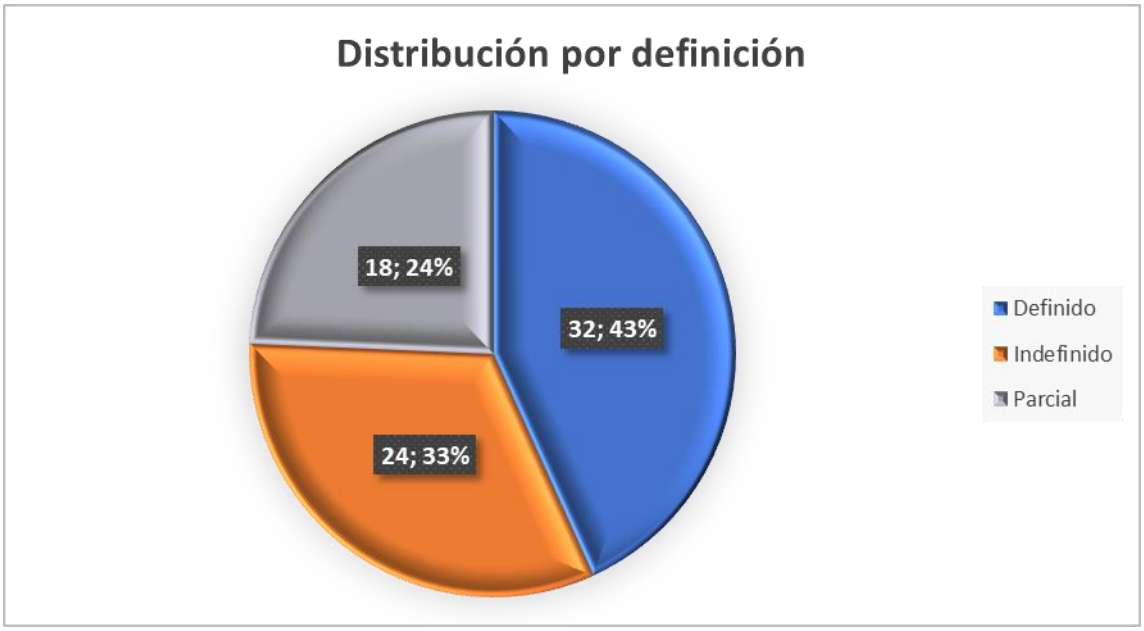
Un concepto en películas diferentes puede tener tratamientos distintos, así que los análisis que se pueden hacer son generales y con alto componente subjetivo, de la misma forma que el visionado de una película y la evaluación de un concepto también parte de un componente subjetivo aunque haya intentado objetivizar lo máximo posible las categorías de análisis. En cuanto al análisis, mostraré unos gráficos globales para cada categoría y el detalle para los conceptos con más apariciones.

Los conceptos con más apariciones son el cifrado de sustitución monoalfabético, el cifrado por libro, la tinta invisible, el cifrado por transposición y la máquina Enigma.

Distribución por definición

Recuerdo en primer lugar que la “definición” era la aparición del nombre y concepto criptográfico representado y que tiene tres valores:

- Definido (se dice el nombre y se define)
- Indefinido (ni se dice el nombre ni se define)
- Parcial (o se dice el nombre o se define)



Concepto	Definido	Indefinido	Parcial	Total apariciones
Sustitución monoalfabético	2	6	2	10
Cifrado por libro	6		2	8
Tinta invisible	4	1	1	6
Cifrado por transposición	1	2	1	4
Máquina Enigma	3		1	4

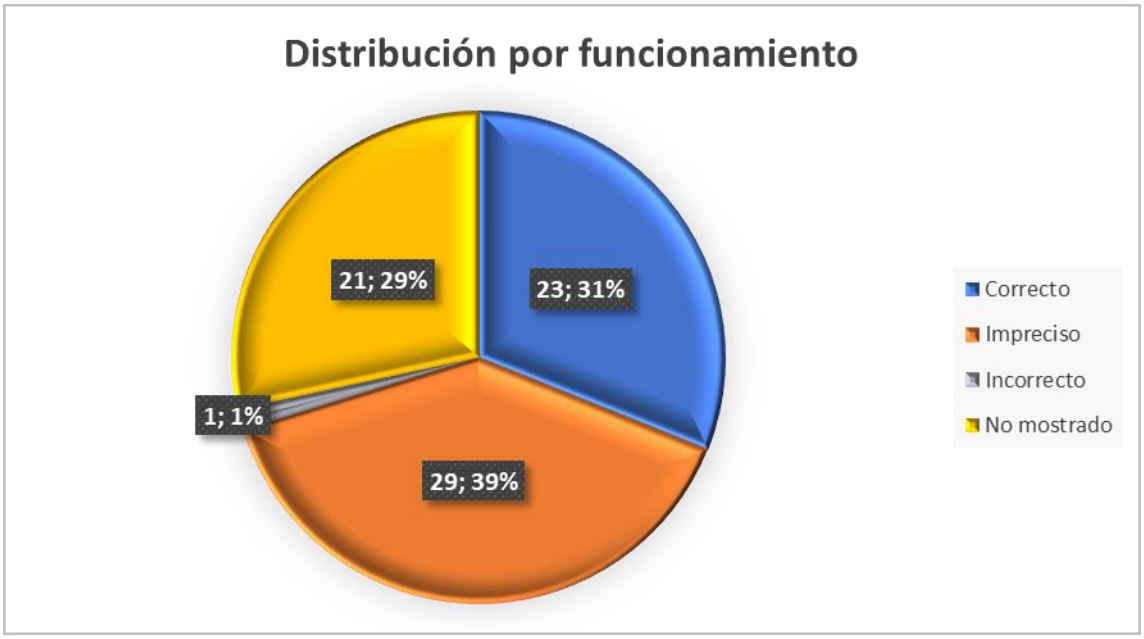
En la distribución general se observa que los conceptos definidos y nombrados constituyen la categoría más alta. Los indefinidos ocupan el segundo lugar de la clasificación. Una definición parcial es menos frecuente.

Respecto a los conceptos observados individualmente encontramos las siguientes conclusiones:

- El cifrado por libro, la máquina Enigma y la tinta invisible están mayoritariamente explicados y nombrados. La máquina Enigma es la parte central de los argumentos de la mayoría de películas en las que aparece y hay un esfuerzo por hacer compresible lo que es, aunque no su funcionamiento como se verá después. El cifrado por libro y la tinta invisible son técnicas divertidas de explicar que entroncan con juegos que podemos haber hecho todos en algún momento de nuestra vida y las explicaciones son más sencillas y necesitan menos metraje para que el público las entienda. Creo que esto justifica que se definan mejor.
- En la mayoría de apariciones del cifrado de sustitución monoalfabético ni se nombre ni se define, se utiliza sin más detalles.
- El cifrado por transposición, con menos apariciones, tiene una distribución variada. En algunos casos se explica lo que es y cómo funciona utilizando letras de Scrabble (“Enola Holmes”) y en otros, la disposición de la cámara sobre el texto claro y el texto cifrado permite observar qué tipo de cifrado es. Podría haber incluido la escítala en esta categoría, pero en los dos casos que aparecen se utiliza correctamente sin nombrar ni dar ninguna explicación sobre la técnica.

Distribución por funcionamiento

Este criterio consistía en mostrar el funcionamiento del concepto en pantalla, con valores que incluyen que el funcionamiento no es mostrado, que se hace con falta de precisión, que es correcto o que es una invención.



Concepto	Correcto	Impreciso	Incorrecto	No mostrado	Total apariciones
Sustitución monoalfabético	3	2	1	4	10
Cifrado por libro	2	4		2	8
Tinta invisible	5	1			6
Cifrado por transposición	2	2			4
Máquina Enigma	1	1		2	4

Para este concepto hay una distribución muy equilibrada. No he encontrado prácticamente casos de un uso totalmente incorrecto ya que muchos de los que estaban poco claros he tenido que clasificarlos en imprecisos dada la falta de detalles. Dicha categoría acaba siendo la más numerosa.

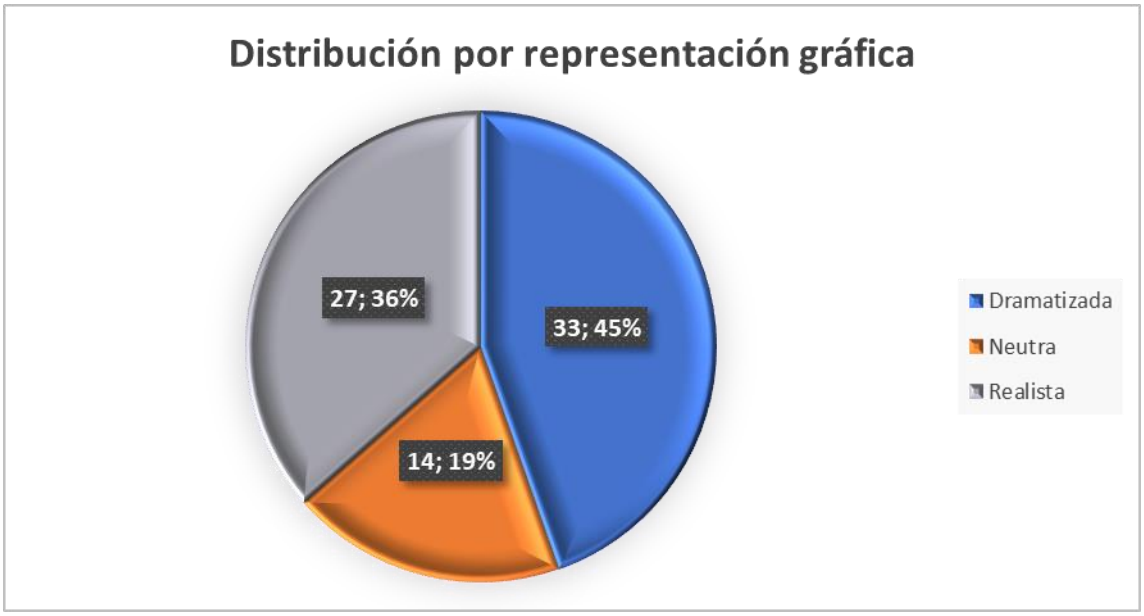
En cuanto a los conceptos con más aparición:

- La tinta invisible es el concepto representado con más corrección en su uso. Probablemente por la misma razón que en el caso anterior, conecta con muchos juegos infantiles y eso ayuda a que sea una técnica fácil de enseñar.
- En el resto los valores están más distribuidos, pero en todos los casos se puede encontrar una aparición con un uso correcto.

