Criptografía y Cine

De la libreta de Turing a la pantalla ¿Como ve el cine la criptografía?

Roberto Magán Parro

Máster Universitario en Ciberseguridad y Privacidad.

Protocolos criptográficos y aplicaciones de Seguridad.

Tutor/a de TF

Rafael Páez Reyes

Profesor/a responsable de la asignatura

Andreu Pere Isern Deyà

Junio 2023

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*De la libreta de Turing a la pantalla ¿Como ve el cine la criptografia?*
Nombre del autor:	*Roberto Magán Parro*
Nombre del consultor/a:	*Rafael Páez Reyes*
Nombre del PRA:	*Andreu Pere Isern Deyà*
Fecha de entrega:	*06/2023*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad.
Área del Trabajo Final:	*Protocolos criptográficos y aplicaciones de Seguridad.*
Idioma del trabajo:	*Castellano*
Palabras clave:	*cinematografía, criptografía, criptología, cine*

Resumen del Trabajo

La criptografía, que nace más como labor de artesanía o artística que como ciencia, ha ganado en nuestros días especial importancia debido, sobre todo, a la excepcional expansión que han experimentado las comunicaciones, actividades y transacciones basadas en mecanismo y dispositivos electrónicos. Nunca, en ningún momento anterior de nuestra historia, las interacciones, tanto personales como profesionales, económicas o comerciales habían sido tan numerosas, complejas y comunes, ni habían comportado tantos riesgos para la privacidad y la confidencialidad.

Junto a las múltiples oportunidades que esta interconexión y tránsito de información nos ofrece, también han florecido, como no podía ser de otra forma, las amenazas. Y con ellas la necesidad de preservar la privacidad, confidenciales e integridad tanto en los canales como y sobre todo de la información que por ellos transita.

El cine, arte que nació empeñándose en atrapar y conservar embellecida la realidad que nos rodea, no podía dejar de emplear la criptografía en su discurso; bien sea como herramienta o decorado bien como interprete secundario o principal.

El objetivo de este trabajo es analizar como esta disciplina se ha visto reflejada en el cine y cuan correcta ha sido la interpretación.

Abstract

Cryptography, which was born more as a craft or artistic work than as a science, has gained special importance nowadays, mainly due to the exceptional expansion experienced by communications, activities and transactions based on electronic mechanisms and devices. Never before in our history have interactions, both personal

and professional, economic and commercial, been so numerous, complex and common, nor have they entailed so many risks to privacy and confidentiality.

Along with the multiple opportunities that this interconnection and transit of information offers us, threats have also flourished, of course. And with them the need to preserve the privacy, confidentiality, and integrity of both the channels and the information that passes through them.

Cinema, an art that was born with the aim of capturing and preserving the reality that surrounds us, could not fail to use cryptography in its discourse, either as a tool or a set, or as a secondary or main interpreter. The objective of this work is to analyze how this discipline has been reflected in the cinema and how correctly it has been.

Índice

Lista de Figuras

Lista de Tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

Criptografía (de cripto- y -grafía.)

"1.f. Arte de escribir con clave secreta o de un modo enigmático." (Real Academia Española, s.f., definición 1) *(Real Academia Española 2014)*

"La criptografía (del griego κρύπτος (kryptós), «secreto», y γραφή (graphé), «grafo» o «escritura», literalmente «escritura secreta») se ha definido, tradicionalmente, como el ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados" *(Wikipedia 2023)*

Parece probable que desde el momento en que la humanidad comenzó a comunicarse empleando grupos de símbolos escritos además de hacerlo con su voz, surgiese la necesidad de ocultar parcial o totalmente algunos de esos grupos con el objetivo de hurtarlos a miradas indeseadas o indiscretas. No parece pues descabellado pensar entonces, que la criptografía, de una forma u otra y con mayor o menor acierto forma parte de la historia humana desde hace tanto tiempo como lo tienen nuestros primeros escritos.

Del cine no podemos decir lo mismo; aunque creo que el deseo y la necesidad de contar historias forma parte de nuestra esencia, no es hasta bien avanzada la edad moderna cuando aparece el cine para ayudarnos en esta tarea y añadir a la palabra, hablada o escrita, la riqueza adicional de la música y las imágenes.

Como aficionado al cine y neófito interesado en criptografía, la propuesta de contribuir en el análisis de la combinación de ambos me resultó muy atractiva desde el mismo momento en que supe que existía tal posibilidad.

El presente ejercicio trata pues de revisar como el cine se acerca a la criptografía y determinar cuan acertada o fallida resulta esta representación y si esta última es capaz de convertirse en protagonista o no deja de ser un elemento más de los decorados entre los que transcurre la verdadera acción.

Para alcanzar lo mencionado, he fijado los objetivos que se describen en el epígrafe siguiente.

1.2. Objetivos del Trabajo

Los objetivos del presente son los incluidos a continuación

- Analizar la importancia que algo ajeno y alejado del lenguaje cinematográfico, como es la criptografía, puede contribuir en el desarrollo de una historia, en algunos casos de manera significativa.

  Con lo anterior pretendo contribuir, de manera modesta, a entender cómo pueden llegar a relacionarse diferentes disciplinas,

desbordando lo que en teoría son sus áreas de aplicación naturales para contribuir al desarrollo de otras.

- Analizar y mostrar la influencia que una determinada tecnología o la resolución de un problema, tenía en el entorno y el momento en el que se desarrolla la película.

  Así por ejemplo en el caso de Enigma, el uso de la tecnología empleada por los nazis resultaba crucial en el aseguramiento de sus comunicaciones y, por tanto, en el desarrollo de sus operaciones. Por el contrario, el esfuerzo y ruptura final del código por parte de los polacos en primer lugar y los británicas más tarde, tuvo gran influencia en los esfuerzos que finalmente llevarían a los países aliados a la victoria en el conflicto; especial importancia tuvo este hecho, la ruptura del código, en la guerra que se desarrolló en el atlántico norte y que mientras las comunicaciones fueron seguras apuntaba a un desenlace diferente.

  Con todo lo anterior se pretende mostrar la importancia de una disciplina como la criptografía.

- Contribuir a determinar cuan ajustadas y realistas son las representaciones que de la criptografía es capaz de hacer el cine. Tal y como indica *Robert Krapp: "The problem with audiovisual representations of cybersecurity in particular and computer networks in general is that they are all too often turned into ludicrous caricatures on screen."* [1] (Krapp 2019)

  No se pretende aquí determinar si el detalle de lo incluido en las películas es completamente fiel ni represente el mecanismo utilizado con precisión matemática, más bien se analizará que sea plausible y ajustado a la realidad y no resulte ridículo. Por supuesto, allí donde se empleen cifrados clásicos *simples,* este ajuste resultará sencillo. No lo será tanto cuando se trate de dispositivos más complejos.

  Tampoco se pretende juzgar la imaginación del autor, si en alguna de las películas analizadas aparece algún mecanismo inventado o "futurista", de nuevo intentaré analizar su viabilidad hasta donde sea posible.

1.3. Impacto en sostenibilidad, ético-social y diversidad

Siendo el producto principal del presente un estudio incluyendo el resultado del análisis de los medios seleccionados y las conclusiones a las que dicho análisis conduzca, no contará con elementos susceptibles de impactar de manera positiva o negativa a la evolución medioambiental ni en la sostenibilidad. Lo único que podría destacarse es que tratándose de un trabajo presentado en formato electrónico, el coste e impacto de impresión del mismo desaparece.

[1] El problema con las representaciones audiovisuales de Ciberseguridad en particular y redes informáticas en general es que con demasiada frecuencia se convierten en la pantalla en ridículas caricaturas"

En lo que hace referencia a la diversidad, sea esta de género, raza o condición, de nuevo, no parece fácil que haya influencia sobre ella, por las mismas razones ya mencionadas antes; sí que existiría el riesgo de incurrir en incorrecciones, mayormente formales, que pudiesen afectar negativamente el producto final. Es por ello por lo que prestaré especial atención a todo lo que hace referencia al lenguaje no sexista y me aseguraré de incluir correctamente las referencias y colaboraciones que correspondan sin emplear otros criterios que no sean los de utilidad. Por ejemplo, en todo lo que hace referencia a las películas, las referencias incluirán, siempre que sea posible, los protagonistas tanto masculinos como femeninos, en caso de no contar con figuras de ambos sexos, lo anterior no será de aplicación.

De la misma forma, en aquellas referencias que sea posible y no resulte un ejercicio forzado, se realizará el esfuerzo de contribuir a visibilizar figuras que habitualmente no son mencionadas -p.e. en Bletchley Park el 75% de personal eran mujeres, es innegable pues su contribución al criptoanálisis de Enigma-.

El mismo ejercicio se realizará en relación con la nacionalidad de las películas; siempre que sea posible incluiré filmografía de diferentes nacionalidades con la intención no sólo de darles visibilidad, sino también para tratar de atenuar el sesgo que, de manera inevitable, las diferentes nacionales imprimen a sus historias.

Tratándose de un trabajo en el que la propiedad intelectual tiene un papel predominante debido a que una parte sustancial del mismo se sustenta en la visualización de películas, si incluyo aquí el compromiso de evitar el uso de copias no autorizadas de las películas; emplear imágenes de dominio público siempre que sea posible y cuando no lo sea incluir las menciones y referencias oportunas; la anterior también resulta de aplicación en todo lo que hace referencias a citas, artículos, páginas web, etc.

1.4. Enfoque y método seguido

Para cubrir los objetivos indicados en el punto correspondiente, el enfoque y metodología propuesta es la siguiente.

1.4.1. Inventario

Como punto de partida, cuento con un inventario de 20 películas

A continuación, algunas de las incluidas, el detalle completo se puede encontrar en la Tabla 2 al final del presente en el apartado correspondiente a Tablas.

- *The Imitation Game*
- *Enigma*
- *Una mente maravillosa*
- *Contacto*
- *Sneakers*
- *National Treasure (La Búsqueda)*

- *El Código Da Vinci*

Si bien el inventario se considera definitivo a-priori, es posible que, en el transcurso de la investigación, sea necesario retirar alguna de la incluidas o añadir alguna no contemplada inicialmente. Si este resultase ser el caso, así se indicará en la tabla correspondiente.

1.4.2. Análisis de la Película

Se realizará una pequeña tarea de investigación sobre cada uno de los filmes incluidos en el inventario con el objetivo de localizar información útil sobre el mismo y sobre los mecanismos criptográficos que en ella aparezcan. Esta tarea permitirá también localizar la película y determinar si, finalmente es adecuada para incluirla en el inventario definitivo o no, en caso de que no resultase adecuada, se eliminaría de dicho inventario con una breve explicación y se actualizará el inventario según corresponda.

Si en esta investigación se detectase que los mecanismos de encriptado precisan de información adicional, se buscará la misma y se localizarán fuentes, en caso de no localizar dichas fuentes, se evaluará nuevamente la conveniencia o no de mantenerla en el inventario, bien porque no se cuente con la información suficiente, bien porque no se pueda realizar el análisis con la competencia suficiente.

Como parte fundamental de este análisis se contará con una serie de criterios que serán valorados en cada una de las películas. Estos criterios no son matemáticas y no existe una formulación que los respalde, los resultados no serán por tanto exactos y estarán sometidos al criterio de quién esto escribe.

A continuación, el inventario de dichos criterios, una descripción detallada de los mismos puede encontrarse en el capítulo siguiente dedicado a materiales y métodos.

- **Criterio 1**: Papel desarrollado por la criptografía en la película, este podrá ser:
  - *Protagonista*
  - *Secundario*
  - *Actor de reparto*
  - *Extra*
- **Criterio 2:** Clasificación Técnica Criptográfica, categorizada en base a tres subcriterios.
  - *Técnica*
    - Manual
    - Mecánica (o Electromecánica)
    - Electrónica (o Matemática)
    - Cuántica (¿Futura?)
  - *¿Existe o Existió?*
    - Real
    - Inventada
  - *Corrección*

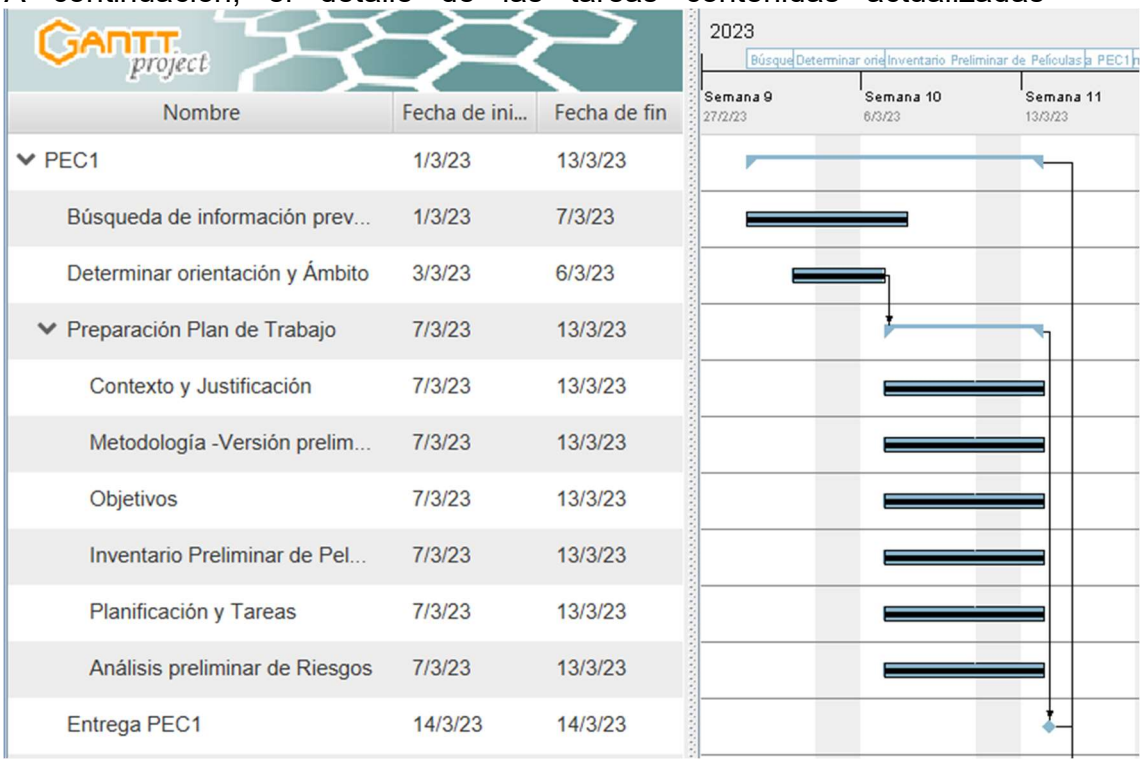
- Correcta
- Incorrecta
- Imposible de determinar

- **Criterio 3:** Influencia, entendida esta como la influencia que la técnica mostrada tuvo o puede tener en el periodo y circunstancias en las que se desarrolla la película.
  - *Alta*
  - *Media*
  - *Baja*
  - *Sin influencia*

1.5. Planificación del Trabajo

Las tareas consideradas son las incluidas en el Project que se adjunta, por supuesto se trata de una primera iteración y una planificación preliminar, en ella se puede comprobar que al menos con cada entrega se planifica una actualización de esta, sin que se puedan realizar actualizaciones adicionales siempre que así se precise

A continuación, el detalle de las tareas contenidas actualizadas



Nombre	Fecha de ini...	Fecha de fin
PEC1	1/3/23	13/3/23
Búsqueda de información prev...	1/3/23	7/3/23
Determinar orientación y Ámbito	3/3/23	6/3/23
Preparación Plan de Trabajo	7/3/23	13/3/23
Contexto y Justificación	7/3/23	13/3/23
Metodología -Versión prelim...	7/3/23	13/3/23
Objetivos	7/3/23	13/3/23
Inventario Preliminar de Pel...	7/3/23	13/3/23
Planificación y Tareas	7/3/23	13/3/23
Análisis preliminar de Riesgos	7/3/23	13/3/23
Entrega PEC1	14/3/23	14/3/23