- Los usos imprecisos se pueden también se podrían usar con fines didácticos dado que son un buen punto de partida para añadir explicaciones.

Distribución por representación gráfica

La representación gráfica indica como la película está mostrando el concepto, si hay una representación dramatizada (principalmente fílmica, aunque no sea falsa), que se busque una apariencia ligeramente similar o que se emplee una representación realista.



Concepto	Dramatizada	Neutra	Realista	Total apariciones
Sustitución monoalfabético	5	2	3	10
Cifrado por libro	5	1	2	8
Tinta invisible	1		5	6
Cifrado por transposición		2	2	4
Máquina Enigma	2	2		4

Estamos ante películas y no sorprende si la categoría que contiene la mayoría de apariciones es la que prima el contenido cinematográfico frente al real. Sin embargo, en el apartado realista las apariciones no están tan alejadas, por tanto, podemos pensar que en las muestras analizadas hay un cierto equilibrio.

Respecto a los conceptos destacados:

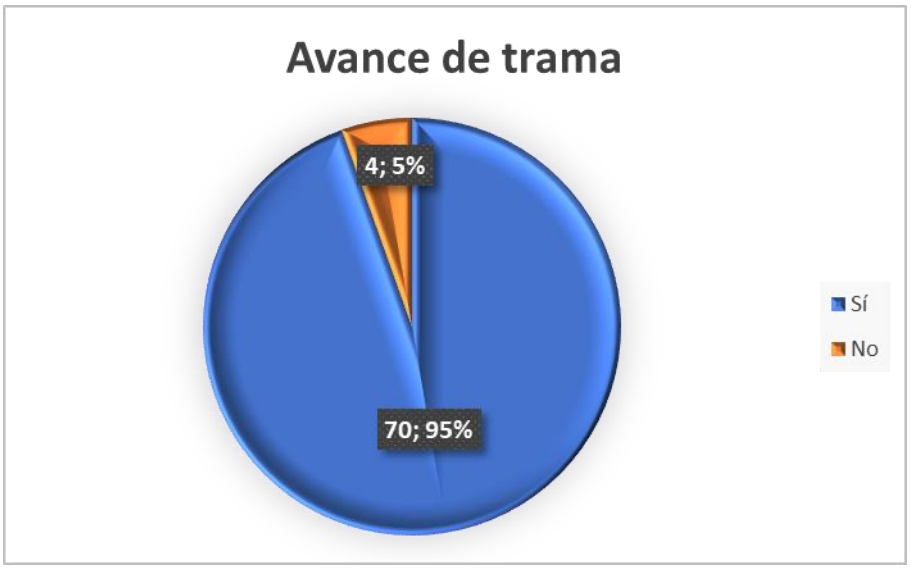
- En el caso de la tinta invisible, hay en general una tendencia a representarlo de forma realista.

- En el cifrado por libro hay una representación más dramatizada puesto que en muchas representaciones basta con tomar un libro y extraer un mensaje descifrado sin apenas haber contado ni una página y sin una sola elipsis. O también está el hecho de adivinar el libro casi por arte de magia.
- En el resto de conceptos, las representaciones están más equilibradas, pero como se ha explicado al principio hay una tendencia general a hacer el concepto atractivo para el espectador y eso conlleva un componente dramático y divertido que se aleja de la realidad más rutinaria.

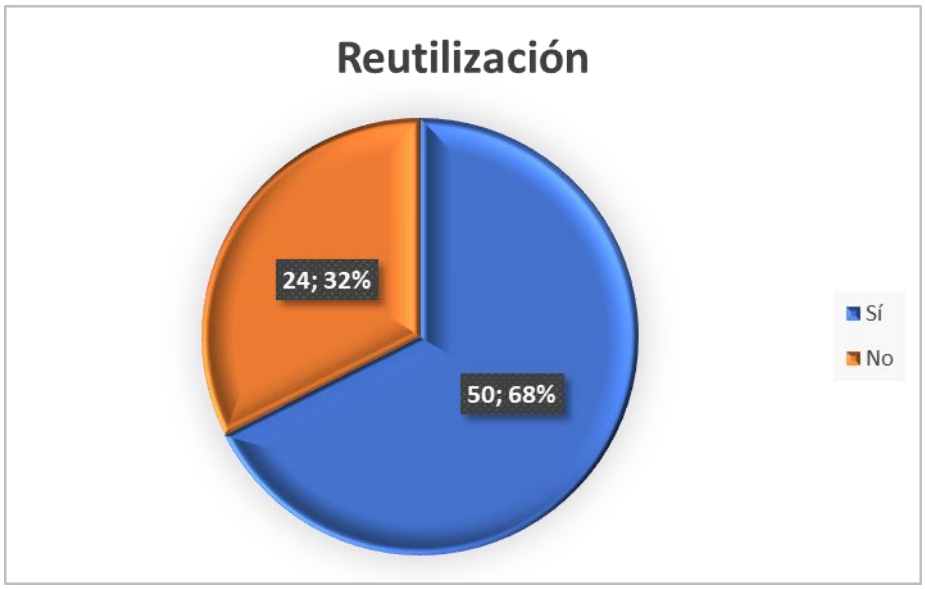
5.4. Distribuciones por avance de trama, reutilización y marketing

Para acabar se analizan los valores booleanos, que indican por un lado si el concepto encontrado permite avanzar de alguna manera la trama de la película, si se reutiliza en diferentes escenas de la película o si se referencia en el marketing (sinopsis, trailer).

En la gran mayoría de películas, el concepto analizado permite avanzar la trama o forma parte de la trama principal. Únicamente en casos particulares como “The final countdown”, “Gravity falls” o “A Christmas story” los conceptos se usan sin que tengan peso en las acciones principales de los personajes sino como acompañamientos, elementos secundarios o juegos con el espectador.



Hay más equilibrio en la reutilización, aunque en la mayoría de las películas el concepto no se menciona una única vez, si no que se reutiliza en diferentes escenas donde consigue más explicaciones o tiempo de pantalla y uso.



En las referencias en el marketing la distribución está equilibrada. La mayoría de referencias se encuentran en el tráiler de la película y a continuación en la sinopsis. Las referencias en los carteles son muy limitadas.

5.5. Conclusiones del análisis

A partir del análisis realizado, la primera conclusión que puedo extraer es que el cine hace una representación limitada de conceptos criptográficos, algo que ya se podía anticipar en mi introducción cuando afirmaba que el tratamiento de los conceptos técnicos es mucho más reducido que los sociales, políticos o históricos. Es más complejo realizar un análisis sobre la representación de los conceptos técnicos en el cine. En primer lugar, porque se encuentran muchas menos películas que los empleen, sobre todo cuando tratamos un tema tan específico como la criptografía. En segundo lugar, porque las explicaciones técnicas son vistas como un repelente de espectadores: cifrados que se definen en detalle en el guión, como el que aparece en “Sherlock Holmes: A game of shadows”, son reducidos en el montaje final a un par de insertos porque alejarían la atención del clímax entre los dos antagonistas; contratar expertos como consultores, el caso de Leonard Adleman para “Sneakers”, se emplea para crear de nuevo un guión con ideas cercanas a la realidad que son explicadas como si un científico loco de una película de terror tomase el escenario, y eso teniendo en cuenta que en esa película se busca un cierto realismo.

No podemos decir que es una disciplina totalmente maltratada en el cine, puesto que he encontrado buenos ejemplos de tratamiento, pero sí que se une al resto de disciplinas técnicas que no reciben la atención que deberían. El espectáculo, la acción, la intriga y las tramas que avanzan incansablemente son objetivos que están por encima, en general, de las explicaciones detalladas sobre cómo funciona un cifrado. En los anteriores análisis he encontrado ejemplos de todo tipo, por supuesto, y hay muchas producciones que dedican un mínimo de cuidado a que las cosas suenen verdaderas y se muestren cercanas a una realidad comprensible. “Cipher bureau” o ”Rendezvous” muestran una parte del trabajo de las oficinas de cifrado y se entretienen en el análisis de frecuencia, añadiendo un toque James Bond al trabajo de los agentes para compensar. Las películas que se ocupan de la Enigma parten de hechos históricos verdaderos y hablan de la máquina con cierto detalle incorporando acción o giros de guion poco probables. Los cifrados mas cercanos a los juegos infantiles, como la tinta invisible, la transposición o la sustitución simple reciben una exposición más detallada gracias a la cercanía con el espectador. Las películas de aventuras, como “La búsqueda” o las basadas en el universo de Sherlock Holmes se atreven a llegar un poco más lejos porque el espectador espera que en el ADN de esas producciones haya elementos enigmáticos que necesitan de cierto tiempo de análisis, como se esperarían de forma natural en un videojuego o en una ‘escape room’. A pesar de que el sentido del espectáculo prima en todas estas producciones, podemos extraer conocimiento de cada una de ellas, con esfuerzo e implicación por supuesto, pero si las matemáticas generales tienen difícil reflejo en el cine, ¿qué se podía esperar de una disciplina como la criptografía?

Hay un elemento importante que está detrás de varias de las conclusiones extraídas hasta ahora y es el tiempo. El metraje de una producción cinematográfica es limitado y dedicarle una gran parte del mismo a explicaciones muy técnicas reduce la posibilidad de todo lo demás, de todo lo que convierte al cine en cine en todas su épocas: la acción y la trama (y no hablo de acción en el sentido Bond, todo en el cine es acción). En producciones más largas, con más tiempo y más exposición, las explicaciones y los detalles pueden interferir menos en el resto de elementos y es lo que ocurre con las series o los videojuegos. En las primeras, la mayor extensión de metraje permite flexibilidad a la hora de presentar conceptos, y ahí tenemos ejemplos como “Rubicon”, “The Wire” o “Mr Robot” que merecerían estudios detallados. En los segundos, el tiempo depende del jugador, y los enigmas y los principios detrás de los mismos están en variados casos extraídos de la criptografía.

Las conclusiones no son negativas si se revisan los análisis anteriores y se piensa en el amplio volumen de material pendiente de analizar. Son aún menos negativas si conecto este análisis con el segundo objetivo de este trabajo, la realización de un proyecto didáctico. Hay tantos conceptos representados en las películas analizadas, con mayor o menor detalle, que muchos de ellos pueden emplearse como parte de un proceso de enseñanza, partiendo tanto de aquello que está bien explicado como de aquello erróneo. El cine puede servir como punto de partida para enseñar y analizar la criptografía, ya que muestra desde usos más estrafalarios de conceptos hasta usos más cotidianos, sin olvidar las representaciones históricas. Este aspecto es realmente importante puesto que me permite no desechar los análisis anteriores aunque en muchos casos se queden a medias en la función de definir con detalle temas relacionados con la criptografía. Los datos están ahí, en mayor o menor medida, y permiten profundizar, generar curiosidad y extender conocimiento.

Como enlace entre las dos partes de este trabajo, la de análisis cinematográfico y la divulgativa, acabaré este capítulo mostrando dos timelines sencillos, uno con conceptos criptográficos y otro con películas donde se pueden encontrar algunos de esos conceptos. Esto abrirá la puerta para definir mi idea de un proyecto didáctico sobre la disciplina utilizando el cine y otros medios.

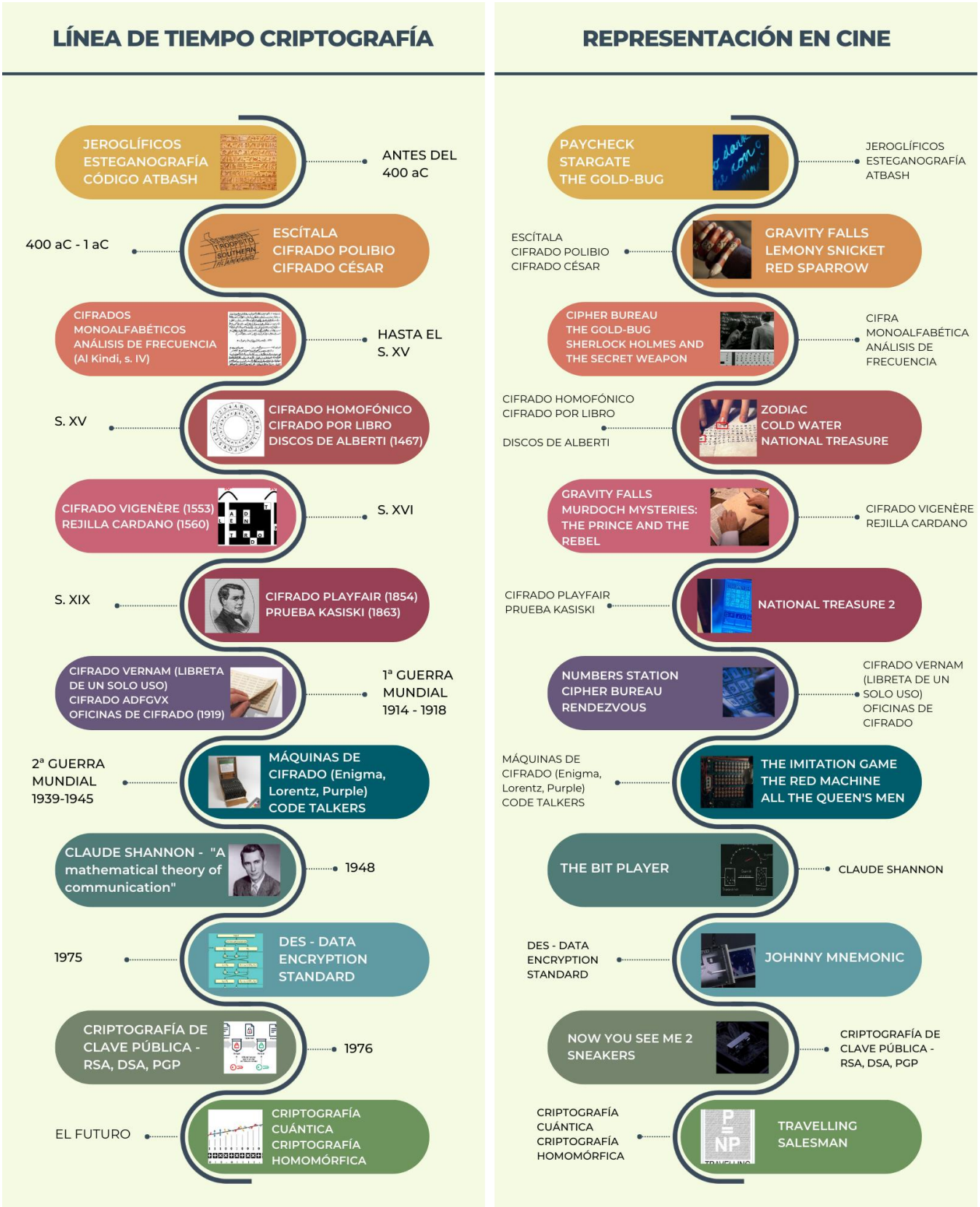


Figura 79: Líneas de tiempo

6. PROYECTO DIDÁCTICO

En este capítulo se detalla de forma esquematizada el proyecto didáctico que forma parte de los objetivos previstos en el TFM. Los diferentes aspectos que se discutirán son la descripción del curso, el público que pudiera recibirlo, materiales y elementos de evaluación y un listado de los temas. Acabaré con el detalle de uno de los temas en forma de unidad didáctica.

6.1. Descripción general del curso

Esta ficha presenta el diseño de un curso de introducción a la historia de la criptografía, partiendo del cine y otros medios. Por un lado, se presenta la historia de los códigos y cifrados desde las culturas antiguas hasta el siglo XXI, presentando los principios detrás de esta necesidad de disponer de comunicaciones secretas. Por el otro, no se puede olvidar la guerra constante entre criptografía y criptoanálisis y se discutirán algunos métodos para romper estos códigos y cifrados. Por último, se conectan estas ideas con cuestiones propias de la era Internet como secreto, privacidad y seguridad.

La base del curso serán elementos de los medios de masas y culturales (cine, series, libros, videojuegos) que permitirán conectar los conceptos con explicaciones más o menos detalladas en función de los objetivos del formato de curso. Los ejercicios girarán también alrededor de estos elementos de la cultura popular, que se analizarán y compararán, y también de búsquedas más teóricas o actividades de opinión y debate.

6.2. Público destinatario del curso

El principio general detrás de este curso es que sea adaptable a diferentes tipos de público. El tema puede tratarse desde diferentes perspectivas y profundizando más o menos en función de la audiencia. En primer lugar, se puede considerar como una serie de conferencias independientes que presenten diferentes temas relacionados con la criptografía a partir de películas u otros elementos propios de la cultura de masas. En segundo lugar, se puede partir de esas conferencias para construir un programa enlazado de un curso completo en una asociación o centro de actividades; en este caso se podrían añadir algunas actividades complementarias para que los asistentes hagan en casa. En tercer lugar, se puede presentar como un curso optativo en ESO o Bachillerato que sirva para presentar la materia a alumnos de diferentes edades; en la actualidad, tanto la ESO como el Bachillerato potencian la existencia de asignaturas optativas fuera de las troncales que permitan desarrollar competencias dentro de marcos de actividad más concretos. Desde una misma base se pueden

desarrollar programas variados con enfoques específicos que permitan entender las bases de la criptografía a un público amplio no necesariamente técnico.