Imagen 1 – Planificación PEC1

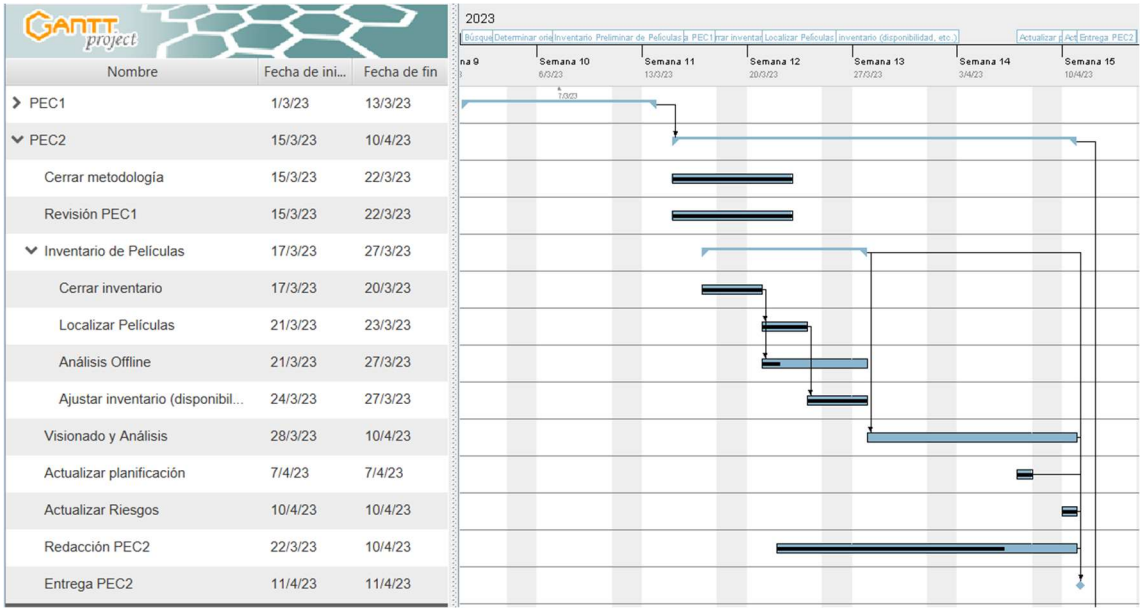


Imagen 2 – Planificación PEC2

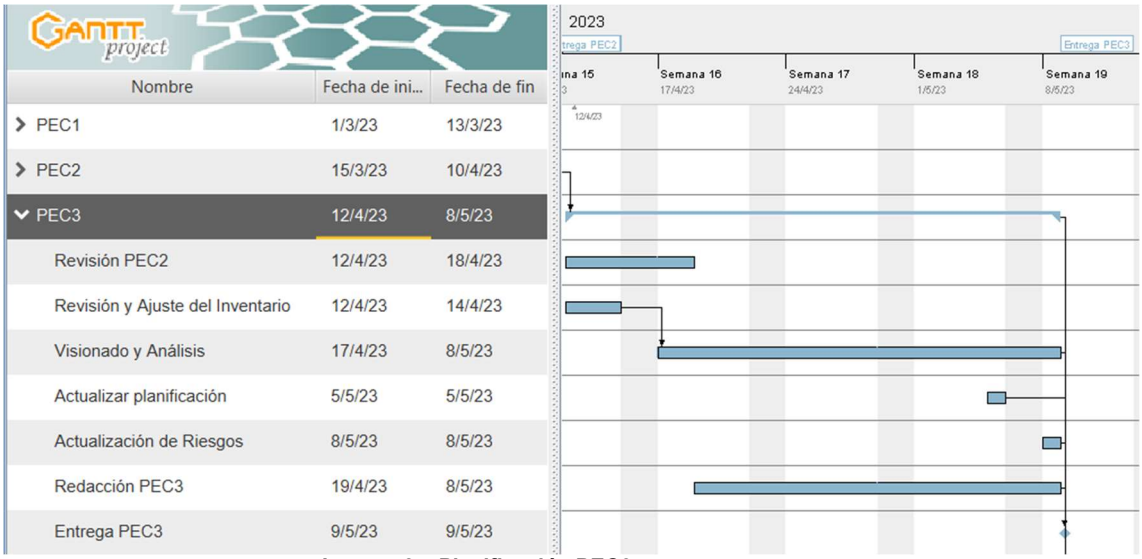


Imagen 3 – Planificación PEC3

Y el gráfico de estas

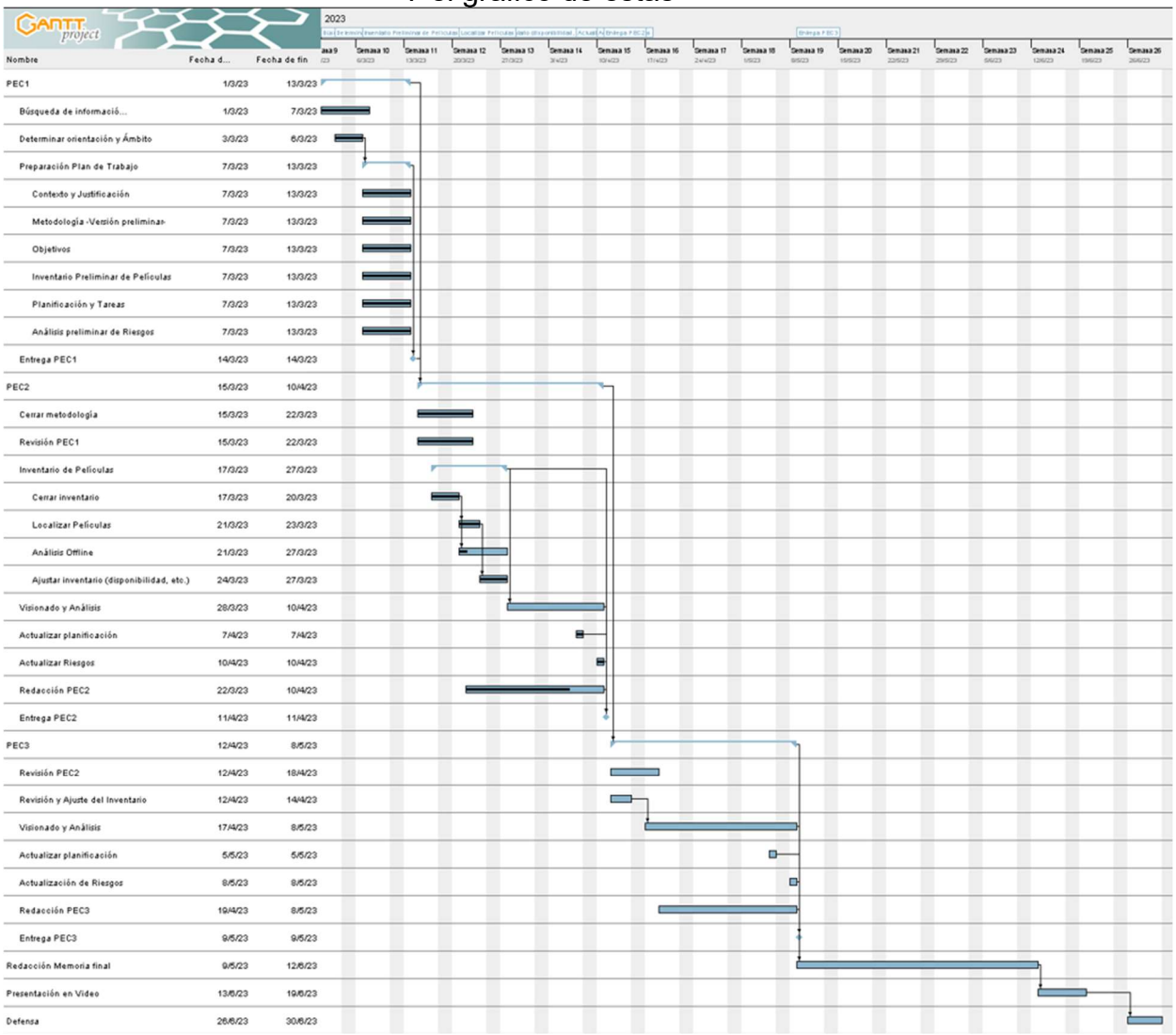


Imagen 4 – Planificación General

1.6. Análisis de Riesgos

Como todo análisis de riesgos, el ahora incluido se trata de uno inicial que deberá revisarse, enriquecerse y adecuarse según transcurra el proyecto. Dicha revisión se ha incluido como tarea en cada una de las fases y tiene como objetivo reflejar los cambios y modificaciones que puedan producirse.

El resultado se muestra en la tabla correspondiente al final del presente documento (Tabla 1)

1.7. Estado del Arte

Al plantear el presente trabajo y con la intención de situarlo en contexto y asegurar, en la medida de lo posible, que la aproximación propuesta y las ideas y conclusiones expuestas resultan novedosas, al menos parcialmente, he realizado una revisión de los trabajos anteriores en el mismo ámbito y de algunos de los artículos publicados.

Para llevar a cabo lo anterior, además de contar con la inestimable colaboración del tutor (Rafael Páez Reyes), he realizado diferentes búsquedas (se detallarán en el anexo correspondiente) tanto en buscadores tradicionales de internet (Google, Bing, etc.) como en las bases de datos de literatura académica disponibles (Google Scholar, etc.) con el objetivo de localizar materiales de referencia, películas y trabajos anteriores.

Centrando el resultado en los trabajos y artículos localizados en el momento de redactar el presente, la filmografía y obras de referencia se detallarán en los apartados correspondientes, destaco a continuación aquellos que considero reseñables; señalar que, en una fase tan temprana del trabajo, el inventario mencionado es preliminar y será depurado y ajustado según corresponda.

1. *Fajardo Rodriguez, David. Criptografía y cine. Análisis y uso didáctico de la representación de la criptografía en el cine* (FAJARDO RODRÍGUEZ 2023)

   Interesante y detallada revisión de los usos de diferentes técnicas criptográficas a lo largo de la historia y como dichas técnicas se muestran en la pantalla.

   Además de la revisión anterior, el trabajo propone el uso de diferentes películas como apoyo didáctico en la enseñanza de la criptografía.

2. *Domínguez Boiza, Carlos. Criptografía y cine: criptografía en el cine bélico.* (DOMÍNGUEZ BOIZA 2023)

   Trabajo focalizado en el uso que de la criptografía se hace en los conflictos bélicos y como el cine lo ha reflejado.

   Del análisis realizado sobre la representación de Enigma en el film *"Descifrando Enigma"* (The Imitation Game), cabe destacar la exhaustividad del mismo y el nivel de detalle expuesto.

3. *Bomfim, Fabiana de Souza. História da Matemática e Cinema: O caso da criptografia na introdução do ensino de Álgebra* (BOMFIM 2017)

   Se trata de un trabajo presentado como parte del programa para la obtención del título de Profesora de Ciencias. El trabajo analiza el uso de materiales extra como apoyo en la enseñanza de matemáticas. En este caso se centra en el uso de la criptografía como soporte en la enseñanza de álgebra y entre los ejercicios propuestos se hace uso de la película *The Imitation Game.*

4. *Krapp, Peter. Beyond schlock on screen: Teaching the history of cryptology through media representations of secret communications.* (Krapp 2019)

   Según el resumen contenido en el propio artículo, este trata sobre cómo introducir a una clase de estudiantes de humanidades en la historia de la criptología, prestando especial atención a las películas. Trata de concienciar a los estudiantes sobre la necesidad de desarrollar soluciones nuevas y creativas que permitan mostrar diferentes tecnologías (computación, redes de computadoras y ciberseguridad) de una manera precisa e informada.

5. *Sarnek, Marcin. "Cryptographer-Magician" and other modes of presence of cryptography in contemporary American cinema.* (SARNEK 2014)

   Se trata de un análisis selectivo de varias películas estadounidenses (Swordfish, Pi, Mercury Rising, U-571, Windtalkers) en términos de la presencia en las mismas de temas relacionados con la criptografía.

2. Materiales y métodos

2.1. *Inventario de películas.*

Las películas consideradas se incluyen en la tabla correspondiente al Inventario de Películas que puede encontrarse en el apartado correspondiente a Tablas (Tabla 2)

2.2. *Descripción de los criterios de análisis.*

2.2.1. Criterio 1: Papel desarrollado en la película

Paso en este punto a describir los criterios mencionados en la introducción en el apartado correspondiente a Enfoque y Método seguido (epígrafe 1.4)

- **Protagonista:** Aquellos en los que la criptografía tiene un papel "protagonista", sin ella la historia sería otra o, directamente, no sería.

  Con lo que he revisado hasta el momento, hay varias candidatas disponibles y algunas destacan: *The Imitation Game, Enigma y Sneakers*. La primera y la segunda a pesar de tener como elemento común el mismo dispositivo, tienen sin embargo y con la

información disponible por el momento al menos, diferentes formas de abordarlo; en el primer caso el protagonista indiscutible es Turing y en el segundo el propio dispositivo, Sneakers también gira alrededor del mismo eje, la criptografía y un dispositivo tan *milagroso* como lo sería *la piedra filosofal.*

- **Secundario:** Aquellos en los que la criptografía sin ser *protagonista* indiscutible actúa como secundario de lujo y elemento necesario en el avance de la trama.

  En este caso y sin contar todavía con la lista completa, incluyo películas como *Una mente maravillosa, Contact, El Código Da Vinci y National Treasury*. En ellas esta disciplina ayuda de manera evidente al avance de la trama y en otros momentos la sostiene o ayuda de manera destacada a su sostenimiento.

- **Actor de reparto.** Aquellas en las que es un elemento que ayuda en la construcción de la estructura, aún sin tener un papel preponderante, colabora con el resto. El autor la considera elemento necesario. Empleando un símil literario, el de la *Pistola de Chejov*: "*Elimina todo lo que no tenga relevancia en la historia. Si dijiste en el primer capítulo que había un rifle colgado en la pared, en el segundo o tercero este debe ser descolgado inevitablemente. Si no va a ser disparado, no debería haber sido puesto ahí" (Chéjov)* (Bill 1987) *y* (Goldberg 1976)

- **Extra:** El elemento es residual, aparece de la misma forma que los clientes de una cafetería.

2.2.2. Criterio 2: Clasificación Técnica Criptográfica

Como ya indiqué en el epígrafe 1.4, emplearé aquí tres subcriterios, que paso a describir a continuación

- **Técnica**[2]
  - *Manual:* Entendida esta como aquella que se desarrolla desde los comienzos de esta disciplina y hasta aproximadamente la primera guerra mundial. En este periodo las técnicas criptográficas y criptoanalíticas evolucionaron sin duda, pero siempre dentro de los límites establecidos por aquello que puede realizarse a mano o con la ayuda de dispositivos rudimentarios y, en gran medida, artesanos.
  - *Mecánica (o Electromecánica*): Se extiende desde poco antes del comienzo de la Primera Guerra Mundial y prácticamente hasta nuestros días. El principal exponente de este periodo son los dispositivos de rotores ampliamente empleados durante al Segunda Guerra Mundial y cuyo más famoso interprete sería Enigma, dispositivo alemán que

[2] Si bien he realizado ciertos cambios o modificaciones, esta distribución está basada en gran medida en lo incluido en la entrada correspondiente a Historia de la Criptología (History of cryptology) contenida en la Encyclopedia Britannica (SIMMONS 2022)

protagoniza al menos dos de los filmes incluidos en el inventario de películas incluido.

- *Electrónica (o Matemática):* Podemos marcar el comienzo de esta etapa en la publicación de Claude Shannon de 1948: Teoría Matemática de la Comunicación (SHANNON 1948). Hitos importantes de este periodo son la publicación de los Algoritmos DES y AES y la que es la base de la criptografría actual: Criptografía asimétrica o de clave pública.
- *Cuántica (¿Futura?):* Aunque no soy capaz de conocer el futuro, parece que -por el momento al menos- las tendencias apuntan a una diversidad de alternativas, por ejemplo: algoritmos resistentes a la computación cuántica, basados en redes o retículas (O'Neill 2020); computación confidencial, encriptación completamente homomórfica (IBM 2021), (BUCHMANN, y otros 2016)[3]. Y en cuanto a las comunicaciones, protocolos como BB84, Silberhorn, Decoy state, etc. permiten la distribución de lo que ha dado en llamar *Quantum Key Distribution (QKD)* que tratan de evitar los problemas asociados a las claves públicas[4] además de las comunicaciones basadas en el entrelazamiento cuántico[5].

  Como lo anterior acabe llevándose a la práctica y cuanto de ello acabe mostrándose en el cine, no puedo saberlo, pero, sin la menor duda, resultará interesante verlo y espero poder hacerlo; mientras tanto si algo parecido a lo anterior se muestra en alguno de las películas seleccionadas, este deberá ser el valor asignado a este segundo criterio.

- **¿Existe o Existió?.**

  Este segundo de los subcriterios, tiene la intención de diferenciar aquellos mecanismos que tengan o hayan tenido existencia real, estén en uso o no, de aquellos otros que no tengan visos de ser reales.

  Por supuesto, en el segundo caso, inventados, me enfrentaré a la complicación adicional de asignar el tercer criterio, ¿es posible determinar si un mecanismo inventado es correcto o no?; intentaré en este caso, asociar lo mostrado con alguno de los mecanismos reales y conocidos para determinar cuan cercano estaría el mecanismo inventado al real y cuan viable resulta. Si no es posible esta asociación, el tercero de los criterios no podrá ser evaluado y se optará por la tercera de las opciones incluidas.

- **Corrección**

[3] Además de los mencionados, se puede encontrar información adicional sobre lo mencionado en los enlaces siguientes:
- *Así es el futuro de la criptografía: física cuántica* (JULIÁN 2015)
- *What Is the Future of Quantum-Proof Encryption?* (GARISTO 2022)
- *The Future of Cryptographic Security in the Age of Quantum* (PEDERSEN 2021)

[4] Quantum Key Distribution (GILLIS 2022)

[5] - Científicos españoles logran comunicaciones cuánticas seguras por primera vez en el rango de las microondas (EuropaPress 2019)
- Long-distance distribution of genuine energy-time entanglement (Cuevas, y otros 2013)

Entendiendo aquí que no espero de una película una descripción detallada y matemática de los mecanismos empleados, de la misma forma que no suele ser el caso que durante una comida el director se explaye señalándonos como ha conseguido el cocinero el punto del filete que consume el protagonista, este tercer criterio se basa más en la plausibilidad o no de lo mostrado en pantalla.

Como ya he dicho más arriba en este mismo punto, no pretendo con este criterio que el mecanismo empleado sea descrito en detalle o se ajuste al cien por cien al funcionamiento real; más bien se busca que lo incluido sea correcto, o no, en lo esencial.

Como ya se ha comentado en el punto anterior, podría darse el caso de que lo exhibido fuese un mecanismo inventado, y de ser así, en este punto me encontraría con la dificultad adicional de tratar de determinar si un mecanismo no real es esencialmente correcto o no. Emplearé en este intento lo explicado en el punto anterior y, si aun así, no fuese posible, para esos casos he decidido incluir un tercer valor: *"Imposible de determinar"*

2.2.3. Criterio 3: Influencia

Para el último de los objetivos mencionados, el de la influencia en el momento y situación que refleja la película, se empleara una clasificación basada en cuatro grados:

- **Alta**: Cuando lo mostrado en la pantalla influye de manera crítica en la acción y situación que se muestra en la película. Sería el equivalente a protagonista en el primero de los criterios mencionados. Un ejemplo claro de esta influencia sería, de nuevo, Enigma y lo que significó en las operaciones aliadas durante la Segunda Guerra Mundial.
- **Media**: Si la técnica y empleo de lo mostrado en la película tiene una influencia significativa pero no crítica en la acción y situación que se muestra. Como ejemplo y sin haber realizado el visionado y análisis de la película, podría incluirse en este punto los delirios de John Nash (*"Una mente maravillosa")*, aunque estos hubiesen tenido una forma diferente, no hubiesen cambiado el hecho cierto de que sufría de *esquizofrenia paranoide*
- **Baja**: Lo mostrado en el filme si bien tiene cierta importancia, podría ser sustituido por algún otro elemento, técnica o dispositivo sin que la esencia de lo mostrado se vea afectada. Empleando de nuevo un ejemplo, el hecho de que el mensaje extraterrestre se encuentre codificado en las entrañas del número π añade intriga al guión de *Contact*, pero no dudo que Carl Sagan hubiese encontrado sin demasiados problemas un mecanismo igual de impactante y efectivo de no haber decidido emplear este.
- **Sin influencia**: Como se menciona en su equivalente del primer criterio, la presencia o no de elementos criptográficos no representa ninguna diferencia significativa en la historia reflejada.

Una vez cerrado el inventario y fijados los criterios de evaluación y valoración, el paso siguiente es el visionado de las películas

seleccionadas y su clasificación atendiendo a los mencionados criterios, también incluiré el mecanismo criptográfico empleado y una descripción de este. Si el mecanismo resultase imposible de identificar, trataré de identificar aquel o aquellos que más cercanos se encuentren y en los que el guionista o director pudiesen haberse inspirado.

2.3. Uso de la herramienta Cryptool2[6]

Siempre que sea posible y para facilitar la comprensión de los mecanismos criptográficos empleados, haré uso de la herramienta *Cryptool 2* con el objetivo de mostrar ejemplos de uso de los mostrado en la película o el mecanismo criptográfico empleado.

2.4. Buscadores y Referencias.

Otro elemento importante tanto en la construcción del inventario como en el análisis de las películas y en la búsqueda de información han sido diferentes buscadores y enlaces que relaciono a continuación.

2.4.1. Cinematográficos

- https://www.justwatch.com/es Localizar plataformas y/o enlaces en los que visionar los filmes seleccionados.
- https://www.filmaffinity.com/ Base de datos de películas
- https://www.imdb.com/ Base de datos de película

2.4.2. Académicos

- Google Académico https://scholar.google.es/
- Dialnet https://dialnet.unirioja.es/
- Academia https://www.academia.edu/
- Redalyc https://www.redalyc.org/home.oa
- Microsoft Academic: https://www.microsoft.com/en-us/research/project/academic/

2.5. Criptografía, cronología

No pretendo en este apartado hacer una revisión histórica de los diferentes métodos y herramientas que la criptografía ha venido utilizando a lo largo del tiempo; se trata más bien de una breve cronología que ayudará a situar cada uno de estos mecanismos en el momento en que fueron desarrollados o empleados, sirve también para tener una visión global de la continua evolución a la que esta disciplina se encuentra sometida.

Para completar lo anterior, incluyo también un sencillo resumen de los algoritmos empleados por los mecanismos incluidos en la cronología anterior.

[6] Los datos de la herramienta y la descarga de la misma puede realizarse desde el link siguiente: CrypTool 2 - CrypTool Portal

Ambas ilustraciones pueden encontrase en el artículo: *Evolution of encryption techniques and data security mechanisms* (SINGH y MANIMEGALAI 2015)

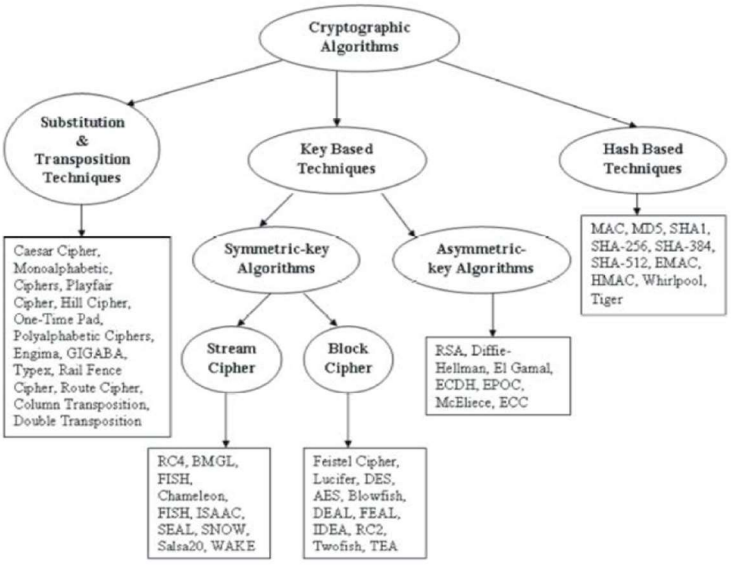


Imagen 5 – Algoritmos Criptográficos

Y a continuación la cronología.[7]

Period/Year	Name(s) of Inventors and Description of the Technique
	Classical Cryptography
Before Christ Era (BC)	•Hieroglyphic Symbols used by Egypts, 4000 BC – AD 400, to transfer religious literature and sacred writing
	•Phaistos Disks made using clay by Greeks, 1800–1600 BC, first movable type printing
	•Substitution Cipher, Steganography, Caesar Cipher by Romans - 600 BC
	•Spartans Skytale Device by Greeks, 500 BC
	Medieval Cryptography
1000 AD	•Frequency Analysis by Arabs
1467	•Cipher Disk
	•Polyalphabetic Cipher by Leon Battista Alberti used in Mechanical Cipher Machines
1585	•Vigenere by Bellaso
1795	•Jefferson Disk by Thomas Jefferson used in World War II by US Navy
1932	•Enigma used for Military Communications in World War II
	•SIGABA used in World War II by USA
	•Typex used in Rotor Machines by British
1940	•One Time Pad used in Banking initiated by Frank Miller
1942	•SIGSALY used in World War II
	Modern Cryptography
1949	•Mathematical Theory of Cryptography published by Shannon
1970	•Quantum States by Stephen Wiesner
1973	•Feistel Network Block Cipher Design by Horst Feistel
1975	•Public-key Cryptography
1976	•Key Exchange Algorithms by Diffie-Hellman-Merkel
1977	•Data Encryption Standard (DES) by USA used for enciphering PIN numbers and bank transactions
	•RSA by Ronald Rivest, Adi Shamir and Leonard Adleman, used for Secured Communication
1982	•Feynman ciphers by Richard Feynman
1984	•BB84 -First Quantum Cryptography Protocol designed by Charles Bennett and Gilles Brassard
	•Probabilistic Encryption by Shafi Goldwasser and Silvio Micali
	•Chaotic Encryption by Matthews
1994	•Peter Shor Algorithm
	•Tiny Encryption Algorithm by David J. Wheeler and Roger M. Needham
1995	•SECMPEG by Jurgen Meyer, Frank Gadegast used for Video Encryption
1996	•Zig-Zag Permutation Algorithm by Lei B. Y, Lo K. T and Haijun Lei used for Text, Image and Video Encryption
1998	•Twofish by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson
	•Quantum Cryptography
	•Video Encryption Algorithm (VEA) by Changgui Shi and Bharat Bhargava
	•MPEG Video Encryption Algorithm (MVEA) by Changgui Shi and Bharat Bhargava
1999	•Real-time Video Encryption Algorithm (RVEA) by Changgui Shi, Wang SY and Bharat Bhargava
2000	•Partial Encryption by Howard Cheng and Xiaobo Li
2001	•Advanced Encryption Standard (AES)
2003	•Frequency Domain Scrambling approach by Wenjun Zeng and Shawmin Lei
	•Selective Encryption by Xiliang Liu and Ahmet M. Eskicioglu
2005	•MHT Scheme by Chung Ping Wu and Jay Kuo C. C
2006	•Wavelet Packet Transform Algorithm by Dominik Engel and Andreas Uhl
2007	•PRESENT Algorithm by Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. Robshaw, Yanick Seurin and C. Vikkelsoe used for VLSI chip design
2009	•LCASE (Lightweight Cellular Automata-based Symmetric-key Encryption) by Somanath Tripathy and Sukumar Nandi
2010	•International Data Encryption Algorithm by Rajashekhar Modugu, Yong-Bin Kim and Minsu Choi
2011	•Humming Bird-2 by Daniel Engels, Markku-Juhani O. Saarinen, Peter Schweitzer and Eric M. Smith

Imagen 6 – Historia y Cronología de técnicas criptográficas

Siempre que se precise incluiré en las películas una descripción de los mecanismos empleados y las referencias históricas que puedan ayudar a contextualizarlos.

A continuación, y para finalizar con este apartado, incluyo una selección de artículos que me parecen particularmente interesantes por su contenido y brevedad y que realizan una excelente tarea de síntesis en lo que a la historia de la criptografía se refiere.

7 Una cronología más exhaustiva y completa puede encontrarse en el Anexo del mismo nombre del libro *Historia de la Criptografía* de *Manuel J. Prieto* (PRIETO 2020)

- *History of cryptography* (GRUSKA 2019)
- *A Brief History of Cryptography* (KOTAS 2000)
- *Evolution of encryption techniques and data security mechanisms* (SINGH y MANIMEGALAI 2015)
- *A short history of Chryptography* (COHEN 1990-1995)
- *History of cryptology* (SIMMONS 2022)

3. Análisis

3.1. The Imitation Game – Descifrando Enigma[8][9]

3.1.1. Resumen y Datos Técnicos

Película británica del año 2014. Basada en el libro de Andrew Hodges "Alan Turing: The ENIGMA" fue dirigida por Morten Tyldum e interpretada en sus principales papeles por Benedict Cumberbatch en el papel de Alan Turing y Keira Knightley en el de Joan Clarke.

Biopic sobre el matématico inglés Alan Turing, ambientada en el periodo correspondiente a la Segunda Guerra mundial y en los esfuerzos realizados por el equipo de Bletchley Park en el criptoanálisis de ENIGMA y la construcción de The Bombe.

3.1.2. Análisis

Antes de pasar a describir el funcionamiento de ENIGMA, que sin duda en esta película desempeña un papel protagonista, me gustaría repasar varios de los mecanismos criptográficos que se muestran en ella y nos ayudan a comprender la pasión por la criptografía del otro gran protagonista del filme: Alan Turing.

En la película se muestran o mencionan cuatro mecanismos criptográficos, tres de ellos resultan correctos en su descripción y uso y uno, el que aparece en segundo lugar, no he sido capaz de identificarlo, o su uso es incorrecto y hace imposible su correcta identificación.

Sin entrar en el principal de ellos, el último, que merece una descripción más detallada que se realizará posteriormente en este mismo apartado, los mencionados mecanismos son:

- Cifrado Cesar
- Cifrado desconocido, ¿posible Vigenére?
- Cifrado de Beale
- Cifrado de sustitución polialfabético mediante rotores (ENIGMA)

[8] El análisis que sigue es, probablemente el más detallado de los que se incluyen en este trabajo, los motivos para ello son, entre otros:
- Calidad de la descripción de los mecanismos criptográficos empleados en la película
- Información mostrada
- Viabilidad de reproducir los mecanismos empleados
- Existen abundantes referencias de calidad en relación con los mecanismos y dispositivos empleados.
- Importancia histórica de los mecanismos descritos y de manera principal el que hace referencia a *Enigma.*

Si el resto de los análisis no alcanzan la profundidad de este es debido a la imposibilidad o incapacidad por mi parte para localizar información o datos suficientes en algunos casos y en otros porque los mecanismos son inventados o irreales.

[9] (Cumberbatch, Knightley y Dance, y otros 2014)

El último de ellos es el principal protagonista de la película, sin embargo, resulta interesante que en la misma se incluyan conceptos adicionales de criptografía y sean estos tratados con corrección. Revisamos a continuación el tratamiento de cada uno de ellos en la película

3.1.2.1. Código Cesar

Cifrado de textos por sustitución monoalfabética; basado en el desplazamiento de las letras un número de posiciones conocido tanto por el emisor del mensaje como por el receptor de mismo.

En la película se emplea dicho mecanismo para el intercambio de mensajes entre Alan Turing y uno de sus compañeros de escuela que es quién introduce a Alan en el mundo de la criptografía y los códigos; entre ellos se establece, además, una relación amistosa y sentimental.

Se nos muestran en la película un claro mensaje cifrados empleando esta técnica:

WII CSY MR XAS PSRK AIIOW HIEVIWX JVMIRH

⇓

SEE YOU IN TWO LONG WEEKS DEAREST FRIEND

Se trata de un cifrado obtenido realizando un desplazamiento de 4 caracteres. Si empleamos Cryptool 2, el resultado tanto del cifrado como el descifrado se muestra a continuación

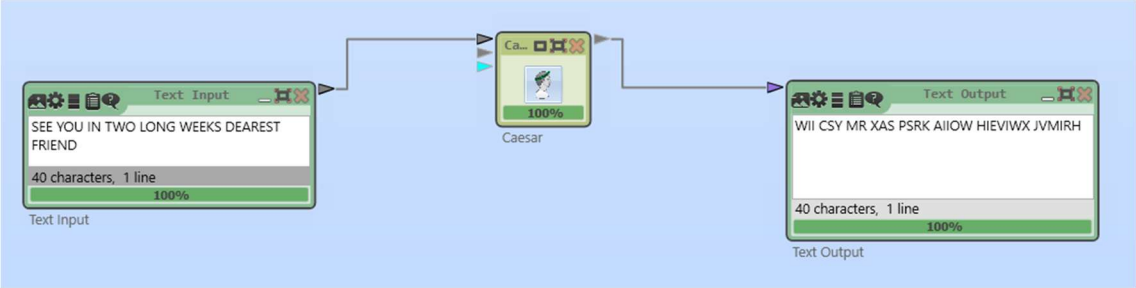


Imagen 7 – Cifrado Cesar en "Descifrando ENIGMA"

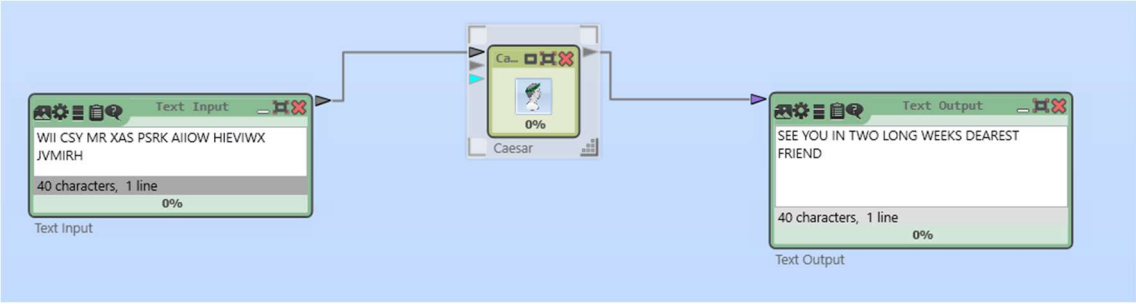


Imagen 8 – Descifrado Cesar en "Descifrando ENIGMA"

3.1.2.2. Posible Cifrado Vigenère

En la segunda ocasión en la que aparece un mensaje cifrado entre los personajes mencionados en el punto anterior, el mensaje (cifrado y descifrado) tiene el aspecto siguiente:

P ZQAE TQR

⇓

I LOVE YOU

Empleando en Cryptool el mismo tipo de cifrado que en el caso anterior, el resultado obtenido resulta, sin embargo, ilegible.

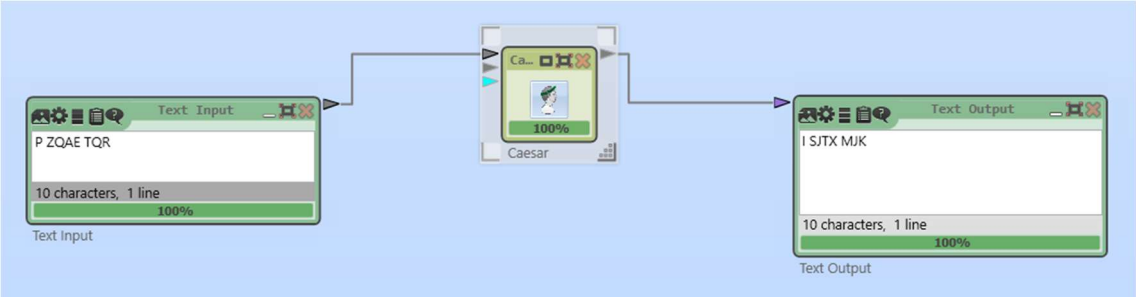


Imagen 9 – Intento de descifrado 2º mensaje -Código Cesar-

Los intentos realizados con diferentes desplazamientos no dan lugar a ningún resultado satisfactorio. Parece por tanto que en esta segunda ocasión no se trata de un código Cesar, podría tratarse de un error o una incorrección voluntaria, pero si tengo en cuenta el cuidado y cariño con el que son tratados el resto de los aspectos de la película, me resisto a creer que se trate de lo segundo y, en cuanto a lo primero, no puedo resistirme a realizar un análisis más detallado.

Podemos observar en el código mostrado un par de elementos interesantes:

- Observamos que la letra O se representa en las dos ocasiones que aparece con el mismo símbolo: Q
- La letra E no está cifrada y se muestra tanto en el mensaje en claro como en el cifrado con el mismo símbolo.

El motivo para decantarme por el uso de un código Vigenère es debido a que en las imágenes en las que se muestra a Turing descifrando el primero de los mensajes, podemos ver en la página del libro en que se apoya una rejilla de este estilo; además, en un par de imágenes del laboratorio en que trabajan los criptógrafos de Bletchley Park, podemos ver un par de pizarras con lo que sería, de nuevo, una rejilla del mismo tipo.

No obstante, lo anterior, si se trata de un código Vigenère, la clave empleada debería coincidir en ambas O con el mismo carácter de la clave o no sería posible la coincidencia (una de las razones para poner en marcha este tipo de claves es evitar un ataque por análisis de frecuencias que en este caso resultaría posible) problema aparte es la coincidencia de la letra E.

En caso de no tratarse de este tipo de código y si continúo si aceptar que se trate de un error, las posibilidades son múltiples y no cuento con indicios adicionales en la película que me permitan continuar avanzando en el análisis. Podría tratarse de diferentes códigos Cesar, aplicando uno a cada carácter individual o cualquier otro tipo.

3.1.2.3. Cifrado de Beale

Mencionado en la película tras la intercepción, por parte de los oficiales de seguridad, de un mensaje enviado, presumiblemente, por parte de uno de integrantes del equipo de Turing; al no poder identificar el libro que emplean emisor y receptor en la comunicación y desconocer, por tanto, la clave, este no puede ser leído y resulta imposible identificar al remitente, un supuesto espía ruso del que no se descarta que pueda ser el propio Turing.

No será hasta bien avanzada la película que este pequeño misterio acabe desvelándose y sea la Biblia el libro empleado en estas tareas, en particular: *"Pedid y se os dará; buscad y hallaréis". Mateo 7:7*

3.1.2.4. Encriptación electromecánica: ENIGMA[10]

Sin duda y como ya he indicado al comienzo de esta exposición, una de las protagonistas de la película y del periodo en el que se mantuvo en uso.

No es mi intención detallar de forma exhaustiva el funcionamiento de este excelente dispositivo, para ello existen multitud de libros y artículos que lo hacen con más fortuna de lo que yo sería capaz; tampoco pretendo hacerlo con el procedimiento seguido, por los polacos primero y los ingleses más tarde, en su ruptura. Me limitaré a unas pinceladas sobre su funcionamiento que ayuden a entender lo que en la película sólo se menciona.

Debemos la existencia de este dispositivo al inventor alemán Arthur Scherbius que en 1918 funda junto a su socio y amigo íntimo Richard Ritter la compañía Scherbius y Ritter que sería la responsable de inventar y fabricar los dispositivos ENIGMA, de la que la primera patente data del mismo año.

Se crearon diferentes versiones de este dispositivo, pensadas tanto para su uso militar como civil, pero sería la adopción masiva del mismo por parte del ejército alemán, su uso en la Segunda Guerra Mundial y su posterior ruptura los que harían famoso este ingenioso aparato.

ENIGMA constaba esencialmente de tres elementos, interconectados todo ellos mediante un cableado. Estos eran:

- **Teclado:** Empleado por el operador para introducir el texto que se pretende encriptar.
- **Modificador o motor de encriptación:** Encargado de modificar cada una de las letras introducidas a través del teclado.

[10] Existen múltiples fuentes en las que encontrar explicaciones detalladas, más o menos claras y comprensibles, tanto en inglés como en castellano. Sin entrar en la infinidad de ellas que podemos localizar en internet, a continuación, cuatro libros que pueden emplearse para conocer con mayor detalle el funcionamiento y operación de este dispositivo.

- (Singh 2000) p 145-218
- (Lehning 2022) p 307-337
- (PRIETO 2020) p 185-220
- (Kahn 1991)

En relación con el último de los libros, el autor David Kahn, aparecerá a su vez como “extra” en otra de las películas analizadas: Zodiac, debido a que uno de sus libros “The CodeBreakers” inspiró, al menos parcialmente, el código empleado por el asesino en serie que en ella aparece

- **Tablero de salida:** Conjunto de letras iluminadas cada una de ellas iluminada por una lámpara que muestran el carácter de entrada modificado en el motor.

Si bien existieron algunas versiones civiles que imprimían el texto de salida, sería la versión con el tablero iluminado -la que aparece en la película- la empleada por parte del ejército y armada alemanas.

Por supuesto, el componente que nos interesa de manera especial y el que describiremos en detalle es el modificador o motor de encriptación.

El núcleo principal de este motor eran varios cilindros conectados entre sí y encargados, cada uno de ellos, de realizar una modificación sucesiva al carácter introducido a través de teclado.

Cada uno de estos cilindros realizada una sustitución monoalfabética del carácter que recibía. Para ello, cada cilindro se cableaba conectando una letra de entrada con una letra diferente de salida, esta transformación era por tanto fija.

Un ejemplo posible de esta transformación sería en que se muestra en la tabla que se muestra a continuación.

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

Tabla 1: Ejemplo de sustitución rotor ENIGMA

El cableado de cada uno de los cilindros o rotores era diferente, de tal forma que la sustitución que realizaba cada uno de ellos difería de la realizada por el resto; sustitución de la que en el ejemplo anterior mostrábamos una posible.

Los operadores disponían de cinco cilindros (posteriormente se ampliarían hasta ocho) diferentes entre los que escoger, en el caso del ejército y la aviación, y ocho (posteriormente se ampliaría a diez) en el caso de la marina.

Si el sistema hubiese hecho uso de un único rotor sin más cambios o modificaciones, cada vez que se introdujese la leta A, por ejemplo, en el teclado hubiese resultado una C, este tipo de transformación es esencialmente un cifrado de sustitución monoalfabético simple, como ya indiqué más arriba, con todas las debilidades propias de este tipo de cifrado.

Se introduce aquí la primera de las mejoras, tras cada pulsación el rotor gira 1/26 de vuelta de tal forma que volver a teclear una A no dará como resultado C sino D, obtenemos de esta forma un cifrado polialfabético con relativa sencillez.

Un ejemplo de lo anterior se muestra en las tablas que siguen.

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

C

Tabla 2: Sustitución de la primera letra del texto en un rotor ENIGMA

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

Tabla 3: Sustitución de la segunda letra del texto en un rotor ENIGMA

Ahora disponemos de 26 alfabetos para encriptar el texto, se dificulta el análisis de frecuencia, sin embargo, cada 26 letras la secuencia vuelve al comenzar incrementando la posibilidad de repeticiones.

Para hacer menos frecuente esta repetición, podemos incrementar el número de cilindros o rotores, si introducimos un segundo cilindro con una sustitución diferente y que avance 1/26 de vuelta cuando el primero complete una, el número de alfabetos se multiplica por 26 y lo mismo sucederá si añadimos un tercero que se comporte como el anterior; es decir, gira 1/26 de vuelta cuando el anterior completa la suya.

De esta forma obtenemos un total de 26x26x26=17.576 alfabetos posibles para encriptar un mensaje.

Los rotores podían además colocarse en cualquier posición inicial, esta posición sería la clave con la comenzaríamos a encriptar

Sólo restarían dos componentes adicionales para completar el que sería el dispositivo ENIGMA mostrado en la película, estos son el reflector y el clavijero.

El primero de ellos se trataba de un cilindro adicional que devolvía la señal a través de los rotores, en sentido contrario en esta ocasión, es decir comenzando por el último y saliendo por el primero, no añadía complejidad adicional a la encriptación, pero era de utilidad para que se pudiese emplear el mismo sistema con las mismas configuraciones en las tareas de encriptado y desencriptado, aunque como veremos más adelante, también introducía un elemento por el que comenzar a romper el código.

El segundo y último de los componentes mencionados se trata del *clavijero*. Este elemento permitía mediante la conexión por cables entre dos letras intercambiarlas, es decir si conectásemos la **a** con la **b**, al pulsar la letra **a** en el teclado, el circuito que se activaría sería el correspondiente a la letra **b**.

El operador de ENIGMA disponía en las primeras versiones de seis de estos cables, que se incrementaría posteriormente a 10, que debía conectar siguiendo las instrucciones del libro de códigos perteneciente al día en cuestión.

Este elemento si aporta complejidad al encriptado, y no poca, e incrementa el número de diccionarios de manera significativa.

La última consideración no hace referencia a dispositivos sino a funcionalidad, los rotores eran extraíbles y podían colocarse en cualquier

orden; de nuevo una configuración que aporta complejidad al encriptado resultante.

Basta con hacer un pequeño cálculo para conocer el número total de claves que se podían conseguir con el dispositivo.

Rotores: Cada uno de los tres rotores puede situarse en 26 posiciones diferentes: 26 x 26 x 26 = 17.576
Orden de los rotores: Pueden disponerse de 6 maneras diferentes 1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, 3-2-1
Clavijero: El número de maneras de conectar, y con ello intercambiar, seis pares de letras entre 26 posibles da como resultado 100.391.791.500

Total = 17.576x6x100.391.791.500 = 10.586.916.764.424.000

Número que llevó a pensar a su inventor que el sistema resultaría imposible de descifrar (sin conocimiento de la configuración con que se operaba)

A continuación, una imagen con rotores de 6 letras que muestra gráficamente lo comentado en los párrafos anteriores.

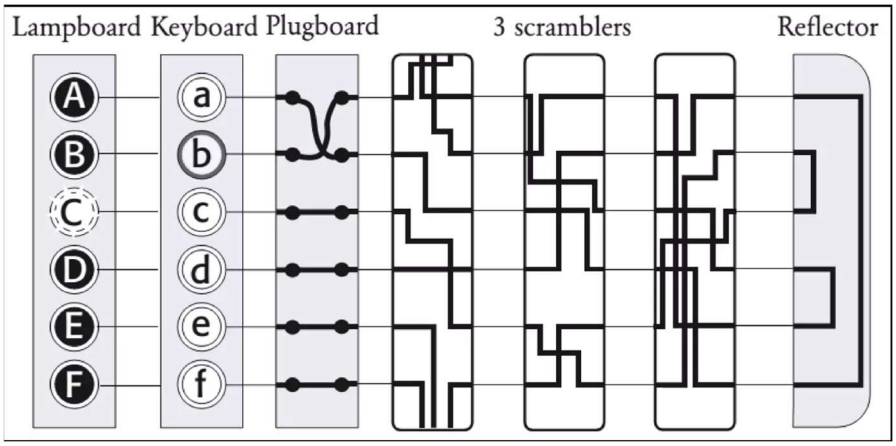


Imagen 10 – Esquema de funcionamiento de ENIGMA con seis letras[11]

Y a continuación incluyo un ejemplo empleando cryptool 2. Se incluyen imágenes de la configuración del dispositivo y dos posibles salidas, una desencriptando con la misma configuración de ENIGMA y otra sin conocer la clave del día.