6.3. Competencias generales

Las competencias generales que se trabajarán son las siguientes, aunque dependerán del tipo de curso que se plantee:

1. Plantear problemas y formular preguntas que se pueden responder a partir de la investigación.
2. Usar el lenguaje técnico propio de la materia para interpretar y transmitir información.
3. Relacionar conocimientos, ideas y habilidades con otros que provengan de disciplinas distintas.
4. Analizar textos, imágenes y vídeos.
5. Elaborar textos y otros elementos comunicativos para presentar ideas y reflexiones.
6. Valorar las aportaciones propias y ajenas en las diferentes actividades del curso.

6.4. Objetivos del curso

Los objetivos principales del curso son los siguientes, pero se pueden ajustar en función del público destinatario y de la extensión:

1. Conocer la historia de la criptografía y el valor de las comunicaciones secretas a lo largo de la historia.
2. Comprender la relación entre criptografía y criptoanálisis y los avances en ambas disciplinas.
3. Analizar la presentación de conceptos criptográficos en libros, películas y otros elementos de la cultura de masas.
4. Debatir sobre temas generales como el impacto de la criptografía en conflictos históricos, la privacidad en la vida actual, o los caminos futuros de las disciplinas criptográficas.

6.5. Actividades de evaluación

En general el curso tendrá una serie de actividades más o menos evaluables en función del planteamiento del mismo, ya que no es lo mismo impartirlo para participantes de un centro de actividades que para alumnos de ESO o Bachillerato.

Las actividades propuestas serían las siguientes:

1. Debates centrados en temas como la privacidad y la necesidad de cifrar la información, la "guerra" constante entre criptografía y criptoanálisis o la representación de determinados conceptos criptográficos en películas.
2. Análisis de películas o series y relación con conceptos criptográficos o momentos de la historia de la criptografía.
3. Análisis de la adaptación al cine de técnicas de criptografía empleadas en novelas. El objetivo del ejercicio sería realizar un estudio comparativo.
4. Según el tipo de curso, un examen parcial.

6.6. Distribución de contenidos del curso completo

Partiendo de la breve historia de la criptografía del apartado 2 y de las líneas de tiempo elaboradas en el apartado anterior, he construido un programa dividido en 10 temas. Por cuestiones de tiempo y de alcance de este TFM no he detallado los contenidos de cada tema, pero creo que los títulos son razonablemente explicativos y su contenido se puede relacionar con la mencionada historia del apartado 2.

TEMA 1: ¿Qué es la criptografía? Relación con la esteganografía y los jeroglíficos.

TEMA 2: De la escítala a las cifras vikingas

TEMA 3: Cifrados por transposición

TEMA 4: Cifrado de sustitución monoalfabético. Análisis de frecuencia.

TEMA 5: EL camino hacia el cifrado polialfabético.

TEMA 6: Cifrado de sustitución polialfabético.

TEMA 7: Primera Guerra Mundial y años posteriores.

TEMA 8: Segunda Guerra Mundial.

TEMA 9: Criptografía Moderna I. La digitalización de la información y la criptografía de clave simétrica.

TEMA 10: Criptografía Moderna II. Criptografía de clave simétrica y el futuro de la criptografía.

6.7. Materiales generales del curso

Los materiales generales del curso son los siguientes:

1. Diversos capítulos sobre libros de historia de la criptografía como los que aparecen en las primeras referencias de la bibliografía.
2. Películas: una parte es el listado analizado en los apartados previos de este trabajo.
3. Series de televisión: es necesario realizar un análisis previo de series equivalente al que hecho con las películas.
4. Novelas y cuentos: "El escarabajo de oro" de Poe, "Viaje al centro de la Tierra" de Verne, cuentos y novelas de Conan Doyle, "Johnny Mnemonic" de Gibson, "La clave está en Rebeca" de Follet, "Criptonomicón" de Stephenson, entre otros.
5. Documentales: es necesario realizar un análisis previo equivalente al hecho con las películas.

6.8. Detalle de unidad didáctica de ejemplo

Voy a detallar una de las unidades didácticas o temas como ejemplo de lo que podría ser el curso completo. Por cuestiones de espacio y duración de este TFM me resulta muy difícil detallar todas las unidades, así que he tomado el tema 4 con el fin de desarrollarlo pensando en un público de Bachillerato. Estoy suponiendo que es una optativa con 2 horas a la semana de clase y un total de 40 horas, por tanto, a cada tema se le pueden dedicar en principio 4 horas. Se trata de un plan aproximado que habría que ajustar a la organización real de un curso de Bachillerato.

Tema 4: Cifrado de sustitución monoalfabético. Análisis de frecuencia.

Temporización: 4h.

Objetivos básicos:

1. Entender qué es el cifrado de sustitución monoalfabético y cómo funciona.
2. Entender el contexto histórico en el que aparece.
3. Diferenciar diferentes tipos de cifrado monoalfabético: cifrado César, cifrado con palabra clave o libro código, cifrado Atbash, el cifrado francmasón.
4. Entender el criptoanálisis de este cifrado.
5. Aplicar el análisis de frecuencias a un texto sencillo.

Evaluación específica:

1. Ejercicio de análisis de una película que contenga este cifrado
2. Ejercicio de análisis de frecuencias.
3. Dos actividades secundarias
    a. tipos de cifrado
    b. frecuencias de aparición de letras del español, catalán, francés e inglés.

Distribución horaria de contenidos y actividades

Hora	Contenidos	Actividades
1	• Fragmento de "Sherlock Holmes and the Secret Weapon". • Explicación sobre el cifrado de sustitución monoalfabético y el contexto histórico.	Distribuir diferentes tipos de cifrado monoalfabético entre los alumnos para que investiguen sobre ellos.
2	• Puesta en común de los diferentes tipos de cifrado. • Fragmentos de “Gravity Falls”. • Explicación del cifrado Cesar y el cifrado por palabra clave o libro código.	Análisis de una película que contenga un cifrado de sustitución monoalfabético.
3	• Puesta en común breve del análisis de la película. • Explicación del cifrado Atbash y el cifrado francmasón. • Muestra de un fragmento de gameplay de “Assassin's Creed II”, donde aparece el cifrado francmasón para resolver un puzle. • Contexto histórico del análisis de frecuencias y explicación inicial.	Búsqueda de las frecuencias de aparición de las letras en español, catalán, inglés y francés.
4	• Fragmento de “Cipher Bureau”. • Aplicación del análisis de frecuencias a un texto sencillo. • Resumen general del tema.	Análisis de frecuencias de un texto.

7. CONCLUSIONES Y TRABAJO FUTURO

Para estas conclusiones finales recupero las preguntas iniciales que han guiado el desarrollo de este trabajo: ¿Cómo ha representado el cine esa historia de la criptografía? ¿Se encontrarán reflejos fidedignos gracias a los cuales se puedan aprender algunos conceptos? ¿O será un uso muy funcional y más cercano a la ficción necesaria para hacer avanzar una trama? A partir de ellas voy a guiar esta reflexión de cierre y sugerir futuros desarrollos para este trabajo.

He analizado un número razonable de películas, 60, aunque he visto algunas más que aparecían referenciadas en diferentes fuentes pero que en realidad no contenían elementos de interés directo. En estas 60 películas he encontrado una gran variedad de temas, de conceptos y de referencias a la criptografía y al criptoanálisis. Puedo dividir esas producciones en cuatro grupos:

- Tendríamos un primer grupo, en el que la documentación utilizada no llega a la versión final que se proyecta, pero hay un cuidado y un interés por buscar la verosimilitud. En esos casos hay películas como "Enola Holmes", "Sneakers", "Sherlock Holmes: Juego de Sombras" o "Viaje al centro de la Tierra". Esta última abre también el capítulo de las adaptaciones de novelas o relatos que utilizan la criptografía y muestran el variado respeto que existe por las fuentes originales en función de la producción que veamos.
- En un segundo grupo se juega con el enigma y el misterio como vehículo en el que insertar algún elemento criptográfico porque así la atracción que se genera en el espectador es más importante; aquí tendríamos películas como "El código Da Vinci", "La búsqueda" o "The message".
- Un tercer grupo importante son las que presentan un periodo histórico destacable, como las películas que hablan de la Segunda Guerra Mundial o los biopics.
- Finalmente, en un último grupo, la representación de la criptografía moderna es mucho más limitada puesto que se basa en algoritmos de difícil representación y de teorías matemáticas que necesitarían mucho tiempo de pantalla para ser explicadas. No obstante, he encontrado algunos ejemplos que sirven para reflexionar alrededor de la criptografía moderna, sus implicaciones y otras evoluciones futuras.

Recuperando las conclusiones del apartado 5.5, estas son las ideas principales:

- El cine hace una representación limitada de conceptos criptográficos puesto que no se encuentran demasiadas películas que los empleen y porque las explicaciones técnicas se supeditan a la acción y a la trama.

- El tiempo es un factor importante a la hora de considerar esta representación. Las películas tienen una duración muy limitada y se intenta que las explicaciones detalladas no distraigan de la trama y de la acción principal.
- Como se ha visto en la clasificación de películas anterior, hay una gran variabilidad de casos y aquellos elementos criptográficos que se pueden integrar mejor con desarrollos históricos o forman parte natural de tramas, como en las películas de aventuras, disfrutan de más tiempo de exposición y más explicaciones.
- Una gran mayoría de los ejemplos analizados pueden utilizarse desde un punto de vista educativo puesto que son un buen punto de partida para analizar conceptos o para aprender de ellos.

En resumen, respecto a las preguntas iniciales, la respuesta es que la casuística es variada. La representación de los conceptos criptográficos está supeditada a la trama puesto que son elementos de apoyo, y a la vez se puede aprender de ellos. Se encuentran reflejos fidedignos de ciertos conceptos, pero también hay usos muy funcionales y limitados a parte de tramas de misterio. De la misma manera hay representaciones gráficas que buscan el realismo junto a otras que se saltan cualquier explicación con un mínimo de sentido. Pero el análisis de esas 60 películas me permite ser razonablemente positivo respecto a la presencia de suficientes elementos como para poder construir a partir de ellos explicaciones más extensas. Y eso formaba parte también de este trabajo: encontrar el contenido suficiente como para poderlo utilizar como recurso para un curso de historia de la criptografía.

El trabajo futuro debería dirigirse a profundizar en las siguientes áreas:

- Realizar un nuevo visionado más profundo de las películas analizadas para extraer más detalles. Este trabajo que se presenta aquí ha pretendido apoyarse en ver el mayor volumen posible de películas posible en el tiempo limitado del que se disponía, sacrificando en algunos casos la profundización. En una segunda fase de análisis, se puede trabajar en esta dirección.
- Ver y analizar las películas de la lista que no han podido formar parte de este trabajo, más de 30. Estos films pueden proporcionar nuevos elementos de juicio y servir también como recursos para el programa educativo.
- Seguir buscando en la filmografía producciones que contengan elementos criptográficos para hacer crecer esa lista y que sea lo más completa posible. Esta búsqueda debería también insistir en filmografías de otros países además de Estados Unidos, buscando en el cine asiático, por ejemplo, un camino que no ha sido fácil en esta primera fase del trabajo. El estudio de estas nuevas producciones permitirá también refinar los criterios que se están aplicando, aplicarlos a las ya vistas y reconstruir los análisis globales, y profundizar en

ellos. En esta revisión de criterios también se puede considerar la adición de otros que puedan ser relevantes.

- Elaborar material audiovisual: un vídeo conteniendo las escenas más interesantes de las películas analizadas, que sirva como apoyo para el proyecto didáctico y como apoyo a un segundo nivel de análisis en profundidad sobre las películas.
- Profundizar en la descripción del proyecto didáctico para el que habría que detallar todos los temas, los recursos y materiales y crear todas las unidades didácticas con el fin de poder ponerlo en marcha en alguno de los ámbitos que he definido en este trabajo.
- Convertir este trabajo en un libro de carácter divulgativo que exponga la relación entre la criptografía y el cine. Desde un punto personal, creo que se trata de un proyecto muy estimulante y sobre el cual me gustaría centrarme en un futuro muy próximo si el tiempo y la oportunidad me lo permiten.

8. GLOSARIO DE TÉRMINOS

Anagrama: proceso de transposición de las letras de un texto en claro para obtener un texto que oculta el mensaje original.

Cifrado: transformación de una pieza de información, denominada texto claro, en otra ininteligible (texto cifrado) empleando un procedimiento y clave determinados.

Cifrado de clave pública o asimétrico: sistema en el que se usan claves distintas para cifrar y descifrar, y parte de la clave es conocida (clave pública) mientras que otra parte no lo es (clave privada). Empleará normalmente algoritmos de cifrado basados en problemas matemáticos de alta complejidad (problemas NP) que no pueden resolverse en un tiempo realista con las capacidades computacionales actuales.

Cifrado de clave privada o simétrico: sistema en el que usa la misma clave para cifrar y descifrar la información, clave que permanece en secreto.

Cifrado de sustitución: cifrado en el que cada letra del texto en claro se sustituye por otra letra o signo en el texto cifrado.

monoalfabético: cada letra se ve siempre sustituida por la misma empleando un único alfabeto de cifrado.

polialfabético: se utilizan varios alfabetos de cifrado por lo que cada letra o conjunto de letras se va a cifrar con un alfabeto diferente.

Cifrado por transposición: cifrado en el que las letras o las unidades de texto que se definan cambian su posición según un esquema determinado.

Código: sistema de ocultación de información en el que conjuntos de letras son transformados en otros conjuntos arbitrarios de letras o símbolos.

Criptoanálisis: técnica de transformación de un texto cifrado en texto claro sin conocer la clave secreta y/o el modo.

Criptografía: técnica de transformar un texto usando una clave secreta para que sea inteligible únicamente para aquellos que conozcan el modo de descifrado y la clave.

Criptología: ciencia que estudia el cifrado de la información, de los sistemas que lo realizan. También se ocupa del proceso inverso, el de la obtención de la información sin conocer claves o sistemas.

Curva elíptica, algoritmo: algoritmo empleado por la criptografía de curva elíptica. Se trata de un sistema de clave pública desarrollado en 1985 que, basándose en el problema del logaritmo discreto en curvas elípticas, permite el uso de claves más cortas que RSA.

DES: algoritmo de clave privada desarrollado en 1975 y adoptado como estándar en Estados Unidos hasta que fue desencriptado en 1999.

DSA: algoritmo de clave pública para la firma (autenticación) de mensajes estandarizado por el NIST (National Institute for Standards and Technology) en 1994.

Entropía: la cantidad de información necesaria para enviar y recibir un mensaje con precisión, teniendo en cuenta el nivel de incertidumbre respecto a lo que el mensaje enviado podría decir.

Estación de números (numbers station): emisoras de radio de onda corta de origen indeterminado. Transmiten voces generadas de forma artificial que leen secuencias de números, letras, código morse o datos en general. Su origen se sitúa en el periodo de la Primera Guerra Mundial y se relacionan con servicios de inteligencia.

Esteganografía: conjunto de técnicas que permite la ocultación de mensajes dentro de otros elementos portadores, ya sean estos inteligibles o no.

Función de un solo sentido (one-way function): función matemática fácil de calcular en un sentido, pero muy difícil en el contrario.

Jeroglífico: sistema de escritura formado por símbolos y figuras que representan palabras o ideas. Aunque en el momento de su creación y uso no había un principio de ocultación de la información, el proceso de descifrado de estos sistemas ha implicado técnicas muy similares a las que se enmarcan dentro del criptoanálisis.

Libreta de un sólo uso (One-time Pad): cifrado manual basado en una libreta en la que cada página contiene una clave a utilizar con un mensaje y después de su uso será destruida.

Libro de claves: documento que contiene las claves que se utilizarán en un sistema durante un tiempo determinado.

Rejilla: cartón o papel en el que se recortan huecos para dejar una serie de espacios en blanco en los que se puede escribir un determinado mensaje que luego se completa alrededor con un texto portador inteligible.

RSA: Rivest, Shamir y Adleman; desarrollado en 1979, es un sistema de cifrado de clave pública en el que la seguridad la proporciona el problema de la factorización de números enteros grandes.

Texto cifrado: texto resultante de aplicar una operación de cifrado a un texto claro.

Texto claro: texto con significado dentro del idioma o código que se esté utilizando.

9. BIBLIOGRAFÍA

[1] Singh, Simon (2000). Los códigos secretos. Madrid: Debate.

[2] García Carmona, Joaquín (2011). *Tratado de criptografía con aplicación especial al ejército*. Madrid: Ministerio de Defensa.

[3] Kahn, David (1996). *The Codebreakers. The comprehensive history of secret communication from the ancient times to the internet.* New York: Touchstone.

[4] Bauer, Craig P. (2016). *Secret history. The story of cryptology.* London: Chapman & Hall/CRC.

[5] Bauer, Craig P. (2019). *Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies.* New Jersey: Princeton University Press.

[6] Sorando, José María (2015). *Aventuras matemáticas en el cine*. España: Guadalmazán.

[7] Sorando, José María (2016). *Cine y matemáticas: Resolviendo problemas*. España: Guadalmazán.

[8] Sorando, José María (2020). Matemáticas de cine. España: Guadalmazán.

[9] Polster Burkard & Ross Marty (2012). *Math goes to movies.* Baltimore: Johns Hopkins University Press.

[10] von Hallberg Robert (2015). *The Maltese Falcon to Body of Lies: Spies, Noirs and Trust*. New Mexico: University of New Mexico Press.

[11] Hackman Michael (2005). *Citizen Spy: Television, Espionage and Cold War Culture.* Minnesota: University of Minnesota Press.

[12] Thomson, Patricia (2015). Decoding a legacy. *American Cinematographer, vol. XCVI, núm. 1,* páginas 22, 24, 26, 28.

[13] Argy, Stephanie (2009). Post Focus. Creating a Stylized Caper. *American Cinematographer, vol. 90, núm. 10,* páginas 76-80.

[14] Macnab Geoffrey (2001). Peeping Tommies. *Sight and Sound, vol. 11, num. 10,* páginas 16-18.

[15] Krapp Peter (2019). Beyond Schlock on Screen: Teaching the History of Cryptology Through Media Representations of Secret Communications. *Proceedings of the 2nd International Conference on Historical Cryptology,* páginas 79-85.