[11] El gráfico pertenece al libro de Simon Sigh, Los códigos secretos y puede encontrarse en la página 158

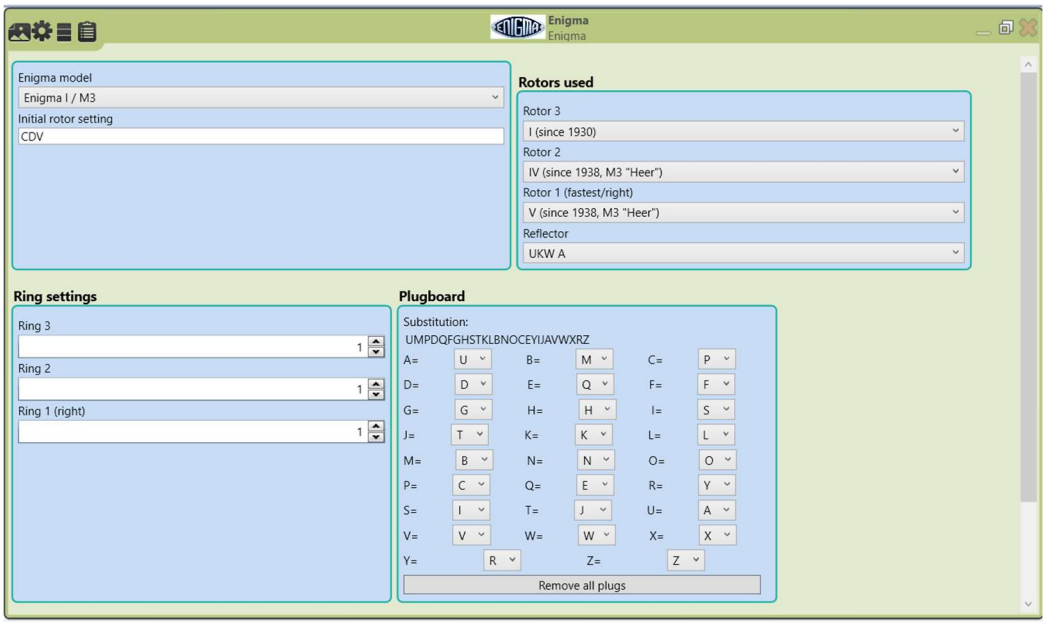


Imagen 11 – Configuración de ENIGMA en Cryptool2

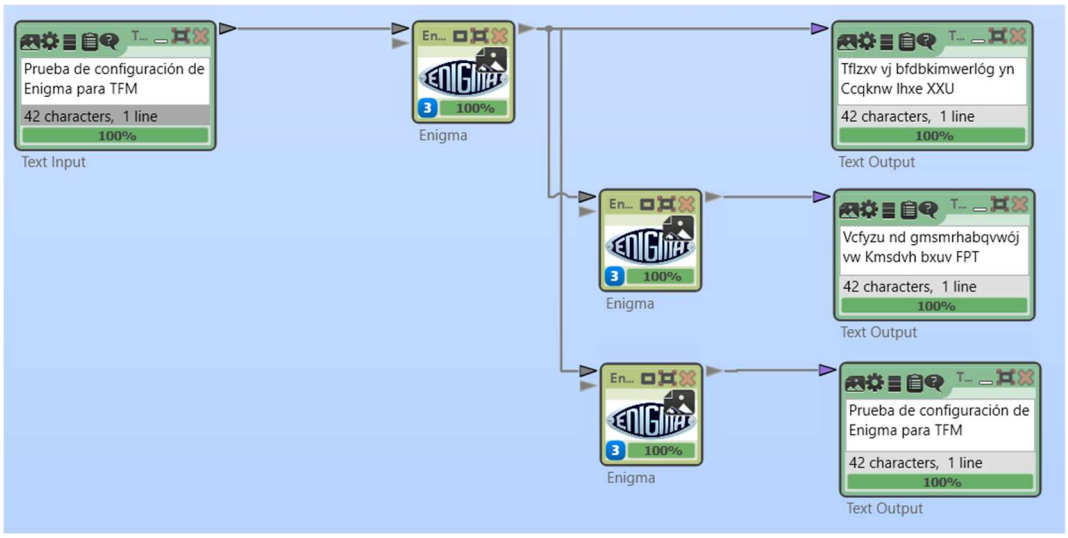


Imagen 12 – Ejemplo de uso de ENIGMA con Cryptool2[12]

Una vez finalizada la descripción del funcionamiento del sistema, sólo quedaría explicar el procedimiento de operación para que el contexto en el que se desarrolla la película quede explicado.

De acuerdo con lo descrito en los párrafos anteriores, queda esbozado que la "clave" de operación de ENIGMA constaba de varias acciones:

- Que rotores debían ser utilizados (3 de los cinco disponibles u ocho en momentos posteriores)
- Orden de instalación de estos
- Posición inicial de los mismos
- Conexiones del clavijero

[12] La primera máquina Enigma conectada a la salida no está configurada de la misma forma que la de entrada, la segunda si lo está, como era de esperar la primera de las Enigma no es capaz de decodificar correctamente, mientras que la segunda lo hace sin problema.

- Posición del reflector[13]

Estos datos se incluían en el libro de claves que debía ser distribuido a las unidades que hacían uso de ENIGMA[14].

Podemos encontrar ejemplos de estas claves sin más que realizar una sencilla búsqueda en internet[15], en mi caso empleo el que se muestra en el artículo de Antonio Barro Ordovás escrito en la *Revista general de la marina* (*La clave ENIGMA, p 238)* (Barro Ordovás 2017)

DATUM	WALZENLAGE	RINGSTELLUNG	STECKERVERBINDUNGEN	GRUNDSTELLUNG
01	III I II	0 X R	DO RZ XO UP LS QN	RDK
02	II III I	R T I	UX KI SW TA OR NU	TLF
03	III II I	A K P	HR DY BN SK AT VT	DSE

Imagen 13 – Ejemplos de claves diarias máquina ENIGMA

Creo que, a pesar del idioma, la imagen resulta bastante intuitiva, la primera columna corresponde a la fecha, la segunda son los rotores a emplear y el orden en el que deben colocarse, la tercera hace mención al *anillo*[16] un componente de ENIGMA que no he mencionado en la descripción para simplificarla esta, la cuarta posición correspondería al intercambio de letras que se realiza mediante el clavijero y la última sería las posiciones iniciales de los rotores.

Para finalizar con lo aquí descrito haré una breve reseña a una mejora de operación empleada por los operadores del dispositivo; como hemos dicho en varias ocasiones, la operación del dispositivo se realizaba en base a los libros de códigos distribuidos por el ejército alemán periódicamente. Ateniéndonos al pie de la letra a lo allí reflejado, la posición de los rotores debía ser la indicada para el día en cuestión y para todos los mensajes enviados; es en este punto donde se introduciría la mejora: cambiar esta clave en cada uno de los mensajes enviados.

Para realizar lo anterior se procedía como sigue, la clave del día se empleaba para codificar una nueva terna seleccionada al azar, esta se enviaba en el encabezamiento y se repetía dos veces para evitar posibles problemas de transmisión, una vez seleccionada esta nueva clave, era esta la empleada para encriptar el mensaje. El receptor no tenía más que desencriptar la nueva clave empleada en el mensaje, posicionar los rotores de acuerdo con lo allí indicado y una vez hecho, desencriptar el mensaje en sí.

La película no muestra lo aquí descrito, ni se pretende. En cuanto al criptoanálisis realizado primero por los polacos y posteriormente por los ingleses tampoco se muestra en detalle, de hecho, el importante papel

[13] No lo he comentado en la descripción, pero el reflector podía conectarse de diferentes formas, aunque esta no solía cambiarse, también hemos dicho que este componente no añade complejidad a la encriptación.
[14] No hace falta remarcar la importancia de esto libros, era mucha y la posibilidad de obtenerlos condujo a la realización de varias operaciones, sobre todo en relación a los empleados por la marina y se describe con algo más de detalle en análisis posteriores (U-571)
[15] ***"Enigma daily Keys"*** da bastantes resultados en este sentido.
[16] *"… los rotores tenían la posibilidad de girar el ánima (cableado interno) respecto a la corona exterior con las letras, es decir, que si giramos este elemento dos grados (de 26 posibles), aunque en la ventana veamos la letra A, internamente el cableado corresponderá a la C y así será transformado…"* (Zúñiga Azcue s.f.)

desempeñado por los primeros casi no es mencionado, tampoco el hecho de que La Bomba está inspirada en la empleada por aquellos.

Sólo quiero mencionar que si bien el diseño de ENIGMA era bastante robusto como hemos podido ver en la descripción, también tenía algún punto débil, por ejemplo, la presencia del reflector que permitía emplear el sistema para encriptar y desencriptar también servía para impedir que una letra en claro pudiese obtenerse también en el código encriptado en ninguna situación, esto que aparentemente podría ser una ventaja, resulta ser un inconveniente si se conoce de antemano, como así era.

No fue este el único error cometido por los alemanes que cometieron algunos al diseñar la operación del sistema, por ejemplo:

- La clave del día o la clave del mensaje se incluía dos veces en el encabezado este, si se hacía así era para evitar errores en la transmisión.
- El intercambio de letras no podía realizarse entre vecinas, p.e. no se podía intercambiar la **a** con la **b** o la **s** con la **t.**
- La posición de un rotor no podía mantenerse dos días seguidos en la misma posición.

Este tipo de limitaciones reducían el número de posibilidades del sistema y una vez que fueron detectadas o conocidas, facilitaron el análisis de los mensajes cifrados.

A este tipo de errores se unirían los propios de los operadores, como hemos comentado un poco más arriba para no emplear la disposición diaria fijada para los rotores, los operadores seleccionaban una al azar para cada mensaje, esta ventaja aparente se convirtió en desventaja cuando algunos de los operadores comenzaron a emplear siempre la misma o alguna previsible como QWE o cualquier otra secuencia de letras consecutivas en el teclado[17].

Al innegable genio de Turing se unieron pues los errores de los diseñadores y operadores de ENIGMA, brindando al primero y al resto de analistas las grietas que permitirían la ruptura del código.

La película muestra con suficiente fidelidad, para lo que se esperaría en una representación de este tipo, la tarea desarrollada en Bletchley Park. El papel desempeñado por la criptografía y elementos criptográficos es sin duda protagonista y no es posible dudar de la importancia que estos códigos y su ruptura representaron en la época en la que se desarrolla la acción y también en la historia real de la Segunda Guerra Mundial.

3.2. Enigma[18]

3.2.1. Resumen y Datos Técnicos

Película Anglo Norteamericana del año 2001 basada en la novela del mismo nombre de Robert Harris. Fue dirigida por Michael Apted e

[17] El nombre de estas configuraciones, denominadas *cillis* parece provenir de una de estas claves CIL que se repetía a menudo por parte de uno de los operadores de enigma.
[18] (Stoppard, y otros 2001)

interpretada en sus principales papeles por: Dougray Scott (Thomas Jericho), Kate Winslet (Hester Wallace) y Saffron Burrows (Claire).

Ambientada en la Segunda Guerra Mundial en Bletchley Park. Los códigos de ENIGMA ya han sido rotos, pero los alemanes han cambiado su libro de claves y es preciso romper, una vez más el código SHARK empleado por la Marina alemana. Thomas Jericho vuelve a Bletchley Park para contribuir en el criptoanálisis y averiguar que se oculta tras la desaparición de Claire.

3.2.2. Análisis

Aunque en esta ocasión ENIGMA ya ha sido vulnerada y sus códigos son accesibles para la inteligencia británica, la Marina alemana y en particular sus submarinos han cambiado el libro de claves y el trabajo realizado hasta entonces ha perdido casi todo su valor.

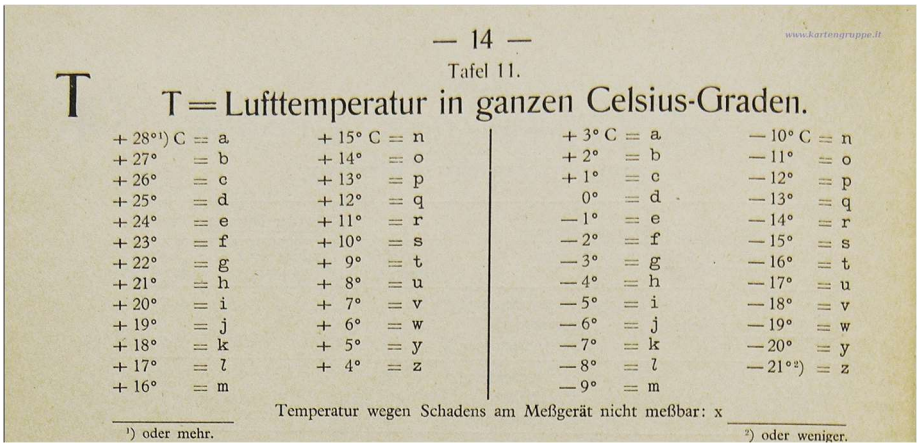
El planteamiento resulta interesante, por no decir apasionante, salvo por una importante incorrección; como ya hemos visto en el detallado análisis del funcionamiento de ENIGMA llevado a cabo en la película anterior, *Descifrando Enigma*, y los detalles sobre el uso de la versión naval que podemos encontrar en la revisión de *U-571*, el cambio de los libros de códigos formaba parte del procedimiento habitual de uso de ENIGMA. En el caso de la versión naval, este cambio se producía con una frecuencia algo superior a la de las versiones del resto de armas del ejército alemán, pero no por ello dejaba de hacerse. Parece pues, que el problema planteado en la película no era tal, más bien un inconveniente al que los criptoanalistas de ULTRA debían estar acostumbrados.

Bien es cierto que en algunas ocasiones se capturaron libros de códigos en submarinos alemanes y estos proporcionaron las configuraciones de los sistemas ENIGMA durante sus periodos de vigencia, pero también es cierto que, en otras muchas ocasiones, se trabajaba sin ellos actualizados.

Más problemático hubiese resultado el cambio en el *Short Weather Cipher (Cifrado Meteorológico corto)* u otros libros de códigos cortos, de cuyas versiones varias acabaron en manos inglesas y resultaron de gran ayuda en la tarea del criptoanálisis de la versión naval de ENIGMA; aunque también se produjeron dichos cambios, hago mención a ello más abajo en este mismo apartado. Pero no es el caso, en la película se menciona dicho libro de códigos y se considera vigente.

Aprovecho esta mención para hacer una descripción, aunque sea somera, del funcionamiento de este cifrado, conocido también como *Libro de señales meteorológicas cortas (weather short signal book).*

Estas señales se empleaban para el envío y recepción de informes meteorológicos empleando mensajes de siete letras posteriormente cifrados empleando ENIGMA. El código empleaba letras para enviar datos meteorológicos como se muestra para la temperatura en la imagen inferior.



— 14 —

Tafel 11.

T = Lufttemperatur in ganzen Celsius-Graden.

+ 28°[1]) C = a	+ 15° C = n	+ 3° C = a	— 10° C = n
+ 27° = b	+ 14° = o	+ 2° = b	— 11° = o
+ 26° = c	+ 13° = p	+ 1° = c	— 12° = p
+ 25° = d	+ 12° = q	0° = d	— 13° = q
+ 24° = e	+ 11° = r	— 1° = e	— 14° = r
+ 23° = f	+ 10° = s	— 2° = f	— 15° = s
+ 22° = g	+ 9° = t	— 3° = g	— 16° = t
+ 21° = h	+ 8° = u	— 4° = h	— 17° = u
+ 20° = i	+ 7° = v	— 5° = i	— 18° = v
+ 19° = j	+ 6° = w	— 6° = j	— 19° = w
+ 18° = k	+ 5° = y	— 7° = k	— 20° = y
+ 17° = l	+ 4° = z	— 8° = l	— 21°[2]) = z
+ 16° = m		— 9° = m	

Temperatur wegen Schadens am Meßgerät nicht meßbar: x

[1]) oder mehr.

[2]) oder weniger.

Imagen 14 – Código corto para la temperatura

De forma semejante se codificaban el resto de los datos incluidos en la señal: temperatura del agua, presión atmosférica, humedad, dirección y velocidad del viento, visibilidad, nubosidad, longitud y latitud.

De estos libros de códigos se emplearon al menos tres durante el conflicto, a saber: el primero llamado *Weimar* fue reemplazado por el denominado *Eisenach* en enero de 1942 que a su vez sería sustituido por el *Naumburg* en marzo de 1943. De ellos los dos primeros acabaron en manos británicas. (wikipedia 2022)

Continuando con la revisión de la película, indicar que a pesar de lo que en mi opinión es un error y ya he comentado más arriba, alguno más he encontrado y los describiré algo más adelante, destacaría algunos detalles interesantes que se muestran en el filme y, estos si, resultan esencialmente correctos en lo que fueron las tareas rutinarias de descifrado realizadas por el equipo de ULTRA.

- Las primeras escenas de la película recogen lo que sería la configuración y preparación de un sistema ENIGMA de tres rotores para ser operado. Resulta interesante ver gráficamente lo que he descrito en el análisis de la primera película.
- Aparecen, una vez más, los crucigramas y el ejercicio presentado por el Daily Telegraph con el objetivo de reclutar criptógrafos.
- Se hace mención de las diferencias entre las versiones navales de ENIGMA y el resto de las empleadas durante la contienda; es decir, la versión naval operaba con cuatro rotores mientras que el resto lo hacían con tres.
- Mientras que la *Luftwaffe* y el *Heer* enviaban los mensajes agrupados en series de cinco letras, la *Kriegsmarine* lo hacía en grupos de cuatro.
- Se menciona la existencia de *"cillis",* en esta ocasión el operador comienza siempre los mensajes con ADU que en la película traducen como *"Angels Danced United"* (Los Ángeles danzan unidos). El nombre original podría provenir, de CIL, código de tres letras identificado en las transmisiones de uno de los operadores de ENIGMA.

En cuanto al error al que he hecho mención más arriba, está relacionado con el uso de sistema TypeX ingleses en el descifrado rutinario de

mensajes codificados una vez se había localizado la clave del día y la configuración de ENIGMA.

En la película se muestra este como el proceso habitual para el descifrado de mensajes, aunque para ello se precise de una plantilla a la que se hace mención, pero no se nos explica ni su uso ni como se obtenía.

Si bien tanto el sistema TypeX como la ENIGMA alemana y los SIGABA norteamericano y PURPLE japones estaban todos ellos basados en el uso de rotores, el funcionamiento de cada uno era diferente y veo muy complejo realizar la configuración mencionada.

No he encontrado, además, en ninguno de los documentos, libros ni enlaces consultados referencia alguna a este uso de los dispositivos ingleses. Esto sin mencionar que, desde mi punto de vista, y una vez que los ingleses dispusieron de sistemas ENIGMA, hubiese resultado más sencillo construir los necesarios para realizar la tarea.

En resumen y para finalizar, no cabe duda de la importancia que el mecanismo criptográfico empleado y su ruptura tuvieron en el desarrollo de la Segunda Guerra Mundial; la corrección en el uso del mecanismo por parte del guionista y director de la película sin ser incorrecta si muestra errores e imprecisiones. En este caso, ENIGMA, su uso y las tareas para descifrarlo son más un gran decorado y una magnífica excusa sobre la que se desarrolla la verdadera acción que un elemento protagonista de esta.

3.3. A Beautiful Mind – Una mente Maravillosa[19]

3.3.1. Resumen y Datos Técnicos

Película norteamericana del año 2001 basada en la novela del mismo nombre de Sylvia Nasar. Fue dirigida por Ron Howard e interpretada en sus principales papeles por: Russell Crowe (John Nash), Jennifer Connelly (Alicia Nash), Ed Harris (Parcher) y Christopher Plummer (Dr. Rosen).

Biografía del matemático y premio nobel de economía, por su trabajo sobre Juegos no Cooperativos (Nash 1951), John Nass. La película narra la vida y enfermedad del afamado matemático.

3.3.2. Análisis

Desde el punto de vista de la criptografía y los códigos, la película los menciona en varias ocasiones; al comienzo, señalando la importancia del trabajo que los matemáticos realizaron rompiendo los códigos japoneses o en la fabricación de la bomba atómica y a lo largo del desarrollo de esta en múltiples ocasiones, siempre a través de las ensoñaciones y paranoias que el protagonista sufre a consecuencia de su enfermedad.

Salvo en la primera ocasión en la que la información se inserta entre los datos capturados a una emisora soviética, en el resto esta se encuentra en códigos insertados en diferentes artículos de periódicos o revistas. En

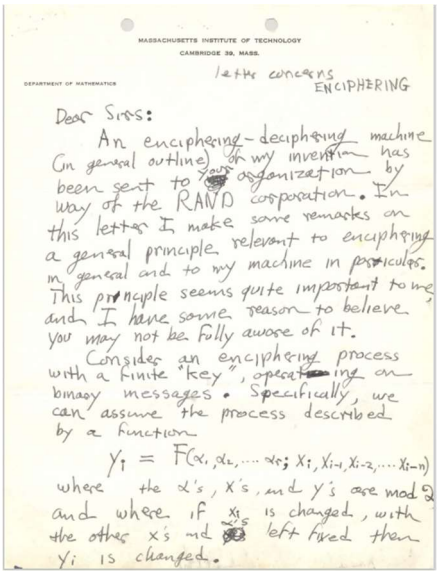
19 (Crowe, Connelly y Harris 2001)

el primero de los casos mencionados, se trataría de localizaciones expresadas mediante latitudes y longitudes, en el resto no se identifica la supuesta información que Nash encuentra en sus revisiones.

Diagnosticado de Esquizofrenia Paranoide, todo lo anterior formaba parte de las ensoñaciones propias de su enfermedad y no tenía existencia real, resulta por tanto imposible realizar ningún tipo de análisis.

A pesar de lo anterior y de lo mostrado en la película, tras la desclasificación reciente de varios documentos pertenecientes a la NSA, se demuestra el interés real de Nash en la criptografía, más allá de sus ensoñaciones paranoides[20].

En la imagen siguiente podemos ver la primera página de una de las cartas enviadas por el matemático a la agencia en la que hace referencia a una máquina criptográfica de su invención



MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE 39, MASS.

DEPARTMENT OF MATHEMATICS

letter concerns
ENCIPHERING

Dear Sirs:

An enciphering-deciphering machine (in general outline) of my invention has been sent to your organization by way of the RAND corporation. In this letter I make some remarks on a general principle relevant to enciphering in general and to my machine in particular. This principle seems quite important to me, and I have some reason to believe you may not be fully aware of it.

Consider an enciphering process with a finite "key", operating on binary messages. Specifically, we can assume the process described by a function

$$y_i = F(x_1, x_2, \ldots x_n; x_i, x_{i-1}, x_{i-2}, \ldots x_{i-n})$$

where the x's, x's, and y's are mod 2 and where if x_i is changed, with the other x's and left fixed then y_i is changed.

Imagen 15 – Fragmento de una de las cartas enviadas por Nash a la NSA

Más allá del innegable interés de la película y la figura que evoca, los elementos criptográficos resultan de difícil identificación y la importancia de estos no deja de ser secundaria en el desarrollo de la historia.

En cuanto a la importancia de la criptografía en el momento histórico en el que se desarrolla la acción, esta era sin duda importante o muy importante, no podemos olvidar que en estas fechas tenía lugar lo que conocemos como "Guerra Fría" y la información, como ya había sucedido en momentos anteriores de la historia y en particular durante el transcurso de la Segunda Guerra Mundial resultaría fundamental en el devenir de los acontecimientos.

20 Información adicional sobre este tema puede encontrarse en los enlaces siguientes:

- https://www.gaussianos.com/desclasificada-una-profetica-carta-sobre-criptografia-de-john-nash-a-la-nsa/
- https://tallerdecripto.blogspot.com/2012/02/john-nash-un-criptografo-maravilloso.html
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1630570/national-cryptologic-museum-opens-new-exhibit-on-dr-john-nash/
- nash_letters1.pdf (nsa.gov)

3.4. Contact – Contacto[21]

3.4.1. Resumen y Datos Técnicos

Película norteamericana del año 1997 basada en la novela homónima de Carl Sagan. Dirigida por Robert Zemeckis, cuenta entre sus principales intérpretes con: Jodie Foster (Ellie Arroway), Matthew McConaughey (Palmer Joss), Tom Skerritt (David Drumlin), William Fichtner (Kent) y David Morse (Ted Arroway).

Ambientada en los años 90 del pasado siglo, la película se centra en los esfuerzos de la Dra. Arroway, integrante del programa SETI[22] de la NASA, por encontrar señales originadas por civilizaciones extraterrestres, sus esfuerzos se verán recompensados cuando detecten una señal desde Vega que contiene la transmisión televisada de la ceremonia de inauguración de los juegos olímpicos celebrados en Berlín en 1936.[23]

3.4.2. Análisis

Como sucede en alguna otra de las películas incluidas en este inventario, no desempeña la criptografía en este caso un papel especialmente destacado; de hecho, las técnicas mostradas no creo que deban ser consideradas criptografía; aunque se trate, en un caso de una inocente ocultación de información gráfica y en el segundo del uso de un sencillo código de sustitución monoalfabético. Como decía, la intención tras estos artilugios no parece tanto ocultar la información contenida en los mensajes a ojos no autorizados, como a ojos no competentes; se trataría pues en este caso de asegurar que la información la recibe quién dispone de los conocimientos y la tecnología necesarios para leerlos.

No se trata por supuesto de un papel protagonista ni secundario y sería más cercano al de extra que al de intérprete de reparto.

Dicho lo anterior, los mecanismos que se muestran en la película puedo considerarlos esencialmente correctos, más allá del uso que de ellos se hagan y de la existencia o no de los remitentes de estos. Estos serían dos o tal vez tres, los menciono a continuación.

- En la transmisión original recibida, y tras la sorpresa inicial al descubrir que se trata de la ceremonia inaugural de los juegos olímpicos de Berlín celebrados en el año 1936, se realiza un análisis más exhaustivo de lo recibido; a consecuencia de este (realizado además y de manera esencial por un personaje ciego que basa su análisis, por tanto, más en el espectro auditivo que en el visual de el que carece) se detecta que si bien la codificación habitual de este tipo de transmisiones se realiza a 25 fotogramas por minuto, la que se está recibiendo lo está a 50; la mitad de ellos corresponden a la retransmisión original y el 50% restante a una

[21] (Foster, McConaughey y Hurt, y otros 1997)
[22] El programa SETI (Search for Extraterrestrial Intelligence) fue ideado y apadrinado, entre otros, por el autor de la novela y afamado astrónomo y divulgador científico: Carl Sagan
[23] Estos serán los primeros juegos olímpicos de la historia retransmitidos por televisión.

completa colección de documentos cuyo contenido no puede ser interpretado, por el momento al menos.

Se trataría en este caso de una técnica más esteganográfica que criptográfica.

- Una vez encontrados los documentos así transmitidos, el esfuerzo se centra en la interpretación de estos, tarea que resulta imposible para cuantos equipos se enfrentan a ella. Todo ello pese a contar con símbolos y claves en cada una de las hojas que ayudan en la tarea de relacionar las unas con las otras y encontrar el orden correcto en que deben ser colocadas. No es hasta que uno de los protagonistas de la historia emplea una aproximación diferente que no es posible realizar esta tarea, esta aproximación no es otra que abandonar el intento de realizar una distribución bidimensional de los documentos para realizarla con una perspectiva tridimensional (el argumento empleado para apoyar esta aproximación resulta, cuando menos, curioso y se basa en la idea de que mentes extraterrestres emplearan de manera más amplía que nosotros una representación mental más espacial que plana). Una vez se decide el empleo de esta técnica, los documentos cobran sentido y se ordenan de manera natural. No se trataría en este caso de ninguna técnica criptográfica, más bien estamos ante una especie de puzzle.
- Una vez finalizada la ordenación anterior, la lectura de lo contenido se torna sencilla. El lenguaje empleado en ellos está basado principalmente en las matemáticas y es a través de estas que se realiza una primera interpretación, se muestra más abajo en este mismo punto. Se trataría pues de una sencilla técnica de sustitución monoalfabética, en la que cada uno de los signos o símbolos empleados en los documentos tiene una traducción unívoca a uno de los que empleamos por nuestra parte.

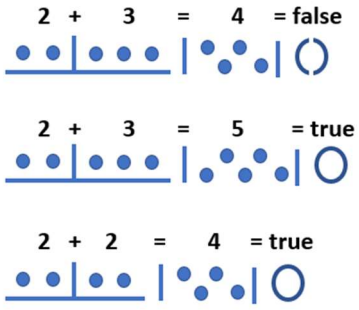


Imagen 16 – Operaciones matemáticas en Contact

En cuanto a la importancia de la técnica empleada, esta es sin duda baja o muy baja, la importancia se encuentra en el mensaje contenido y en las consecuencias de este, el mecanismo empleado para su transmisión no resulta demasiado significativo.

3.5. Sneakers – Los Fisgones[24]

3.5.1. Resumen y Datos Técnicos

Película norteamericana del año 1992. Fue dirigida por Phil Alden Robinson y cuenta entre sus principales intérpretes con: Robert Redford (Bishop), Sidney Poitier (Crease), Mary McDonnell (Liz), Dan Aykroyd (Mother), David Strathairn (Whistler) y Ben Kingsley (Cosmo).

La película transcurre a principios de los años 90 del pasado siglo y se centra en los esfuerzos del equipo de Martin Bishop (Robert Redford), antiguo hacker que evitó el ingreso en prisión al salir a comprar pizza en el momento que su compañero Cosmo era detenido por las autoridades, por sustraer primero y luego recuperar un extraño dispositivo, una caja negra capaz de decodificar cualquier sistema de encriptación, desarrollado por el brillante matemático Gunter Janek.

3.5.2. Análisis

El origen del guión de esta película se encuentra en una anterior y también dedicada a los hackers y phreakers: War Games, Juegos de Guerra en castellano.

El interés de los guionistas por reflejar de manera correcta la criptografía se ve reflejada en el hecho de que solicitasen la colaboración del profesor Len Adleman[25] como consultor matemático, esta colaboración se concretó en las diapositivas que Gunter Janek emplea en su disertación. En pago a dicha colaboración, la esposa del profesor tuvo la oportunidad de conocer y charlar brevemente con Robert Redford.

Otra curiosidad relacionada con la película y, de acuerdo con lo recogido en el blog *"Películas de Culto"* (Películas de Culto 2013), se dio cuando, antes del comienzo del rodaje, el Departamento Naval de Inteligencia contactó con el director para solicitarle que eliminase de la película cualquier mención al dispositivo decodificador. Tras varias horas reunidos con el abogado del estudio, la conclusión fue que se trataba de una broma, probablemente urdida por Robert Redford y Dan Aykroyd.

De todo lo anterior se concluye la importancia que tanto el director como los guionistas prestaron a los elementos criptográficos incluidos en la película; el papel atribuido a esta no es protagonista, pero si se trata de un secundario de lujo.

Analizando con algo más de detalle lo incluido en el filme destacaría lo que sigue.

- Durante la conferencia del Dr. Janek se hace mención a la importancia de la criba de datos numéricos en los algoritmos de encriptado y desencriptado. Afirmación que resulta esencialmente correcta si recordamos la importancia que tiene en la práctica

[24] (Redford, Poitier, y otros 1992)
25 Científico norteamericano, ganador en el año 2002 del premio A.M. Turing junto a Ronald L. Rivest y Adi Shamir por sus contribuciones a la criptografía de clave pública mediante el sistema de encriptación conocido como RSA (Hosch 2022)

criptográfica la dificultad de realizar esta factorización. En la misma conferencia se hacen referencias a los grupos abelianos y *"cicloxxxxxx"*, el segundo termino tal y como yo lo he entendido (*ciclotómicos*) no existe y es incorrecto; no puedo descartar, sin embargo, que se trate de un problema en la traducción y en el original se haga referencia a *"ciclic groups"* y *"abelian groups"*. Para terminar con este punto, señalaré que en la misma conferencia se hace referencia asimismo a la inducción de homomorfismos, se trataría de nuevo de una afirmación esencialmente correcta.

- En un momento posterior de la película Whistler hará mención a que *"… los sistemas criptográficos se basan en problemas matemáticos tan complejos que no se resuelven sin una clave…"*, se trata una vez más de una afirmación correcta.
- El único código que aparece en el film se trata de un anagrama y es resuelto por los protagonistas en el transcurso de una partida de scrabble, el anagrama y el resultado se muestran a continuación

SETEC ASTRONOMY

TOO MANY SECRETS

- Aparecen, de nuevo, los crucigramas en la película. No se trata de ningún elemento central ni destacado; pero, como indicaré en las conclusiones, son varias las películas en las que estos pasatiempos aparecen tengan en ellas un papel relevante o sólo como elementos del decorado.
- Es destacable la importancia que las tareas de inteligencia e infiltración tienen en la película y resultan cruciales tanto en la obtención de los códigos de acceso que emplea el Dr. Jarek, como en la grabación de la voz de uno de los personajes que permitirá a la postre la infiltración en las instalaciones donde se encuentra la caja negra.
- La caja negra que es el objeto fundamental de la película es un dispositivo capaz de decodificar cualquier encriptado. Por supuesto en ningún momento se nos explica el funcionamiento ni los principios en que está basada.
- Los códigos que pretenden romperse con el dispositivo no son los del oponente (los rusos en este caso) sino más bien los propios. Conectaría este punto con los ataques a la privacidad que mencionaremos algo más adelante en este mismo trabajo en películas como Snowden y Mercury Rising.

Se trata, por tanto, de una película cuidadosa con los detalles, en la que la criptografía, sin jugar un papel estelar, desempeña un bien merecido papel secundario. Tratándose de un recurso ficticio, la omnipresente caja negra no deja de recordarme a dispositivos de los que ahora hablamos mucho, computadores cuánticos que prometen hacer lo que en esta película no es más que una entelequia, romper cualquier código; sea este propio o extraño.

3.6. National Treasure – La Búsqueda[26]

3.6.1. Resumen y Datos Técnicos

Película norteamericana del año 2004. Fue dirigida por Jon Turteltaub y cuenta entre sus principales intérpretes con Nicolas Cage (Benjamin Frnklin Gates), Diana Kruger (Abigail Chase), Justin Bartha (Riley Poole), Sean Bean (Ian Howe) y Jon Voight (Patrick Gates).

Benjamin Franklin Gates, siguiendo la tradición familiar, ha dedicado toda su vida a la búsqueda del legendario tesoro de los Caballeros Templarios, oculto en algún lugar de los Estados Unidos. Parece que en esta ocasión ha encontrado la pista definitiva entre los restos de la nave Charlotte.

3.6.2. Análisis

Divertida película en la que la criptografía no es más que otra prueba entre el conjunto de ellas que deberá superar el protagonista para encontrar el legendario y famoso tesoro de los Caballeros Templarios.

Entre acertijos y dispositivos curiosos, encontramos dos mecanismos de ocultación de la información que merece la pena examinar.

- En el reverso de la Declaración de Independencia de los Estados Unidos, Timothy Matlack[27] calígrafo y supuesto redactor de esta; incluyó, ocultas con zumo de limón, una lista de cifras agrupadas de tres en tres.

  Se trata en este caso y de nuevo de esteganografía más que de criptografía.
- Una vez localizados los números anteriores, sólo restaría encontrar el mecanismo de cifrado para encontrar el mensaje oculto tras ellas.

  El conocimiento y los datos acumulados por la familia Gates permite a nuestro protagonista deducir que estaríamos ante una cifra Ottendorf o cifrado de libro, basado en las cartas que Silence Dogood envío al periódico New-England Courant en 1722.

  Cada grupo de tres cifras se interpreta como sigue, la primera cifra es el número de la carta, la segunda el número de línea en esa y la tercera, la posición que la letra ocupa en la línea. De esta forma es posible traducir cada grupo de tres cifras en una letra y el conjunto de letras en un texto que resulta ser el siguiente

  The vision to see the treasured past comes as the timely shadow crosses in front of the house of Pass and Stow.

Como resumen y para finalizar, nos encontramos ante una divertida película de acción, una yincana en la que los mecanismos de ocultación de la información son un par de pruebas más entre las varias que debe superar el protagonista en su búsqueda del tesoro.

26 (Cage y Kruger, National Treasure (La Búsqueda) 2004)
27 https://tinyurl.com/2q8tc8zd

3.7. The Da Vinci Code – El Código Da Vinci[28]

3.7.1. Resumen y Datos Técnicos

Película norteamericana del año 2006 basada en el best seller del mismo nombre de Dan Brown. Fue dirigida por Ron Howard y cuenta entre sus principales intérpretes con Tom Hanks (Robert Langdon), Audrey Tautou (Sophie Neveu), Ian McKellen (Sir Leigh Teabing), Jean Reno (Cpt. Bezu Fache) y Paul Bettany (Silas).

El catedrático y experto en simbología religiosa Robert Langdon debe acudir al museo del Louvre para tratar de ayudar a la policía en la resolución del asesinato de uno de sus restauradores que ha dejado diversas pistas en forma de símbolos. En la tarea contará con la ayuda de la criptógrafa de la policía Sophie Neveu, sin embargo no todo es tan sencillo, el principal sospechoso es él y hay más secretos en juego de los que Langdon imagina.

3.7.2. Análisis

En esta ocasión y siendo rigurosos no hay ningún elemento criptográfico en la película; no obstante, si encontramos varios anagramas y un curioso dispositivo que podría conducir a engaño debido a un sugerente nombre: *Cryptex.* A lo anterior añado, además, el uso que Silas hace del latín cuando mantiene una conversación telefónica con su maestro y mentor.

En cuanto a los criptogramas, los que aparecen en la película son los siguientes

- Una serie de Fibonacci desordenada[29]: *13-3-2-21-1-1-8*, que una vez ordenada quedaría como sigue *1-1-2-3-5-8-13-21*. Esta serie será la que permitirá a Langdon y Sophie abrir la caja de seguridad que contiene el Cryptex.
- Cerca del cuerpo del restaurador aparecen también otro par de anagramas: *O, Draconian devil – Oh, lame saint* que correctamente ordenados dan lugar a *Leonardo Da Vinci – The Mona Lisa* y conducirán a nuestros protagonistas hasta el siguiente acertijo en forma de nuevo anagrama.
- El tercer anagrama al que se enfrentarán nuestros atribulados investigadores será: *So dark the con of men* que tras su ordenación conduce a la *Madonna of the Rocks*[30] donde hallarán una peculiar llave que, junto a la serie de Fibonacci, les permitirá algo más adelante abrir la caja de seguridad.

Armados con lo anterior, su ingenio e imaginación, los protagonistas del filme continuarán sus aventuras hasta localizar el resto de los elementos que les permitirán, no sin esfuerzo, revelar el misterio que es coprotagonista de la historia.

28 (Hanks, Tautou y Reno, y otros 2006)
29 A pesar de no guardar ninguna relación, señalo aquí que las series de Fibonacci aparecen también en al menos una película más de las analizadas: Pi, Fe en el caos.
30 Resulta cuando menos sorprendente la gentileza y el conocimiento del moribundo restaurador que siendo francófono hace un notable esfuerzo por traducir todos los anagramas al inglés que sin duda resulta más cómodo para Langdon.

Para terminar mi análisis quedan algunos elementos por revisar

- El *Cryptex*, curioso dispositivo que a pesar de su nombre poco tiene que ver con códigos, o al menos, no más allá de que se precisa uno para abrirlo. En este sentido el ingenioso cacharro sería más parecido a un candado con combinación, y trampa en caso de error, o lo que a mí me parece más atractivo, con una de esas cajas japonesas cuya apertura precisa la resolución de un rompecabezas[31]. En este caso cuenta con cinco discos con 26 letras cada una, sólo la combinación correcta de letras permitirá su apertura.

  En la película contiene información relevante para la resolución del misterio alrededor del Santo Grial que guía toda la trama y para obtener la clave, que resultara ser APPLE, los protagonistas sufrirán alguna prueba adicional y demostrarán su imaginación y capacidad de observación.
- Como ya he mencionado al comienzo de este apartado y aunque no pueda confirmarlo, en las conversaciones que Silas mantiene con su jefe y maestro hace uso del latín. Esto sería debido, con casi total seguridad, al hecho de que ambos pertenecen a una facción ultraconservadora dentro de la iglesia; el uso del latín no hace más que reforzar esta idea y nos aportaría indicios de ello. Sin embargo y tratándose este trabajo del uso de la criptografía en el cine, prefiero pensar que se trata de un mecanismo burdo y artesanal de "encriptación", pero eficaz, dependiendo por supuesto de quién esté a la escucha.

  No sería la primera vez que se emplease, no con latín por supuesto, sino con una lengua más complicada y así tendré la oportunidad de revisarlo en una película posterior.

Como resumen, insistir en que en sentido estricto no hay elementos criptográficos en la película, aunque si diferentes formas, más o menos imaginativas, de ocultar la información. La importancia de estos mecanismos es más bien escasa y si bien los anagramas son correctos, la existencia del cryptex no es más que una invención.

3.8. Pi(π): Faith in Chaos - Pi(π), fe en el caos[32]

3.8.1. Resumen y Datos Técnicos

Película norteamericana del año 1998. Dirigida por Darren Aronofsky está interpretada en sus principales papeles por Sean Gullete (Maximillian Cohen), Mark Margolis (Sol Robeson), Pamela Hart (Marcy Dawson) y Ben Shenkman (Lenny Meyer).

Ambientada en Nueva York a finales del siglo XX, narra la historia de la obsesiva búsqueda que Maximillian Cohen, un matemático reservado y aquejado de fuertes migrañas desde que siendo un niño decidió mirar el

[31] El nombre que reciben estás cajas es Himitsu-bako
[32] (Gullete, Margolis y Hart, y otros 1998)

sol sin protección, lleva años realizando con la esperanza de encontrar un modelo matemático que, presente siempre en la naturaleza, rige la bolsa.

Lo que Maximillian ignora es que sus estudios han despertado el interés de una oscura organización y de la comunidad ortodoxa judía de su ciudad. Ambas están dispuestas a todo para conocer el código que Maximillian busca.