[16] Kelly M.J. (2016). *Six times encryption made it to the movies*. Encontrado en <https://blog.mozilla.org/en/products/firefox/six-times-encryption-made-it-to-the-movies/>

[17] *Four movies about the enigma machine*. Encontrado en <https://www.cliomuse.com/the-enigma-machine--four-movies-about-the-enigma-machine.html>

ANEXO I. LISTADO DE PELÍCULAS

Título	Año	Concepto criptográfico	Momento histórico	Link Filmaffinity / IMDB	Duración (minutos)
The bit player	2018	Claude Shannon	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film856897.html	90
Infinity (Hasta la eternidad)	1996	No hay nada relevante	Siglo XX	https://www.filmaffinity.com/es/film183634.html	119
The Gold-bug (El escarabajo de oro) (TV)	1980	Cifrado de sustitución monoalfabético, análisis de frecuencia	Siglo XIX	https://www.filmaffinity.com/es/film345014.html	45
Sherlock Holmes and the secret weapon (Sherlock Holmes y el arma secreta)	1942	Cifrado de sustitución monoalfabético	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film492304.html	68
The adventures of Sherlock Holmes - The dancing men	1984			https://www.imdb.com/title/tt0506449/	52
Sherlock: The blind banker (TV) (El banquero ciego)	2010			https://www.filmaffinity.com/es/film428114.html	89
Sherlock: The final problem (TV) (El problema final)	2017			https://www.filmaffinity.com/es/film256690.html	89
Sherlock Holmes and the Valley of Fear	1983	Cifrado por libro	Comienzos del siglo XX	https://www.imdb.com/title/tt0238597/	50
The triumph of Sherlock Holmes (El valle del miedo)	1935			https://www.filmaffinity.com/es/film534464.html	85
Batman: Gotham by gaslight (Gotham a luz de gas)	2018	Cifrado de sustitución monoalfabético	Siglo XIX	https://www.filmaffinity.com/es/film929762.html	78
Red Sparrow (Gorrión Rojo)	2018	Escítala	Contemporánea	https://www.filmaffinity.com/es/film650565.html	134
13 hours: the secret soldiers of Bengazhi (13 horas: los soldados secretos de Bengasi)	2016	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film438949.html	144
The key to Rebecca (La clave está en Rebeca)	1985			https://www.filmaffinity.com/es/film664634.html	180
Johnny Mnemonic	1995	Cifrado simétrico	Contemporánea (ciencia ficción)	https://www.filmaffinity.com/es/film222381.html	96
Gone in 60 seconds (60 segundos)	2000	Esteganografía (tinta invisible)	Contemporánea	https://www.filmaffinity.com/es/film331228.html	117
Sneakers (Los fisgones)	1992			https://www.filmaffinity.com/es/film233071.html	126

Midway (La batalla de Midway)	1976	Captura de mensajes cifrados que supone una ventaja táctica	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film914270.html	132
Midway (Midway)	2019	Captura de mensajes cifrados que supone una ventaja táctica	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film765932.html	138
Rendezvous	1935	Descifrado de mensajes como ventaja militar - polialfabético, esteganografía	Primera Guerra Mundial	https://www.filmaffinity.com/es/film744138.html	94
Sphere (Esfera)	1998	Código de sustitución monoalfabético - teclado en espiral	Contemporánea	https://www.filmaffinity.com/es/film556710.html	134
Windtalkers	2002	Code talkers	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film957874.html	133
Zodiac	2007	Código de sustitución homofónico	Años 70	https://www.filmaffinity.com/es/film300908.html	158
Harry Potter and the Chamber of Secrerts (Harry potter y la cámara secreta)	2002	Anagrama	Contemporánea / mundo alternativo en el que existe la magia	https://www.filmaffinity.com/es/film952728.html	154
Swordfish (Operación Swordfish)	2001			https://www.filmaffinity.com/es/film857439.html	99
Cipher Bureau	1938	Oficina de cifrado / Análisis de frecuencia	Entre las dos grandes guerras	https://www.filmaffinity.com/es/film577998.html	64
Panama Patrol	1939			https://www.filmaffinity.com/es/film856727.html	67
The imitation game (Descifrando Enigma)	2014	Enigma / Alan Turing	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film617730.html	114
Pi: faith in chaos (Pi: fe en el caos)	1998		Contemporánea	https://www.filmaffinity.com/es/film679822.html	85
Wargames (Juegos de guerra)	1983			https://www.filmaffinity.com/es/film553168.html	114
Mercury Rising (Al rojo vivo)	1998	Buscar expertos en criptoanálisis mediante pasatiempos	Contemporánea	https://www.filmaffinity.com/es/film830550.html	112
U-571	2000	Enigma	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film188131.html	116
The numbers station (Código de defensa)	2013	Las emisoras de números / Libreta de un solo uso	Contemporánea	https://www.filmaffinity.com/es/film213318.html	88
National Treasure (La búsqueda)	2004	Código libro, tinta invisible	Contemporánea	https://www.filmaffinity.com/es/film721724.html	121

National Treasure 2: Book of secrets (La búsqueda 2: El diario secreto)	2007	Sistema de sustitución bigrámico (Playfair), jeroglíficos	Contemporánea	https://www.filmaffinity.com/es/film372637.html	124
Blackhat (Amenaza en la red)	2015			https://www.filmaffinity.com/es/film271983.html	133
Hackers (Hackers, piratas informáticos)	1995			https://www.filmaffinity.com/es/film347629.html	95
The net (La red)	1995			https://www.filmaffinity.com/es/film822846.html	112
The matrix reloaded	2003	No hay nada relevante	Futuro indefinido	https://www.filmaffinity.com/es/film349820.html	138
Who am I - Kein system is sicher (Ningún sistema es seguro)	2014	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film604935.html	102
The Bourne ultimatum (El ultimatum de Bourne)	2007			https://www.filmaffinity.com/es/film560336.html	111
Live free or die hard (La jungla 4.0)	2007	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film748998.html	130
Män som hatar kvinnor (Millennium I) (Millenium I: los hombres que no amaban a las mujeres)	2009			https://www.filmaffinity.com/es/film675920.html	145
Fant4stic (Cuatro fantásticos)	2015	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film375488.html	100
Lemony Snicket's A Series Of Unfortunate Events (Una serie de catastróficas desdichas de Lemony Snicket)	2004	Escítala	Contemporánea	https://www.filmaffinity.com/es/film931362.html	103
The Da Vinci code (El código Da Vinci)	2006	Esteganografía / Anagramas	Contemporánea	https://www.filmaffinity.com/es/film306442.html	147
Crypto	2019			https://www.filmaffinity.com/es/film941795.html	105
From Russia with love (Desde Rusia con amor)	1963	Máquina lektor - versión dramatizada de la Enigma	Guerra Fría - años 50/60	https://www.filmaffinity.com/es/film823940.html	118
For your eyes only (Sólo para sus ojos)	1981	No hay nada relevante	Años 80	https://www.filmaffinity.com/es/film311420.html	127
The falcon and the snowman (El juego del halcón)	1985	Venta de códigos de cifrado	Guerra Fría - años 70	https://www.filmaffinity.com/es/film654188.html	131
Les vampires (Los vampiros)	1915	Cifrado por transposición, anagrama, código de	Años 20	https://www.filmaffinity.com/es/film208840.html	420

		sustitución			
The nine tailors	1974			https://www.imdb.com/title/tt0071024/	50
Revelation (Revelación)	2001			https://www.filmaffinity.com/es/film298939.html	111
Travelling Salesman	2012	Problema P vs NP	Contemporánea	https://www.filmaffinity.com/es/film567822.html	80
The red machine	2009	Descifrar una máquina Red	Años 30	https://www.filmaffinity.com/es/film215538.html	84
Cold weather	2010	Cifrado por libro	Contemporánea	https://www.filmaffinity.com/es/film449124.html	96
Stargate (Stargate, puerta a las estrellas)	1994	Jeroglíficos	Contemporánea	https://www.filmaffinity.com/es/film687980.html	121
Los crimenes de Oxford	2008	Segunda Guerra Mundial - Criptoanalistas	Contemporánea	https://www.filmaffinity.com/es/film509927.html	110
Bridge of spies (El puente de los espías)	2015			https://www.filmaffinity.com/es/film255419.html	135
Rebellion (serie)	2016			https://www.filmaffinity.com/es/film234651.html	250
Enigma	2001			https://www.filmaffinity.com/es/film361882.html	114
Hunt	2022	Cifrado con "tabla de Polibio"	Años 80	https://www.filmaffinity.com/es/film502702.html	125
The man who new infinity (El hombre que conocía el infinito)	2015	No hay nada relevante	Primera Guerra Mundial	https://www.filmaffinity.com/es/film476371.html	104
Snowden	2016	Cifrado vs Privacidad	Contemporáneo	https://www.filmaffinity.com/es/film892502.html	134
Sebastian	1968	Oficina de cifrado / Análisis de frecuencia	Años 60	https://www.filmaffinity.com/es/film856116.html	100
Black Kiss	2004			https://www.filmaffinity.com/es/film328239.html	133
Safe	2012			https://www.filmaffinity.com/es/film653956.html	94
Alien Code	2017			https://www.imdb.com/title/tt5453522/	97
Knowing (Señales del futuro)	2009	No hay nada relevante	Contemporáneo	https://www.filmaffinity.com/es/film391856.html	130
Tora Tora Tora	1970			https://www.filmaffinity.com/es/film240724.html	143
The silent war	2012	Frecuencias de transmisión de mensajes	Años 50	https://www.filmaffinity.com/es/film256225.html	120
The message	2009	Uso del morse con la lengua china y cifrado de sustitución	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film360678.html	117