3.8.2. Análisis

Más que sobre criptografía, la película trata sobre matemáticas y como estas pueden convertirse en una obsesión.

Toda la película gira alrededor de la creencia del protagonista (Maximillian Cohen) en que *"las matemáticas son el lenguaje de la naturaleza"*, esto se puede expresar en un puñado de sencillos principios que aparecerán en varias ocasiones a lo largo de la historia:

- *"Todo lo que nos rodea se puede representar y entender mediante números"*
- *"Si se hace un gráfico con los números de un sistema, se forman modelos. Estos se encuentran por todas partes en la naturaleza"*

El protagonista centra su análisis en la bolsa de la considera que también es orgánica y por tanto sometida a los principios antes descritos, formará por tanto un modelo que tiene intención de descubrir con la ayuda de una computadora de su creación llamada Euclides.

En la película se mezclan conceptos matemáticos, artísticos, religiosos y místicos. Se habla por ejemplo de Misticismo Judío e interpretación de la Torá, sucesiones de Fibonacci y espirales de Fibonacci.

El análisis de todos los conceptos e ideas mostradas en la película y como estas se conectan y alimentan la obsesión del protagonista resultaría sin duda interesante, aunque alejado del tema de este trabajo. Si de criptografía hablamos, lo único cercano a la misma que se muestra en el filme es la afirmación realizada por uno de los intérpretes, Lenny Meyer, cuando menciona la Torá como *"una cadena de números, un código enviado por dios"* y, por otra parte, el extraño código de 216 números que también se menciona asociado al nombre de dios y que otro de los protagonistas, Sol, recuerda haber hallado durante sus estudios sobre el número Pi(π)

Volviendo a la primera de las afirmaciones mencionadas en el párrafo anterior, el *código de dios*, sin duda está haciendo referencia a la Gematria, que aún sin tratarse de un mecanismo de encriptación si se trataría de un mecanismo de sustitución que podría por tanto, tener cierta, aunque lejana, relación con el tema tratado aquí. Dedicaré por ello algunas líneas a describir someramente su funcionamiento[33].

[33] Más detalle en relación con este tema puede encontrarse en el artículo de la revista ACTA que se incluye en la bibliografía (Zurdo 2008), en la entrada correspondiente de Wikipedia (Wikipedia 2023) (Wikipedia 2023), en la enciclopedia judía en la entrada del mismo nombre (Schechter y Levias s.f.)

En la primera tabla se incluye el equivalente numérico de cada una de las letras hebreas

Valor numérico	Hebreo	Glifo	Valor numérico	Hebreo	Glifo	Valor numérico	Hebreo	Glifo
1	*Alef*	א	10	*Yod*	י	100	*Kuf*	ק
2	*Bet*	ב	20	*Kaf*	כ	200	*Resh*	ר
3	*Guímel*	ג	30	*Lámed*	ל	300	*Shin*	ש
4	*Dálet*	ד	40	*Mem*	מ	400	*Tav*	ת
5	*Hei*	ה	50	*Nun*	נ	500	*Kaf (final)*	ך
6	*Vav*	ו	60	*Sámej*	ס	600	*Mem (final)*	ם
7	*Zayn*	ז	70	*Ayin*	ע	700	*Nun (final)*	ן
8	*Jet*	ח	80	*Pei*	פ	800	*Peh (final)*	ף
9	*Tet*	ט	90	*Tzadi*	צ	900	*Tzady (final)*	ץ

Imagen 17 – Equivalencia numérica de las letras hebreas en la Gematria[34]

En el artículo referenciado más arriba, también se incluye otra equivalencia, pero en esta ocasión empleando el alfabeto latino (para ello debe hacerse uso de transliteración)

LETRA	VALOR	LETRA	VALOR
A	1	M	40
B	2	N	50
C (fuerte)	20	Ñ	60
C (débil)	90	O	6
CH	95	P	80
D	4	Q	100
E	1	R	200
F	80	S	60
G (fuerte)	8	T	9
G (débil)	3	U	6
H	5	V	6
I	10	W	6
J	8	X	80
K	20	Y	10
L	30	Z	7
LL	60		

Imagen 18 – Equivalencia numérica de las letras latinas en la Gematria[35]

Basta pues con transformar cada letra de una palabra o frase en su equivalente numérico para tener una cifra que la represente.

Como ya he señalado más arriba, el uso que de la Gematria se hace por parte de los hebreos tiene más que ver con la religión y la mística que con un intento de ocultar o preservar información, no al menos fuera del ámbito religioso mencionado.

En este sentido resulta interesante reseñar la definición que de Gematria hace la web de dictionary.com: *"Sistema cabalístico de interpretación de las escrituras que substituye una palabra por otra cuyas letras dan como resultado la misma suma"* (Dictionary.com s.f.)

Sería en este contexto en el que la serie de números que ya he mencionado representase el verdadero nombre de dios.

[34] (Wikipedia 2023)
[35] (Zurdo 2008)

Un sencillo ejemplo del uso de Gematria empleando cryptool2 quedaría como vemos en la imagen siguiente:

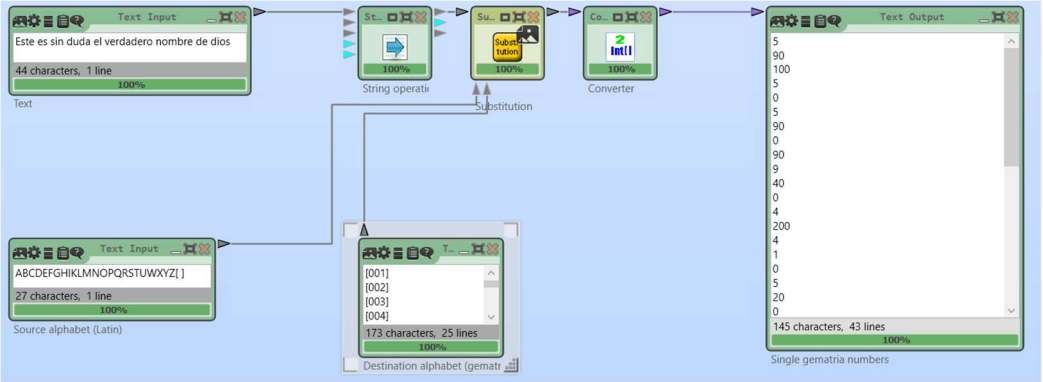


Imagen 19 – Ejemplo de uso de Gematria con alfabeto latino

En la película pues la codificación tiene un papel protagonista y de mucha importancia tanto para el protagonista como para quienes pretenden hacer uso de ella; bien sea con la intención de conocer el verdadero nombre de dios, bien con la intención de lucrarse invirtiendo en bolsa.

Se trataría de un tipo de codificación manual, aunque creo más adecuado decir que es *natural* e inventada, aunque como he explicado antes, podría haber alguna relación con la Gematria, al menos en lo que hace referencia al nombre del creador.

3.9. U-571[36]

3.9.1. Resumen y Datos Técnicos

Película norteamericana del año 2000. Dirigida por Jonathan Mostow e interpretada en sus principales papeles por Matthew McConaughey (Tyler), Bill Paxton (Dahlgren), Harvey Keitel (Chief).

Ambientada en la Segunda Guerra Mundial y durante la batalla del Atlántico, narra la historia del intento de capturar la máquina enigma del submarino U-571, averiado tras su encuentro con un destructor británico, llevada a cabo por parte de la tripulación del submarino americano S-33.

3.9.2. Análisis

Esta es la tercera ocasión en la que aparece como elemento del reparto una máquina ENIGMA. Sirve esto para demostrar la atracción y fascinación que este ingenioso dispositivo continúa despertando casi 70 años después de haber dejado de utilizarse y a pesar de haber sido atacada con éxito por parte de los aliados.

Como ya mencioné en los casos anteriores, en lo que hace referencia al aspecto exterior de la máquina, la representación que de ella se hace en la película, al menos hasta donde nos permiten ver sus fugaces apariciones en pantalla, es correcta.

[36] (McConaughey, Paxton y Keitel, U-571 2000)

En esta ocasión se trata del dispositivo empleado por la marina alemana que, tal y como se muestra, empleó dispositivos de cuatro rotores en lugar de los tres que empleó la infantería y aviación y son los que se muestran en las dos películas anteriores.

No entraré aquí a describir de nuevo el funcionamiento de este dispositivo, creo que la explicación incluida en las entradas correspondientes a: “Descifrando Enigma” y “Enigma” (en particular en la primera de ellas) es suficiente para el objetivo de este trabajo; si dedicaré sin embargo algo de tiempo a describir las diferencias entre el dispositivo de cuatro rotores que aquí se emplea y su equivalente de tres mostrado en las películas antes mencionadas. También realizaré algunas menciones a los libros de códigos, que en esta cobran cierta relevancia al ser uno de los objetivos de la incursión además de la propia máquina.

Comenzar diciendo que, si bien ENIGMA era el dispositivo de encriptación empleado por cualquiera de las armas del ejército alemán durante la Segunda Guerra Mundial, hubo ciertas diferencias entre los dispositivos que emplearon los unos o los otros y también en los protocolos de uso de los mismos.

En el caso de la Kriegsmarine y durante el tiempo que hicieron uso del sistema de tres rotores, hasta febrero de 1942 que cambiarían a un sistema de 4 rotores y diez conexiones en el clavijero, contaban con 8 entre los que seleccionar y el reflector, que era fijo en el caso de la Enigma empleada por el ejército, disponía de 26 posiciones diferentes en el caso de la empleada por la marina; más segura como vemos que su equivalente en el ejército, esto por no contar con que los operadores navales eran más cuidadosos en el uso de los procedimientos. (Singh 2000)

Además de lo anterior y alrededor de la fecha en que se desarrolla la película (febrero de 1942), la marina alemana había decidido cambiar los sistemas de tres rotores por otros de cuatro rotores (con diez entre los que elegir) y el clavijero disponía de 10 conexiones en lugar de las 6 de la versión del ejército, complicando aún más el descifrado del sistema naval.

De aquí la importancia de recuperar alguno de estos sistemas y los libros de códigos. En relación con esto último, debido a la particularidad propia de las operaciones navales, estos tenían una duración más elevada que podía ser de un mes, no podía permitirse que un submarino que podía pasar bastante tiempo sin recalar en puerto no dispusiese de los mecanismos para asegurar sus comunicaciones.

Recuperar uno de estos libros significaba para la inteligencia británica contar con las configuraciones de los sistemas durante todo el periodo restante de validez de estos.

Mención aparte merecen los códigos meteorológicos; sin duda su utilidad estratégica es escasa, sin embargo, conocerlos significaba contar con palabras conocidas en los mensajes interceptados; así, por ejemplo, si se sabía que los mensajes comenzaban con las condiciones meteorológicas y se conocen estas, el empleo del libro correspondiente significaba conocer una palabra en claro y su equivalente encriptado, esto facilitaba sin duda la tarea del criptoanalista.

Resulta por tanto que lo narrado en la película, sin ser tratado en detalle, resulta esencialmente correcto; salvo por el hecho de que fue la marina británica quién realizó la mayoría de estas incursiones y recuperaciones[37] y no sería hasta 1944 cuando lo norteamericanos realizaron una de estas incursiones.

En la película, el papel atribuído a la criptografía no deja de ser de reparto y no cabe ninguna duda de la importancia en el desarrollo de la guerra que representan los elementos y técnicas mencionados.

3.10. Les Vampires – Los Vampiros[38]

3.10.1. Resumen y Datos Técnicos

Serial francés mudo del año 1915 (cuenta con 10 episodios, de ellos analizaré el tercero). Dirigida por Louis Feuillade e interpretada en sus papeles principales por: Musidora (Irma Vep), Édouard Mathé (Philippe Guérande) y Marcel Lévesque (Oscar Mazamette).

El serial se ambienta en París a principios del siglo XX, la ciudad está aterrorizada por una serie de asesinatos y desapariciones llevadas a cabo por una misteriosa organización denominada *"Los Vampiros"*. El intrépido reportero del Globe Philippe Guérande asistido por su amigo y aliado Oscar Mazamette intenta desenmascarar a los miembros de dicha organización y devolver la tranquilidad a la ciudad.

3.10.2. Análisis

Aunque el serial cuente con 10 episodios que hacen de esta película una de las más largas jamás filmadas, en torno a 7 horas, mi análisis se centrará en el tercer episodio, el que lleva por título: *Le_Cryptogramme_Rouge* en castellano *El Criptograma Rojo.* No he sido capaz de hurtarme a lo que el nombre sugiere en relación con el tema de este trabajo.

No obstante, y a pesar del título, la relevancia de la criptografía y los criptogramas en este episodio es menor, como en otros casos analizados, considero que no pasa de encarnar un papel de reparto y en cuanto a la importancia de lo representado, tiene cierta importancia en el desarrollo, pero en el conjunto de lo mostrado esta importancia se reduce y no deja de ser menor. Lo verdaderamente importante son los esfuerzos realizados por el intrépido reportero en sus desvelos por encontrar a quienes forman el temido grupo.

---

[37] En octubre de 1942 sería capturado el U-559 lo que permitió la recuperación de uno de estos sistemas de 4 rotores y confirmar el cableado interno de estos, hastas entonces dicho cableado solo había sido intuido por los criptoanalistas británicos (Lehning 2022).

Esto también aparece correctamente reflejado en los títulos de cierre de la película, donde se menciona y lo atribuye al HMS Petard. Indican también estos títulos la captura del U-110 por parte de los buques HMS Bulldog y HMS Aubretic en mayo de 1941, en este caso se trataba de una enigma de tres rotores.

No sería hasta junio de 1944 que los norteamericanos capturarían un submarino alemán, el U-505, tarea llevada a cabo por el Equipo de Trabajo 22.3 de armada de los Estados Unidos con la intención de recuperar todo el material criptográfico allí disponible. (Subalemanes2 2013)

[38] (Musidora, Malthé y Lévesque, Les Vampires 1915)

Entrando en algo más de detalle, a lo largo de la película encontramos dos ejemplos de criptografía. El primero de ellos, que además sirve como introducción al episodio, se trata de la primera página del librito rojo que da nombre al episodio; un ininteligible código manuscrito al que Philippe se enfrenta armado de papel y pluma. Se trataría de un cifrado por transposición de el que muestro a continuación el original, el texto en claro resultante y el procedimiento empleado para su interpretación.

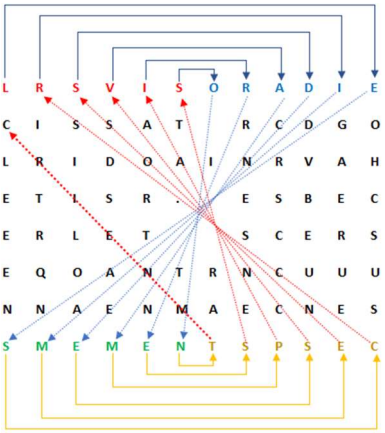


Imagen 20 – Criptograma de Les Vampires

Para interpretarlo, basta con seguir las líneas marcadas, comenzaríamos por la primera letra arriba a la izquierda después primera arriba a la derecha, diagonal hasta la primera letra de abajo a la izquierda, primera letra de abajo a la derecha y así sucesivamente hasta acabar con las letras disponibles, incluidos espacios y puntos.

Existe una alternativa que me parece más ingeniosa y divertida que nos lleva al mismo resultado, bastará para ello con plegar la hoja en dirección sur, norte para después hacer un nuevo pliegue este, oeste.

El resultado con el texto resultante podemos verlo a continuación

Imagen 21 – Texto en claro Les Vampires

Como puede verse en el texto resultante, aparece un espacio que podemos encontrar en el original, una N adicional que podría haberse eliminado y supongo que se mantiene con el objetivo de mantener la estructura y el encantador detalle de incluir el punto final al texto.

Además de lo anterior, la película muestra el que sería un segundo mecanismo de cifrado, más bien se trata de un anagrama, cuando Philippe disfrazado se aventura en el night club *The Howling Cat* y encuentra en la puerta un cartel anunciando la actuación de *Irma Vep,* una observación detallada del mismo llevará a nuestro protagonista a descubrir la palabra Vampire en dicho nombre.

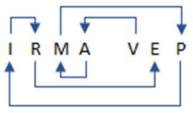


Imagen 22 – Anagrama Les Vampires

Todo lo anterior me sirve para determinar que el uso de la criptografía en este caso es, en lo esencial, correcto y las técnicas empleadas son inocentes pero reales.

3.11. Tinker Tailor Soldier Spy - El Topo[39]

3.11.1. Resumen y Datos Técnicos

Película británica del año 2011, basada en la novela homónima de John Le Carré. Fue dirigida por Tomas Alfredson e interpretada en sus principales papeles por Gary Oldman (George Smiley), Colin Firth (Bill Haydon), Mark Strong (Jim Prideaux) y Benedict Cumberbatch (Peter Guillam).

Ambientada en el periodo de la guerra fría y durante los años 70, nos cuenta la historia de la investigación llevada a cabo por George Smiley, espía de la vieja escuela y hombre de confianza de *Control*, para desenmascarar al agente doble (El Topo al que hace mención el título en castellano) introducido en la cúpula del Circus por Karla, némesis de Smiley y responsable de la 13ª dirección del centro de Moscú (el equivalente inventado por Le Carré para la KGB).

3.11.2. Análisis

Aunque, sin duda, asegurar las comunicaciones entre los agentes de campo del MI6 británico, organización en la que trabajó el autor y que emplea como inspiración en la creación de su imaginario *Circus*, y sus responsables, fuese y continúe siendo hoy en día una prioridad; la presencia de la criptografía y el aseguramiento de las comunicaciones no constituye en esta película un elemento central de la trama, ni siquiera podemos considerarla un personaje del reparto, como máximo se trataría de un extra o un elemento de atrezo que como otros que se muestran en ella (cámaras, micrófonos, máquinas de grabación y escucha, armarios con cerradura de combinación, etc.) ayudan a establecer el ambiente en el que se desarrolla la acción y sirven como soporte al desarrollo de esta.

Con lo anterior en mente, hay que indicar que la criptografía o elementos criptográficos aparecen en un par de ocasiones durante el desarrollo. En ambas ocasiones, los dispositivos de cifrado se presentan como aparatos semejantes a máquinas de escribir eléctricas.

De acuerdo con la información incluida en el artículo: *"Protecting secrets: British diplomatic cipher machines in the early Cold War, 1945–1970"* (Easter 2019), las principales máquinas de cifrado empleadas por el Foreing Office británico en el periodo indicado fueron las siguientes: Typex, Rockex, Noreen y Alvis. Por la información que he podido obtener de ellas, ninguna se parece a lo que se muestra en la película que bien podría tratarse de otro dispositivo como, por ejemplo, un teletipo.

A pesar de lo anterior y como he indicado un par de párrafos más arriba, en esta ocasión el papel atribuido al cifrado no deja de ser simbólico y los

[39] (Oldman, y otros 2011)

dispositivos mostrados sirven al propósito de la película sin desmerecer en exceso.

Entrando en algo más de detalle, en las dos ocasiones en las que se envían o reciben mensajes encriptados, se muestran agrupados en grupos de 5 caracteres numéricos, con diez de estos grupos por línea, por ejemplo:

87264 78534 02484 13774 83984 72498 29723 18573 89275 16493

No conociendo más detalles al respecto, no me es posible identificar el tipo de cifrado empleado; cabe destacar, además, que durante la recepción de uno de estos mensajes en respuesta a uno anterior remitido por uno de los agentes de campo, solicita al operador el desencriptado del mismo, tarea que este lleva a cabo sin más que leer lo que la máquina va escribiendo, no precisando para esta tarea ni libro de códigos ni el empleo de elemento adicional alguno. No parece pues que el mecanismo empleado se vea reflejado con demasiada fidelidad.

3.12. Аэлита – Aelita[40]

3.12.1. Resumen y Datos Técnicos

Película soviética del año 1924, basada en la novela homónima de Alexei N.Tolstoi. Fue dirigida por Yakov Protazanov y está interpretada en sus principales papeles por: Yuliya Sointseva (Aelita), Nikolai Tseretelli (Ingeniero Los), Valentina Kuindzhi (Natasha, esposa del ingeniero Los) y Pavel Pol (Viktor Ehrlich)

Ambientada durante la guerra civil rusa que tuvo lugar tras la revolución de 1917 y en particular en el año 1921 en Moscú que recibe miles de desplazados a consecuencia del conflicto.

En este entorno, el día 4 de diciembre, se recibe en todas las estaciones del planeta un curioso mensaje que parece estar encriptado y tener su origen en Marte. Ninguno de las criptoanalistas encargado de descifrarlo es capaz de hacerlo, pero esto no impide al ingeniero Los imaginar que se trata de una llamada de Aelita, reina de marte, solicitando ayuda; su obsesión además de arruinar su matrimonio, le llevará a construir la nave que lleva años diseñando y emprender el quimérico viaje en busca de Aelita.

3.12.2. Análisis

El mensaje recibido consiste en tres palabras: Anta, Odeli, Uta (Анта, одели, ута). No se nos muestran más detalles en la película hasta el final de la misma; en él, el ingeniero Los, de vuelta en la tierra tras su imaginario viaje a Marte, observa carteles pegados en las paredes que anuncian neumáticos con el mismo nombre que se recibió en la transmisión. Resulta pues que Anta, Odeli, Uta es una marca de ruedas y el mensaje una campaña publicitaria.

[40] (Sointeva, y otros 1924)

De lo anterior resulta que la presunta criptografía resulta ser falsa, no hay mensaje alguno tras lo recibido. En cuanto al papel que desempeña no pasa de ser un elemento más de la tramoya que sustenta el filme, las obsesiones del protagonista y una vía más para contar las bondades de una revolución que acababa de terminar y, como no podía ser de otra forma, del amor.

3.13. Swordfish – Operación Swordfish[41]

3.13.1. Resumen y Datos Técnicos

Película norteamericana del año 2001. Fue dirigida por Dominic Sena e interpretada en sus papeles principales por: Hugh Jackman (Stanley Jobson), Halle Berry (Ginger Knowles), John Travolta (Gabriel Shear) y Don Cheadle (Agente J.T. Roberts).

Stanley Jobson, hacker excarcelado, no puede acercarse a un ordenador si no quiere volver a prisión, pero recibe la visita de Ginger que tiene una oferta irresistible, una buena cantidad de dinero que le permitiría recuperar la custodia de su hija. Para ello sólo tiene que escuchar lo que su jefe, Gabriel, tiene que contarle.

La oferta no será otra que saltarse la seguridad de un banco y realizar algunos movimientos de fondos.

3.13.2. Análisis

Lo primero que señalaría en relación con esta película es que tanto los conceptos criptográficos como informáticos empleados dejan bastante que desear, si bien los primeros no son esencialmente incorrectos los segundos son empleados con una ausencia total de criterio y conectados los unos con los otros sin ninguna lógica real, los términos no son incorrectos pero se entremezclan sin concierto en lo que parece un intento de hacer creíble el discurso.

Palabras y conceptos como: TCP, IP, bits, encriptado, códigos, gusanos, caballo de troya, bomba lógica, hidra, conexión DS3, PDP10, compilación, IDS, puerto y algunos más, se mezclan a lo largo de la película como si de ensalmos, fórmulas o encantamientos se tratase y quienes hacen uso de ellos fuesen aprendices de mago intentando encontrar el orden correcto en el que debe realizarse la invocación.

Merecería la pena hacer una revisión de cada uno de ellos y como son empleados por los guionistas, pero eso se alejaría en exceso del objetivo de este trabajo que se centra en la criptografía, paso pues a revisar lo que hace referencia al objeto de esta exposición.

En cuanto a criptografía, a lo largo de la película aparecen dos conceptos directamente relacionado con ella, a saber:

- Encriptación o Cifrado Vernam
- Cuentas protegidas por un código de 1024 bits.

[41] (Jackman, y otros 2001)

Aparece además un tercero que, sin estar relacionado con la criptografía, si lo está con la privacidad, se trata del programa Carnivore.

Lo que acompaña a estas ideas o conceptos no suele ser correcto en la película, pero creo que merece la pena que haga una revisión, aunque sea esta somera, de la realidad hay tras ellos y así resarcir, aunque sea ligeramente, el maltrato sufrido en el filme.

Comienzo por el final, el sistema Carnivore; se trata de un sistema real, operado por el FBI entre 1995 y 2005 que fue sustituido por un sistema comercial. Diseñado para monitorizar comunicaciones y correos electrónicos; su funcionamiento era muy semejante al de un analizador de paquetes (sniffer) personalizable y que permitía la revisión de todo el tráfico de red a través del proveedor de servicios en el que estuviese instalado. Su instalación precisaba del respaldo de una orden judicial y, en teoría, el sistema estaba diseñado para discernir entre comunicaciones legales e ilegales, tratando sólo estas últimas[42]. En este sistema habría introducido Stanley un virus dejándolo inoperativo durante dos años, sería esta infección la que le llevaría a prisión.

Continuando con los elementos criptográficos mencionados y en primer lugar nos encontramos con la encriptación o cifrado Vernam; de ella en la película se dice lo siguiente:

—¿Qué clase de cifrado?

—Encriptación Vernam

—El código Vernam se destruye al aplicarlo, además de ser un auténtico cifrado de 128 bits

—512 bits

No hay duda de que el cifrado Vernam es real, lo que presenta más dudas es el resto de las afirmaciones incluidas en la conversación.

El cifrado al que se hace referencia en el párrafo anterior, recibe su nombre de Gilbert Vernam, ingeniero de AT&T que lo inventó en el año 1917. Es conceptualmente sencillo: combinamos el texto cifrado con una clave mediante una operación xor (or excluyente) y el resultado sería el texto cifrado que enviamos.

También recibe el nombre de cifrado de flujo debido a que la clave es un flujo de caracteres aleatorio o semialetorio, si bien inicialmente este flujo de caracteres se repetía siguiendo cierta frecuencia, lo ideal es que este sea único y de la misma longitud que el texto a cifrar. Se trata pues de un cifrado de clave simétrica, el receptor precisa aplicar la operación xor al texto cifrado y emplear el mismo flujo de datos para realizar el descifrado del texto y si aceptamos que la generación es aleatoria, la clave es única y diferente para cada mensaje que ciframos. Si la clave es completamente aleatoria, estaríamos ante el caso de libreta de un solo uso que Claude Shannon demostró como irrompible (Shannon 1949).

A continuación, un ejemplo sencillo empleando la herramienta cryptool2

[42] Más datos sobre este sistema pueden encontrarse en el Electronic Privacy Information Center (EPIC 2005), Enciclopedia Británica (Featherly 2015), Ordenadores y Portátiles (Ordenadores y Portátiles s.f.) y Wikipedia (Wikipedia 2022)

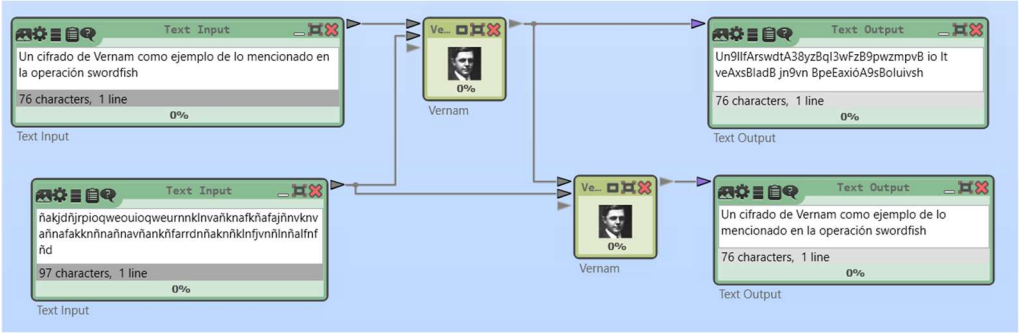


Imagen 23 – Cifrado de Vernam

En relación con el diálogo mencionado más arriba:

- La destrucción de la clave podría considerarse correcta siempre que estemos hablando de una clave aleatoria. A tener en cuenta que la clave que se destruye es la empleada para cifrar, debe existir, o ser posible recrearla, una copia adicional para la lectura de la información cifrada. En cualquier otro caso, resultaría imposible su lectura.
- ¿Código de 128 ó 512 bits? Si empleamos lo mencionado más arriba, la longitud dependerá del mensaje a cifrar, por tanto, no podemos saber si serán 128, 512, 1014 o cualquier número de bits. Si se menciona una clave de longitud fija que se emplea cíclicamente, la afirmación sería correcta pero el cifrado resultaría más débil que el obtenido con un flujo aleatorio continúo.

En segundo lugar y para finalizar con lo relativo a la encriptación, se hace mención en la película a ciertas cuentas cifradas empleando una clave (código) de 1024 bits; no haya más datos al respecto, podríamos pensar que la afirmación es correcta y teniendo en cuenta las limitaciones de los protocolos de clave simétrica, debería tratarse de algún tipo no identificado de clave asimétrica. El problema en este punto viene al final del diálogo, en él Stanley menciona que *"ni siquiera yo puedo cargarme el cortafuegos*", mezclar claves y cortafuegos no parece adecuado en este caso.

Para terminar este análisis no puedo resistirme a añadir un dato adicional que aun no estando relacionado con lo tratado me ha resultado interesante y simpático, en la película y antes de contratar a quién finalmente realizará la incursión, aparece un personaje finlandés de nombre Axl Torvalds que no puede ser otra cosa que un homenaje a Linus Torvalds; tal vez los guionistas no fueron muy duchos en el uso de la terminología propia de la informática y los sistemas de información, pero sin duda estudiaron al respecto y pusieron buena voluntad.

3.14. Windtalkers – Códigos de Guerra[43]

3.14.1. Resumen y Datos Técnicos

Película norteamericana del año 2002. Fue dirigida por John Woo e interpretada en sus principales papeles por Nicolas Cage (Joe Enders),

[43] (Cage, Beach, y otros 2002)

Adam Beach (Ben Yahzee), Christian Slater (Ox Henderson) y Roger Willie (Charlie Whitehorse).

Ambientada en la Segunda Guerra mundial y durante las operaciones norteamericanas en el Pacífico. Debido a la ruptura de los códigos norteamericanos por parte del ejército japonés, los primeros se ven obligados a cambiar de estrategia y deciden utilizar operadores de radio Navajos y códigos basados en el uso de su lengua. La película narra la historia de dos de estos cifradores y los sargentos encargados de protegerlos, o eliminarlos antes de que caigan en manos enemigas.

3.14.2. Análisis

Aunque los sistemas de cifrado norteamericas, basados en máquinas SIGABA, resultaron perfectamente seguros durante su uso en la segunda guerra mundial, los militares norteamericanos no consideraban practico su uso en determinadas situaciones. Por este motivo decidieron buscar opciones más sencillas, aunque resultasen más arcaicas.

Es en este contexto que la idea del ingeniero Philip Johnston tuvo su oportunidad. Dicha idea no era otra que emplear operadores de radio navajos para realizar dichas comunicaciones.

El concepto que subyacía en esta idea no era otro que la dificultad que encontraría cualquiera que escuchase la ecuchase para identificar en que idioma se estaba realizando y, por tanto, interpretarla.

Entre las condiciones que se establecieron para seleccionar el idioma que finalmente se emplearía se encontraban las siguientes:

- El número de hablantes debía ser suficiente para cubrir las necesidades del ejército
- La riqueza del idioma debía ser suficiente para cubrir la mayor cantidad posible de términos militares que deberían usarse durante las transmisiones.
- Los operadores debían contar con formación suficiente como para hablar y escribir en inglés con la competencia necesaria
- Para minimizar el riesgo de que el oponente conociese el idioma, el número de contactos entre miembros de la tribu y elementos ajenos a ella (excluyendo por supuesto a los norteamericanos) debería ser inexistente o muy pequeño.

Una vez establecidas estas condiciones las tribus candidatas quedaron reducidas a cuatro: Navajos, Sioux, Chippewa y Pima-Papagos *(Prieto, Manuel J., Historia de la criptografía (Spanish Edition) (p. 246). La Esfera De Los Libros*). Y de entre ellas, finalmente los Navajos fueron los seleccionados.

Para llevar a cabo las tareas enconmendadas, se elaboró un diccionario navajo-inglés-navajo que permitía transmitir directamente bastantes de los términos militares empleados en la época. Como ejemplo, en la película podemos ver como los operadores de radio son instruidos en el uso de dicho diccionario y podemos ver dos ejemplos

- *Tank (tanque)* se traducía por *“tortuga”* que a su vez en navajo quedaba representado como *Chay-da-gahi*

- *Artillery (artillería)* se traducía como *Many Big Guns (Muchas armas grandes)* que una vez traducido al navajo quedaba representado como *Be-al-doh-tso-lani*

Otros términos empleados fueron, por ejemplo:

- Avión de caza - Hummingbird (colibrí) - Da-he-t¡h-hi
- Avión de observación - Owl (búho) - Ne-as-jah
- Avión torpedo - Swallow (golondrina) - Tas-chizzie
- Bombardero - Buzzard (águila ratonera) - Jay-sho
- Avión de bombardeo en picado - Chicken Hawk - (halcón comepollos) Cini
- Bombas Eggs - (huevos) - A-ye-shi
- Vehículo anfibio - Frog (rana) - Chal
- Acorazado - Whale (ballena) - Lo-tso
- Destructor - Shark (tiburón) - Calo
- Submarino - Iron fish (pez de hierro) - Besh-lo (Singh 2000)

Como puede verse los términos empleados no tienen relación alguna con los términos que representan, centrándose el diccionario principalmente en palabras correspondientes a animales o plantas.

Por supuesto, no todos los términos podrían cubrirse de esta forma, para transmitir el resto de las informaciones no cubiertas por este diccionario, se estableció el envío el envío de las palabras deletreadas y para ello cada letra en inglés tenía asociado una palabra en inglés que a su vez se traducía al navajo; al recibirla, el operador navajo realizada la traducción inversa, pasando del navajo al inglés y empleando la primera letra para construir la palabra.

Con un sencillo ejemplo el uso quedará más claro, emplearemos para ello el término *attack*

A -> ant -> wol-la-chee

T -> turkey -> than-zie

T -> turkey -> than-zie

A -> ant -> wol-la-chee

C -> cat -> moasi

K -> kid -> klizzie-yazzi

El operador que recibía la información sólo debía realizar la traducción a la inversa para obtener el termino original.

El alfabeto así construido tenía el aspecto siguiente:

A - Ant (hormiga) - Wol-la-chee

B - Bear(oso) - Shush

C - Car (gato) - Moasi

D - Deer (ciervo) - Be

E - FJk (alce) - Dieh

F - Fox (zorro) - Ma-e

G - Goat (cabra) - Klizzie

N - Nut (fruto seco) - Nesh-chee

O - Owl (búho) - Ne-ash-jsh

P - Pig (cerdo) - Bi-sodih

Q - Quiver (carcaj) - Ca-yeílth

R - Rabbit (conejo) - Gah

S - Sheep (oveja) - Dibeh

T - Turkey (pavo) - Tfian-zie

H - Horse (caballo) - Lin	U - Ute (indio Ute) - No-da-ih
I - Ice (hielo) - Tkin	V - Victor (triunfador) - A-keh-di-glini
J - Jackass (burro) - Tkele-cho-g¡	W - Weasel (comadreja) - Gloe-ih
K - Khi (chaval) - Klizzie-yazzi	X - Cross (cruce) - Al-an-as-dzoh
L - Lamb (cordero) - Dibeh-yazzi	Y - Yucca (yuca) - Tsah-as-zih
M - Mouse (ratón) - Na-as-tso-si	Z - Zinc (zinc) - Besh-do-gliz

Cómo podemos ver en el ejemplo anterior, el mecanismo empleado tal y como se muestra resulta sensible a un ataque por análisis de frecuencias (siempre que quién escuchase fuese capaz de entender lo transmitido y transcribirlo); para evitarlo, ciertas letras empleaban varios términos homófonos en su transmisión.

A continuación, muestro un ejemplo de cómo quedaría un texto cifrado empleando este código, es posible gracias a que Cryptool dispone de una plantilla con el código navajo

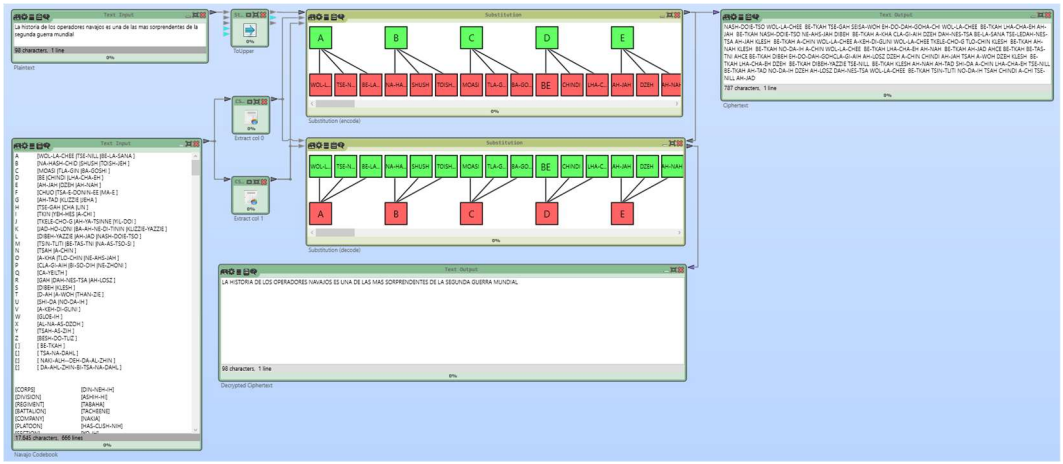


Imagen 24 – Ejemplo de código navajo

El primer uso del idioma navajo en este tipo de transmisiones se empleó, sin demasiado éxito, en la toma de Guadalcanal y su uso se extendió hasta la batalla de Iwo Jima donde se intercambiaron más de 800 mensajes empleando esta técnica.

Sin entrar en los detalles aquí explicados, la película hace uso correcto del procedimiento y aunque no se trate de uno de los ejes centrales de la misma, si representa con dignidad el papel de actor de reparto que el director le atribuye. En cuanto a la importancia del mecanismo empleado en el tiempo y circunstancias en que se emplea, sin duda no dejó de ejercer un papel, si no crítico, si importante en el desempeño de las acciones de guerra en las que se empleó.

3.15. Johnny Mnemonic[44]

3.15.1. Resumen y Datos Técnicos

Coproducción Estadounidense-canadiense del 1995 y basada en el relato homónimo de William Gibson. Fue dirigida por Robert Longo e

[44] (Reeves y Meyer 1995)

interpretada en sus principales papeles por Keanu Reeves (Johnny Mnemonic), Dina Meyer (Jane), Denis Akiyama (Shinji), Takeshi Kitano (Takeshi) e Ice-T (J-Bone).

Ambientada en un futuro distópico (el año 2021 en la película), las megacorporaciones controlan gran parte de las actividades mundiales y la información se ha vuelto ubicua.

Es esta presencia continua de información la que está causando a parte de la población una enfermedad llamada *Síndrome del Temblor Negro.* Jhonny es un mensajero con un implante cerebral capaz de almacenar 160 GB de datos que será encargado de transportar la que resulta ser la cura para dicha enfermedad.

3.15.2. Análisis

No es la criptografía elemento fundamental en esta película; si bien William Gibson y la corriente literaria que el contribuyó a crear (CiberPunk) y de la que es uno de los máximos exponentes hunde sus raíces en la tecnología y, en particular en la informática, no parece que sea la criptografía un elemento de importancia en este decorado.

Si bien los términos técnicos, inventados en su mayoría, son abundantes en la película, la encriptación o codificación de información sólo aparece en un par de ocasiones, la primera en el momento en el que Johnny almacena la información en su implante neuronal, es entonces cuando Johnny instruye a quienes le han contratado en el mecanismo que se empleará para “cifrar” la información y protegerla ante descargas no autorizadas:

- Tomar tres imágenes aleatorias antes de la finalizar la carga de datos
- Imprimir dichas imágenes
- Enviarlas por fax al receptor de información que hará uso de ellas como código de descarga.

Parece que estamos antes un sistema de cifrado de clave simétrica, basado en este caso en imágenes. La clave secreta debe ser transmitida al receptor que de otra forma no podría realizar la descarga ni descifrado de la información.

En un momento posterior de la película se habla de *códigos abrelatas*, códigos de descifrado que podrían basarse en ataques de fuerza bruta (*brute force*) para realizar la descarga o descifrado.

Hay que destacar en la película, como ya hace el autor del relato en casi todas sus obras, el tratamiento tridimensional y espacial de la información, la informática y las redes. De esta forma, la interacción con ellas debe realizarse no como estamos acostumbrados (teclados, monitores, etc.) sino empleando guantes, gafas de realidad virtual, etc. Parece pues que Gibson se adelantó en algunas décadas a la llegada del metaverso.

3.16. Mercury Rising – Al Rojo Vivo[45]

3.16.1. Resumen y Datos Técnicos

Película estadounidense del año 1998 basada en la novela *Simple Simon* del escritor Ryne Douglas Pearson. Fue dirigida por Harold Becker e interpretada en sus principales papeles por Bruce Willis (Art Jeffries), Miko Hughes (Simon Lynch), Kim Dickens (Stacey), Alec Baldwin (Nicke Kudrow) y Chi McBride (Tommy B. Jordan).

Simo Lynch es un niño afectado de autismo que tiene la capacidad de leer los mensajes encriptados con el más moderno de los códigos diseñados por la NSA, Mercury. Tras el asesinato de sus padres como consecuencia de esta increíble capacidad, sólo el agente del FBI Art Jeffries será capaz de protegerlo mientras trata de esclarecer el asesinato, encontrar a los responsables y mantener al niño con vida.

3.16.2. Análisis

La criptografía y el código aparentemente indescifrable inventado por la NSA y de nombre Mercury no es más que una excusa para contarnos la historia de amistad y cariño que se establece entre Simon y Art, Alfred Hitchcock lo hubiese definido, acertadamente en mi opinión, como un *Macguffin*.

Mercury es un nuevo sistema de encriptación de las comunicaciones y los datos que tiene como objetivo proteger los nombres de todos los agentes infiltrados del gobierno de los Estados Unidos y asegurar que sus comunicaciones sean seguras en cualquier circunstancia.