Paycheck	2003	Esteganografía (micropunto)	Contemporánea	https://www.filmaffinity.com/es/film260686.html	114
Viaje al centro de la tierra	1976	Cifrado por transposición	Siglo XIX	https://www.filmaffinity.com/es/film502547.html	90
Viaje al centro de la tierra	1959	No hay nada relevante	Siglo XIX	https://www.filmaffinity.com/es/film505460.html	127
The Prestige (El truco final)	2006			https://www.filmaffinity.com/es/film343841.html	130
Dope	2015	Criptomonedas	Contemporánea	https://www.filmaffinity.com/es/film200755.html	103
Sharpe's sword (La espada de Sharpe)	1995	Cifrado por libro	Siglo XIX	https://www.filmaffinity.com/es/film872899.html	101
The Fifth State	2013			https://www.filmaffinity.com/es/film746598.html	124
All the queen's men	2001	Enigma	Segunda Guerra Mundial	https://www.imdb.com/title/tt0252223/	99
The final countdown (El final de la cuenta atrás)	1985	Códigos con caducidad	Años 80	https://www.filmaffinity.com/es/film231849.html	105
Gravity Falls	2012-2016	Cifrados César, Vigenère - esteganografía	Contemporánea	https://www.filmaffinity.com/es/film999825.html	20
A Christmas story (Historias de navidad)	1983	Cifrado de sustitución monoalfabético - anillos decodificadores	Años 80	https://www.filmaffinity.com/es/film483694.html	94
Murdoch Mysteries: The prince and the rebel	2008	Rejilla de Cardano	Siglo XIX	https://www.imdb.com/title/tt1214506/	48
The Thomas Beale cipher	2010	Los Papeles Beale (cifrado por libro)	Segunda Guerra Mundial	https://www.imdb.com/title/tt1669827/	10
The man who never was (El hombre que nunca existió)	1956	Secráfono	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film131218.html	103
A beautiful mind (Una mente maravillosa)	2001	Captura de mensajes - John Nash	Guerra Fría	https://www.filmaffinity.com/es/film326587.html	130
Now you see me 2 (Ahora me ves 2)	2016	Máquina de desencriptado universal / Tinta invisibles	Contemporánea	https://www.filmaffinity.com/es/film897797.html	129
Con air (Convictos en el aire)	1997			https://www.filmaffinity.com/es/film890214.html	115
The fourth protocol (El cuarto protocolo)	1987	Rejilla de Cardano	Años 80	https://www.filmaffinity.com/es/film356698.html	119
Dirty Harry (Harry el Sucio)	1971			https://www.filmaffinity.com/es/film571114.html	102
Manhunter (Hunter)	1986	Cifrado por libro	Años 80	https://www.filmaffinity.com/es/film249119.html	118

Enola Holmes	2020	Cifrado por transposición, cifrado de sustitución	Siglo XIX	https://www.filmaffinity.com/es/film656850.html	123
Enola Holmes 2	2022	Esteganografía, cifrado por libro, anagrama	Siglo XIX	https://www.filmaffinity.com/es/film927350.html	129
Aelita	1924	Cifrado de sustitución (mensaje del espacio)	Principios siglo XX	https://www.filmaffinity.com/es/film961986.html	120
Sherlock Holmes: A game of shadows (Sherlock Holmes. Juego de Sombras)	2011	Cifrado por libro	S XIX	https://www.filmaffinity.com/es/film937637.html	129
Sekret Enigmy	1979			https://www.filmaffinity.com/es/film152522.html	158
Contact	1997	Cifrado de sustitución	Contemporáneo	https://www.filmaffinity.com/es/film815526.html	150
Alien Hunter	2003			https://www.filmaffinity.com/es/film635384.html	87
The amateur (Servicios secretos paralelos)	1981			https://www.filmaffinity.com/es/film526208.html	112
Breaking the code	1996			https://www.filmaffinity.com/es/film681479.html	75
Cube	1997	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film741341.html	92
First circle	1991			https://www.imdb.com/title/tt0101885/	180
A man called intrepid (Un hombre llamado intrépido)	1979			https://www.filmaffinity.com/es/film985780.html	300
Summer Wars	2009	RSA	Contemporánea	https://www.filmaffinity.com/es/film222123.html	114
The good shepherd (El buen pastor)	2006			https://www.filmaffinity.com/es/film911702.html	160
La piel del tambor	2022	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film911702.html	116
Mary Queen of Scots (María, reina de Escocia)	2018	No hay nada relevante	Siglo XVI	https://www.filmaffinity.com/es/film396709.html	124
Interstellar	2014	No hay nada relevante	Contemporánea	https://www.filmaffinity.com/es/film704416.html	169
Operation Mincemeat (El arma del engaño)	2021	No hay nada relevante	Segunda Guerra Mundial	https://www.filmaffinity.com/es/film261551.html	128
Eye of the needle (El ojo de la aguja)	1981	No hay nada relevante	Años 80	https://www.filmaffinity.com/es/film585050.html	112

ANEXO II. PELÍCULAS ANALIZADAS

Película	Género	Año	País	Duración (min)	Concepto principal	Definición	Funcionamiento	Representación gráfica	Avance trama	Reutilización	Referencias mkt
A BEAUTIFUL MIND (UNA MENTE MARAVILLOSA)	Drama	2001	Estados Unidos	130	Guerra Fría. Interceptar comunicaciones y claves	Parcial	No mostrado	Dramatizada	Sí	Sí	Sí
A CHRISTMAS STORY (HISTORIAS DE NAVIDAD)	Comedia	1983	Estados Unidos	94	Sustitución monoalfabético	Indefinido	Correcto	Realista	No	No	No
AELITA, QUEEN OF MARS	Ciencia ficción	1924	Unión Soviética	111	Códigos espaciales	Indefinido	No mostrado	Dramatizada	Sí	Sí	Sí
ALL THE QUEEN'S NAME	Comedia	2001	Alemania	99	Máquina Enigma	Definido	Impreciso	Neutra	Sí	Sí	Sí
BATMAN GOTHAM BY GASLIGHT (BATMAN GOTHAM A LUZ DE GAS)	Animación	2018	Estados Unidos	78	Sustitución monoalfabético	Indefinido	No mostrado	Realista	Sí	No	No
CIPHER BUREAU	Thriller	1938	Estados Unidos	64	Oficinas de cifrado	Definido	Impreciso	Dramatizada	Sí	Sí	Sí
CIPHER BUREAU	Thriller	1938	Estados Unidos	64	Cifrado por transposición	Definido	Impreciso	Neutra	Sí	Sí	No
COLD WEATHER	Drama	2010	Estados Unidos	96	Cifrado por libro	Definido	Correcto	Realista	Sí	Sí	No
CONTACT	Ciencia ficción	1997	Estados Unidos	150	Códigos espaciales	Parcial	Impreciso	Neutra	Sí	No	No
DOPE	Comedia	2015	Estados Unidos	103	Criptomonedas	Parcial	No mostrado	Neutra	Sí	Sí	No
EL ESCARABAJO DE ORO	Aventuras	1999	España	81	Tinta invisible	Definido	Impreciso	Dramatizada	Sí	Sí	Sí
ENOLA HOLMES	Thriller	2020	Reino Unido	123	Cifrado por transposición	Parcial	Correcto	Realista	Sí	Sí	Sí
ENOLA HOLMES	Thriller	2020	Reino Unido	123	Sustitución monoalfabético	Indefinido	Incorrecto	Dramatizada	Sí	No	Sí
ENOLA HOLMES 2	Thriller	2022	Reino Unido	129	Mensaje oculto	Indefinido	Correcto	Realista	Sí	No	No
ENOLA HOLMES 2	Thriller	2022	Reino Unido	129	Cifrado por libro	Definido	Impreciso	Dramatizada	Sí	Sí	No
ENOLA HOLMES 2	Thriller	2022	Reino Unido	129	Anagrama	Indefinido	Correcto	Realista	Sí	No	No
FROM RUSSIA WITH LOVE (DESDE RUSIA CON AMOR)	Thriller	1963	Estados Unidos	118	Máquina Enigma	Definido	No mostrado	Dramatizada	Sí	Sí	Sí

GONE IN 60 SECONDS (60 SEGUNDOS)	Thriller	2000	Estados Unidos	117	Tinta invisible	Definido	Correcto	Realista	Sí	Sí	No
GRAVITY FALLS	Animación	2012	Estados Unidos	22	Sustitución monoalfabético	Indefinido	No mostrado	Dramatizada	No	No	No
GRAVITY FALLS	Animación	2012	Estados Unidos	22	Sustitución polialfabético	Indefinido	No mostrado	Dramatizada	No	No	No
GRAVITY FALLS	Animación	2012	Estados Unidos	22	Tinta invisible	Definido	Correcto	Realista	Sí	Sí	No
HARRY POTTER AND THE CHAMBER OF SECRETS (HARRY POTTER Y LA CÁMARA SECRETA)	Aventuras	2002	Reino Unido	154	Anagrama	Indefinido	Correcto	Realista	Sí	No	No
HUNT	Thriller	2022	Corea del Sur	125	Sustitución monoalfabético	Indefinido	No mostrado	Dramatizada	Sí	Sí	No
JOHNNY MNEMONIC	Ciencia ficción	1995	Estados Unidos	96	Cifrado simétrico	Parcial	Impreciso	Dramatizada	Sí	Sí	No
LEMONY SNICKET'S A SERIES OF UNFORTUNATE EVENTS (UNA SERIE DE CATASTRÓFICAS DESDICHAS DE LEMONY SNICKET)	Aventuras	2004	Estados Unidos	103	Escítala	Indefinido	Impreciso	Dramatizada	Sí	No	No
LEMONY SNICKET'S A SERIES OF UNFORTUNATE EVENTS (UNA SERIE DE CATASTRÓFICAS DESDICHAS DE LEMONY SNICKET)	Aventuras	2004	Estados Unidos	103	Sustitución monoalfabético	Parcial	Correcto	Realista	Sí	No	No
LES VAMPIRES (LOS VAMPIROS)	Thriller	1915	Francia	421	Cifrado por transposición	Indefinido	Correcto	Realista	Sí	No	No
LES VAMPIRES (LOS VAMPIROS)	Thriller	1915	Francia	421	Anagrama	Indefinido	Correcto	Dramatizada	Sí	Sí	No
LES VAMPIRES (LOS VAMPIROS)	Thriller	1915	Francia	421	Sustitución monoalfabético	Indefinido	No mostrado	Neutra	Sí	No	No
LOS CRÍMENES DE OXFORD	Thriller	2008	España	110	Segunda Guerra Mundial	Definido	No mostrado	Dramatizada	Sí	Sí	Sí
MANHUNTER (HUNTER)	Thriller	1986	Estados Unidos	118	Cifrado por libro	Parcial	Impreciso	Dramatizada	Sí	No	No

MERCURY RISING (AL ROJO VIVO)	Thriller	1998	Estados Unidos	112	Buscar criptoanalistas con pasatiempos en prensa	Parcial	Correcto	Dramatizada	Sí	Sí	Sí
MIDWAY	Bélico	2019	Estados Unidos	138	Segunda Guerra Mundial	Definido	No mostrado	Dramatizada	Sí	Sí	Sí
MIDWAY (LA BATALLA DE MIDWAY)	Bélico	1976	Estados Unidos	132	Segunda Guerra Mundial	Parcial	Impreciso	Dramatizada	Sí	Sí	No
MURDOCH MYSTERIES: THE PRINCE AND THE REBEL	Thriller	2008	Canadá	48	Rejilla de Cardano	Definido	Correcto	Realista	Sí	Sí	No
NATIONAL TREASURE (LA BÚSQUEDA)	Aventuras	2004	Estados Unidos	121	Tinta invisible	Parcial	Correcto	Realista	Sí	Sí	No
NATIONAL TREASURE (LA BÚSQUEDA)	Aventuras	2004	Estados Unidos	121	Cifrado por libro	Definido	Correcto	Realista	Sí	Sí	No
NATIONAL TREASURE 2 (LA BÚSQUEDA 2)	Aventuras	2007	Estados Unidos	124	Cifrado Playfair	Parcial	Impreciso	Realista	Sí	Sí	No
NATIONAL TREASURE 2 (LA BÚSQUEDA 2)	Aventuras	2007	Estados Unidos	124	Jeroglíficos	Parcial	Impreciso	Realista	Sí	Sí	No
NOW YOU SEE ME 2 (AHORA ME VES 2)	Thriller	2016	Estados Unidos	129	Tinta invisible	Indefinido	Correcto	Realista	Sí	Sí	No
NOW YOU SEE ME 2 (AHORA ME VES 2)	Thriller	2016	Estados Unidos	129	Máquina de desencriptado universal	Indefinido	No mostrado	Dramatizada	Sí	No	Sí
PAYCHECK	Thriller	2003	Estados Unidos	114	Micropunto	Indefinido	Correcto	Realista	Sí	No	No
RED SPARROW (GORRIÓN ROJO)	Thriller	2018	Estados Unidos	134	Escítala	Indefinido	Correcto	Realista	Sí	Sí	No
RENDEZVOUS	Bélico	1935	Estados Unidos	94	Primera Guerra Mundial	Definido	Impreciso	Neutra	Sí	Sí	Sí
SEBASTIAN	Drama	1968	Reino Unido	100	Oficinas de cifrado	Definido	Impreciso	Dramatizada	Sí	Sí	Sí
SHARPE'S SWORD (LA ESPADA DE SHARP)	Bélico	1995	Reino Unido	101	Cifrado por libro	Definido	Impreciso	Neutra	Sí	Sí	No

SHERLOCK HOLMES AND THE SECRET WEAPON (SHERLOCK HOLMES Y EL ARMA SECRETA)	Thriller	1943	Estados Unidos	68	Sustitución monoalfabético	Definido	Impreciso	Neutra	Sí	Sí	Sí
SHERLOCK HOLMES AND THE VALLEY OF FEAR (SHERLOCK HOLMES Y EL VALLE DEL MIEDO)	Animación	1983	Australia	50	Cifrado por libro	Definido	Impreciso	Dramatizada	Sí	Sí	No
SHERLOCK HOLMES: A GAME OF SHADOWS (SHERLOCK HOLMES: JUEGO DE SOMBRAS)	Thriller	2011	Estados Unidos	129	Cifrado por libro	Parcial	No mostrado	Dramatizada	Sí	No	No
SNEAKERS (LOS FISGONES)	Thriller	1992	Estados Unidos	126	Máquina de desencriptado universal	Definido	No mostrado	Dramatizada	Sí	Sí	Sí
SNOWDEN	Drama	2016	Estados Unidos	134	Cifrado vs Privacidad	Definido	Impreciso	Neutra	Sí	Sí	Sí
SPHERE (ESFERA)	Ciencia ficción	1998	Estados Unidos	134	Sustitución monoalfabético	Parcial	Impreciso	Dramatizada	Sí	Sí	No
STARGATE (STARGATE, PUERTA A LAS ESTRELLAS)	Ciencia ficción	1994	Estados Unidos	121	Jeroglíficos	Definido	Impreciso	Neutra	Sí	Sí	Sí
SUMMER WARS	Animación	2009	Japón	114	RSA	Indefinido	Impreciso	Dramatizada	Sí	Sí	No
THE BIT PLAYER	Documental	2018	Estados Unidos	90	Claude Shannon	Definido	Correcto	Realista	Sí	Sí	Sí
THE DA VINCI CODE	Thriller	2006	Estados Unidos	147	Tinta invisible	Definido	Correcto	Realista	Sí	Sí	Sí
THE FALCON AND THE SNOWMAN (EL JUEGO DEL HALCÓN)	Bélico	1985	Estados Unidos	131	Guerra Fría. Interceptar comunicaciones y claves	Indefinido	No mostrado	Dramatizada	Sí	Sí	No
THE FINAL COUNTDOWN (EL FINAL DE LA CUENTA ATRÁS)	Bélico	1985	Estados Unidos	105	Códigos en desuso	Indefinido	No mostrado	Dramatizada	No	No	No
THE FOURTH PROTOCOL (EL CUARTO PROTOCOLO)	Thriller	1987	Reino Unido	119	Rejilla de Cardano	Indefinido	Impreciso	Realista	Sí	No	No

THE GOLDBUG TV SPECIAL (El ESCARABAJO DE ORO ESPECIAL TELEVISIÓN)	Aventuras	1980	Estados Unidos	45	Sustitución monoalfabético	Definido	Correcto	Dramatizada	Sí	No	No
THE IMITATION GAME (DESCIFRANDO ENIGMA)	Drama	2015	Reino Unido	114	Máquina Enigma	Definido	Correcto	Dramatizada	Sí	Sí	Sí
THE MAN WHO NEVER WAS (EL HOMBRE QUE NUNCA EXISTIÓ)	Bélico	1956	Reino Unido	103	Secráfono	Parcial	Impreciso	Realista	Sí	No	No
THE MESSAGE	Thriller	2009	China	117	Código Morse y la lengua china	Definido	Impreciso	Neutra	Sí	No	Sí
THE NUMBERS STATION (CÓDIGO DE DEFENSA)	Thriller	2013	Reino Unido	88	Estación de números	Definido	Impreciso	Dramatizada	Sí	Sí	Sí
THE NUMBERS STATION (CÓDIGO DE DEFENSA)	Thriller	2013	Reino Unido	88	Sustitución polialfabético	Parcial	No mostrado	Realista	Sí	Sí	Sí
THE NUMBERS STATION (CÓDIGO DE DEFENSA)	Thriller	2013	Reino Unido	88	Mensaje oculto	Indefinido	Correcto	Realista	Sí	No	No
THE RED MACHINE	Bélico	2009	Estados Unidos	84	Máquina Red	Definido	Impreciso	Realista	Sí	Sí	Sí
THE SILENT WAR	Thriller	2012	Hong Kong	120	Frecuencias de transmisión	Definido	Impreciso	Dramatizada	Sí	Sí	Sí
THE THOMAS BEALE CIPHER	Thriller	2010	Estados Unidos	10	Cifrado por libro	Definido	No mostrado	Dramatizada	Sí	Sí	Sí
TRAVELLING SALESMAN	Ciencia ficción	2012	Estados Unidos	80	Problema P vs NP	Definido	No mostrado	Neutra	Sí	Sí	Sí
U-571	Bélico	2000	Estados Unidos	116	Máquina Enigma	Parcial	No mostrado	Neutra	Sí	Sí	Sí
VIAJE AL CENTRO DE LA TIERRA	Aventuras	1976	España	90	Cifrado por transposición	Indefinido	Impreciso	Neutra	Sí	No	No
WINDTALKERS	Bélico	2002	Estados Unidos	133	Code Talkers	Definido	No mostrado	Dramatizada	Sí	Sí	Sí
ZODIAC	Thriller	2007	Estados Unidos	158	Sustitución homofónico	Parcial	Impreciso	Realista	Sí	Sí	Sí