En la única escena de la película en la que vemos el sistema en funcionamiento, una aparatosa maleta convenientemente adornada con luces y varios dispositivos, tenemos la oportunidad de ver el mensaje en claro y el resultado una vez encriptado

WILL ARRIVE IN 12 HOURS

24lfjdk879:438yg93098y98y5085y49yt42-=yt=590y

En un par de escenas más, podemos ver el resultado de la encriptación, pero no su comparación con el mensaje original; en ambos casos el resultado es algo parecido a las conocidas *sopas de letras* con la diferencia de que en las que se muestran en la película está permitido el uso no sólo de letras y números, sino también de caracteres de puntuación, ortográficos y letras o caracteres griegos. En resumen, parece que el código resultante abarca no sólo ASCII sino que incluye caracteres adicionales.

Con la información disponible, me inclino a pensar que se trata de caracteres seleccionados al azar y tecleados con la intención de hacerlos lo más complicado posible.

Todo lo anterior me lleva a pensar que se trata de un código inventado con poca o ninguna base real e incorrecto, por tanto. De la importancia de

[45] (Willis, Dickens y Baldwin 1998)

este en el desarrollo de la acción, ya he comentado al principio que se trata de una excusa, un macguffin, que no tiene otra motivación que proporcionar un apoyo al desarrollo de la trama.

3.17. Snowden[46]

3.17.1. Resumen y Datos Técnicos

Película norteamericana del año 2016. Fue dirigida por Oliver Stone e interpretada en sus principales papeles por Joseph Gordon-Levitt (Edward Snowden), Melissa Leo (Laura Poitras), Shailene Woodley (Lindsay Mills) y Zachary Quinto (Glenn Greenwald).

En junio de 2013, Edward Snowden a través de los diarios *The Guardian* (Macaskill y Dance 2013) y The Washinton Post (The Washington Post 2013) desveló documentos clasificados pertenecientes a la NSA y relacionados con varios programas de vigilancia masiva. La película narra la historia de Snowden y como se produjo la filtración.

3.17.2. Análisis

La importancia de la criptografía en la película es menor, si bien se menciona en varias ocasiones a lo largo de su desarrollo, estas son anecdóticas. El núcleo principal se centra en la privacidad y como esta es vulnerada de manera reiterada por los estados en lo que se expresa como un intento por mantener a salvo a sus ciudadanos y la propia seguridad de estos; que para alcanzar estos objetivos deba vigilarse de manera continuada e intensiva a los mismos ciudadanos que se pretende proteger parece una cuestión secundaria y no sometida a discusión.

Si de criptología hablamos, a lo largo de la película se hace mención o se emplean varios mecanismos o dispositivos que la implementan o hacen uso de ella, a saber:

- Encriptación con clave simétrica (o secreta) de los documentos contenidos en la tarjeta de memoria que Snowden entrega a los periodistas
- Sistemas ENIGMA, SIGABA (National Museum of the United States Air Force s.f.) y la Línea Caliente (Teléfono Rojo) (Pérez-Desoy i Fages 2013) (Madridejos 2023) entre Washington y Moscú.
- Correo electrónico encriptado
- Diferentes sistemas sin especificar en la encriptación de comunicaciones

De los sistemas y mecanismos mencionados no se hace en la película ninguna descripción o explicación que nos permita saber si son correctos o incorrectos y si el uso que de ellos se hace es realista o no.

Si podemos saber, porque así se mencionado, que para codificar la información contenida en la tarjeta se hace uso de una clave, de longitud

[46] (Gordon-Levitt y Leo 2016)

y características desconocidas, simétrica que Snowden debe enviar a los destinatarios de la documentación antes de que estos puedan leerla.

Por supuesto, los sistemas históricos mencionados son reales, se emplearon en la Segunda Guerra Mundial y la Guerra Fría y hay abundante documentación sobre ellos, su uso y si fueron o no atacados con éxito.

En relación con el uso de un sistema de correo electrónico encriptado, su existencia y uso es sin duda real, son varios los sistemas que podemos emplear en la codificación de mensajes de correo y casi todos los sistemas en uso lo incluyen, siempre que se cuente con un certificado instalado en el equipo que enviará el mensaje que así lo permita. En cuanto a otros servicios que incluyan la encriptación de forma nativa, incluyo protonmail (Proton Mail s.f.) como uno de los más conocidos.

De manera directa o indirecta, en el desarrollo de la película se mencionan otros sistemas de cifrado y encriptación, sin entrar en ningún tipo de detalle acerca de los mismos.

Aunque no se trate de ningún sistema de cifrado, no puedo dejar de mencionar el lenguaje de signos para sordos que el protagonista y uno de sus compañeros emplean para despedirse poco antes de que Snowden abandone por última vez las oficinas de la NSA en Hawái. Sabedores de que las conversaciones se escuchan de manera habitual en dichas instalaciones, así lo atestigua la presencia de un micrófono en la habitación, emplean el lenguaje de signos para despedirse. Como decía, el lenguaje de signos no puede considerarse como un sistema de cifrado, aunque en el caso que mencionamos si permita que la comunicación entre los dos interlocutores se mantenga a salvo de escrutinios no deseados.

3.18. Tora! Tora! Tora![47]

3.18.1. Resumen y Datos Técnicos

Película norteamericana del año 1970. Fue dirigida por Richard Fleischer en las escenas relacionadas con el bando norteamericano y Toshio Masuda y Kinji Fukasaku para las escenas japonesas. Entre sus intérpretes principales destaco los siguientes, Martin Balsam (Almirante Kimmel), Sô Yamamura (Vice-almirante Yamamoto), E.G. Marshall (Tenient Coronel Bratton) y Tatsuya Mihashi (Comandante Genda).

La película narra con todo detalle la preparación y desarrollo del ataque japones a Pearl Harbor el día 7 de diciembre de 1941.

3.18.2. Análisis

No cabe ninguna duda sobre la importancia de la criptografía y el criptoanálisis en el desarrollo de la Segunda Guerra Mundial. La ruptura de los códigos alemanes de ENIGMA por parte de los británicos y el éxito norteamericano en el criptoanálisis de PURPURA, el equivalente japones de ENIGMA, resultarían a la postre determinantes en el curso del conflicto.

[47] (Balsam, y otros 1970)

No obstante, lo anterior y a pesar de que el código diplomático Japonés era en la fecha del ataque (diciembre de 1941) rutinariamente interceptado y traducido, no sirvió en esta ocasión para evitar el ataque japones a Pearl Harbor.

Debido a la importancia de lo aquí mencionado, a continuación, realizo un pequeño recorrido histórico por los sistemas de encriptación empleados por Japón en este periodo y los esfuerzos norteamericanos en su criptoanálisis.

Japón al igual que el resto de los países, comenzó a utilizar sistemas de encriptación electromecánicos y basados en el uso de rotores poco después de finalizada la Primera Guerra Mundial. No habiendo conflictos armados activos, el uso de las comunicaciones cifradas se circunscribía en la época y de manera mayoritaria a los mensajes diplomáticos. Es en este entorno y en febrero del año 1939 que el gobierno de Japón decide comenzar a emplear una nueva máquina de cifrado en sustitución de la empleada hasta entonces y conocida como *Máquina Roja* por parte del gobierno de los Estados Unidos. Esta no es otra que *PÚRPURA*.

PÚRPURA empleaba un diseño algo diferente a su homóloga alemana ENIGMA. Como motor de cifrado contaba con algo parecido a cuatro rotores, un clavijero y algún otro componente adicional, un teclado y una unidad de impresión (PRIETO 2020). El motivo por el que no se conoce con seguridad el diseño de PÚRPURA es debido a que, al contrario de lo ocurrido con ENIGMA, no se contaba con versiones comerciales del sistema lo que dificultaba la reingeniería del sistema.

En cuanto a la operación del sistema, la clave se cambiaba día a día.

En estas condiciones y como también pasaba en Europa, el descifrado de las claves dependía en parte de la suerte y no resultaba fiable. Sin embargo, algunos meses antes del ataque, los norteamericanos habían conseguido romper el código japones, aunque no eran capaces de leer todos los mensajes interceptados.

“Con ayuda de dispositivos de IBM y codificando en tarjetas perforadas los mensajes y las posibles configuraciones de la máquina, los estadounidenses buscaban ir conociendo las claves de configuración y por lo tanto los mensajes. Como vemos, una idea similar a la que se llevó a cabo en Bletchley Park. Si eran capaces de descubrir las claves de un día, y dado que sabían cómo funcionaban las máquinas del enemigo, podrían leer sus mensajes sin problemas. Cada vez que el libro de configuración era modificado, había que empezar de cero, más allá de la experiencia acumulada.” Prieto, Manuel J.. Historia de la criptografía (p. 233).

Empleando MAGIC, los norteamericanos eran pues capaces de descifrar los mensajes diplomáticos japoneses y así lo hicieron en las fechas anteriores al ataque, incluso más rápido de lo que podían hacerlo en la embajada japonesa en Washington. Tanto es así que la entrega prevista del mensaje por parte del embajador japonés debería haberse hecho como muy tarde a las 13:00 hora de Washington, es decir antes del ataque a Pearl Harbor.

A pesar de todo lo anterior y debido a que ninguna de las comunicaciones, salvo la enviada el día 7 de diciembre, contenía información precisa sobre las intenciones japonesas, no fue posible para los Estados Unidos

anticiparse al ataque; aunque el almirante Marshall envió ese día un mensaje a Pearl Harbor alertando del posible ataque, dicho mensaje no fue entregado a tiempo, no ya para evitarlo, incluso para minimizar los daños.

A todo lo anterior también contribuyó el hecho de que, aunque los norteamericanos si habían podido romper el código diplomático, no había ocurrido lo mismo con el naval, las comunicaciones de la marina japonesa continuaban siendo relativamente seguras por tanto.

Todo lo anterior aparece reflejado con bastante fidelidad y corrección en la película.

Para finalizar, muestro un ejemplo del aspecto que tendría un mensaje codificado con Púrpura, empleo para ello y como siempre Cryptool.

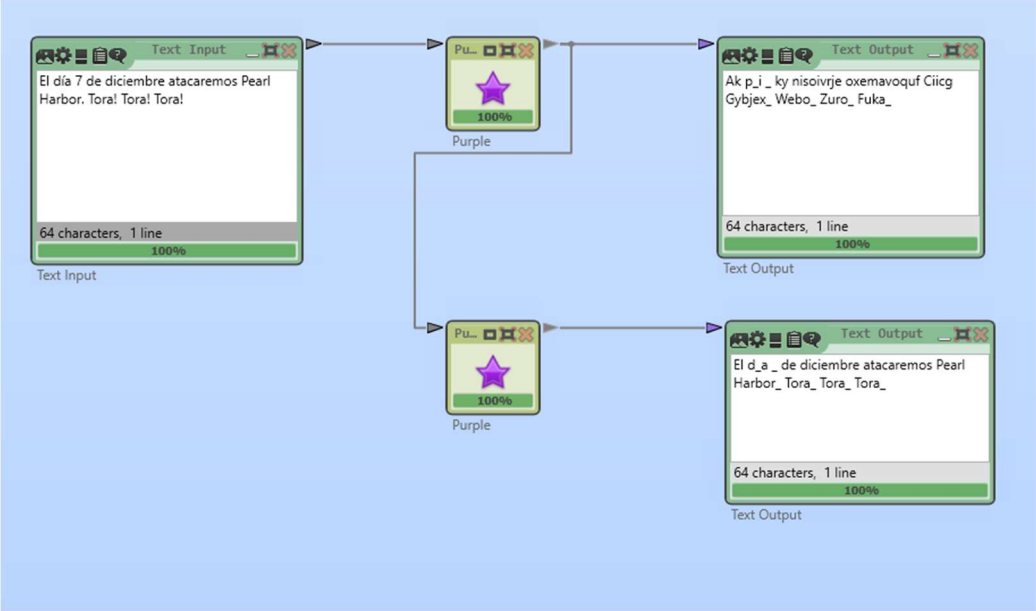


Imagen 25 – Ejemplo de uso de Púrpura

3.19. Zodiac[48]

3.19.1. Resumen y Datos Técnicos

Película norteamericana del año 2007, basada en el libro del mismo título de Robert Graysmith. Fue dirigida por David Fincher en interpretada en sus principales papeles por Jake Gyllenhall (Robert Graysmith), Mark Ruffalo (Ins. David Toschi), Robert Downey Jr. (Paul Avery) y Anthony Edwards (Ins. William Armstrong).

Basada en hechos reales cuenta la historia de la búsqueda del asesino en serie conocido como *"el asesino del zodiaco"*

3.19.2. Análisis

A finales de la década de los 60 del pasado siglo, la zona de la bahía de San Francisco sufrió varios asesinatos cometidos por el que sería

[48] (Gyllenhaal, Downey Jr. y Ruffalo 2007)

conocido como *"asesino del zodiaco"*. Al menos siete personas murieron a manos de este asesino en serie que hoy continua sin ser identificado.

La que probablemente sea la principal característica de este asesino y el motivo por el que he incluido la película entre las analizadas es debido a que el criminal empleó en varias ocasiones mensajes cifrados para dirigirse a la prensa.

El 1 de agosto de 1969 enviaba la primera de ellas, dividida en tres partes, a los diarios Vallejo Times Herald, San Francisco Examiner y San Francisco Chronicle. Cada una de las cartas contenía un tercio de un mensaje cifrado que el asesino invitaba a descifrar para conocer su nombre.

Un profesor de instituto y su esposa fueron quienes descifraron este primer mensaje que se trataba de una sustitución monoalfabética con homófonos, es decir cada una de las letras del alfabeto puede ser sustituida por uno o varios símbolos, el uso de varios símbolos tiene como objetivo dificultar el descifrado por análisis de frecuencias en caracteres comunes.

Tras ser descifrado, resultó que la afirmación de Zodiac era falsa, el mensaje resultante no contenía ni su nombre ni detalles sobre su identidad.

Una segunda carta enviada conteniendo 340 caracteres no pudo ser descifrada, la denominada Z340; al menos no durante la investigación.

Durante la pandemia el matemático australiano Sam Blake decidió intentar descifrar este último mensaje, contacto con el criptólogo norteamericano David Oranchak y un aficionado belga de nombre Jarl Van Eykcke y comenzaron el análisis. En el año 2021 Sam Blake anunciaría que habían podido romper el código y publicó el proceso seguido y el mensaje desencriptado. (Blake 2021)

En esta ocasión a la sustitución, el asesino parece que añadió la transposición para dificultar la tarea de ruptura del código. Idea que resultó efectiva ya que fueron necesarios más de 50 años y múltiples intentos para descifrarlo.

A continuación, incluyo el primer mensaje original, el texto en claro y los códigos de cifrado empleados.

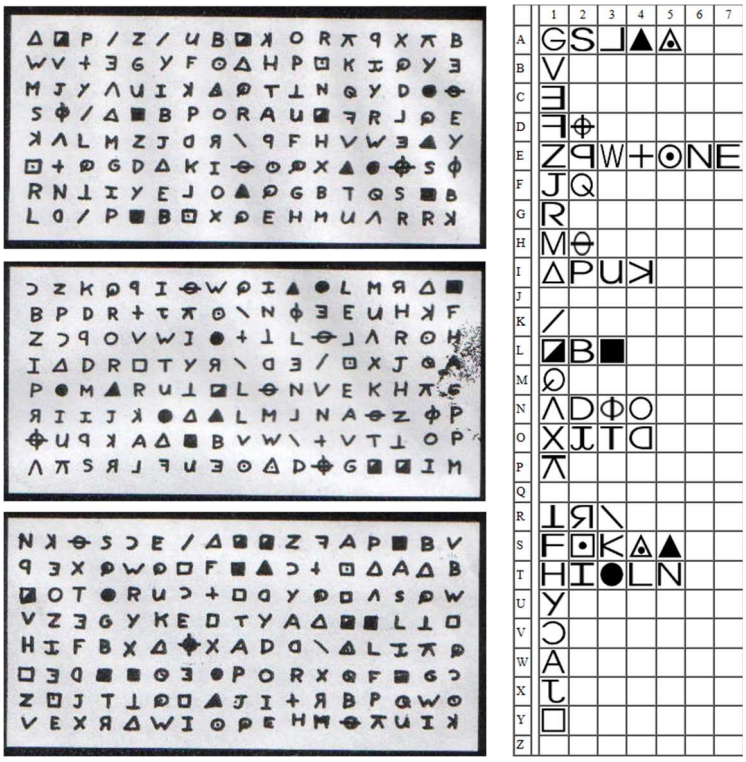


Imagen 26 – Primer mensaje de Zodiac y código empleado[49]

> I LIKE KILLING PEOPLE BECAUSE IT IS SO MUCH FUN IT IS MORE FUN THAN KILLING WILD GAME IN THE FORREST BECAUSE MAN IS THE MOST DANGEROUE ANAMAL OF ALL TO KILL SOMETHING GIVES ME THE MOST THRILLING EXPERENCE IT IS EVEN BETTER THAN GETTING YOUR ROCKS OFF WITH A GIRL THE BEST PART OF IT IS THAE WHEN I DIE I WILL BE REBORN IN PARADICE AND THEI HAVE KILLED WILL BECOME MY SLAVES I WILL NOT GIVE YOU MY NAME BECAUSE YOU WILL TRY TO SLOI DOWN OR ATOP MY COLLECTIOG OF SLAVES FOR MY AFTERLIFE EBEORIETEMETHHPITI

Imagen 27 – Primer mensaje de Zodiac descifrado[50]

En cuanto al segundo de los mensajes mencionados, Z340, también lo incluyo a continuación, así como la codificación y la propuesta de mensaje descifrado por Sam Blake y sus colaboradores.

[49] Las imágenes se pueden encontrar en (Blake 2021) y http://www.scn.org/anon/dossiers/zodiac/zodiac.htm
[50] El mensaje se puede encontrar en https://en.wikipedia.org/wiki/File:Zodiac_cipher.png

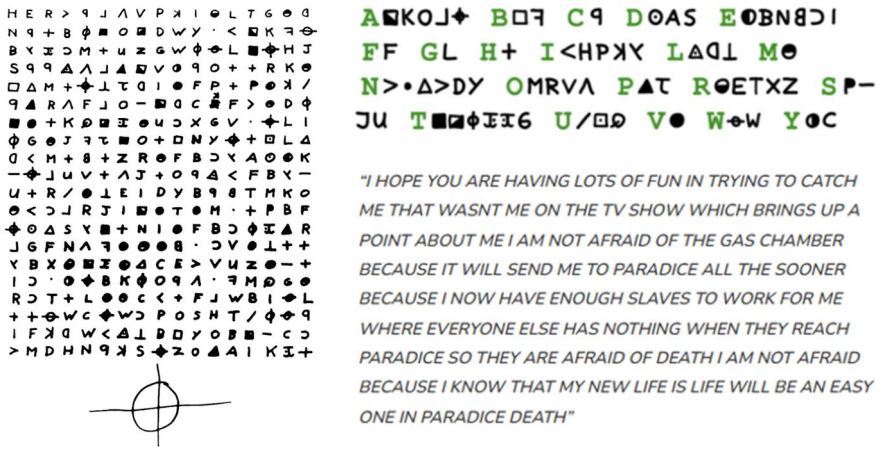


Imagen 28 – Segungo mensaje de Zodiac, código y mensaje en claro[51]

En cuanto a la película, que se centra en el trabajo desarrollado por el autor del libro y protagonista del filme Robert Graysmith, por entonces dibujante del San Francisco Chronicle y el inspector David Toschi encargado de la investigación, respeta con bastante fidelidad lo recogido más arriba en este análisis. En cuanto a los elementos criptográficos, estos se tratan con cuidado y corrección.

El personaje de Robert Graysmith, que también intentaría sin éxito el criptoanálisis de los mensajes, explica parte del proceso seguido:

- Análisis de frecuencias: *"¿cuál es la letra más usada en nuestro idioma?, la 'a' "*.
- Identificación del algoritmo de encriptado como un código de sustitución: *"como el que empleábamos cuando éramos boy scouts".*
- Búsqueda de puntales[52]: *"¿Qué palabra ha tenido que emplear al menos una vez?, matar[53]"*

Hay que destacar también algunos de los libros que aparecen mencionados en la película y que de una u otra forma contribuyeron bien al cifrado, bien a la lectura del texto

- Kahn, David «The Code Breakers». 1967.
- Laffin, John «Codes And Ciphers: Secret Writing Through the Ages». 1964.

En ambos casos se mencionan los libros como fuentes posibles de símbolos de los empleados por Zodiac.

Para terminar, quiero mencionar que parte de la información aquí recogida y algunos de los enlaces empleados, provienen del artículo escrito por Arturo Quirantes en su blog: *El profe de física* (Quirantes 2021), que además contiene una explicación clara y bastante simple del proceso seguido por

[51] Las imágenes pueden encontrarse en (Blake 2021)
[52] Empleo aquí la nomenclatura que ya aparece mencionada en el análisis de la película "Descifrando Enigma" y podemos encontrar en el libro de Simon Sigh (Singh 2000)
[53] Creo que resultará interesante incluir aquí lo escrito por Simon Sigh en su libro en relación con esta búsqueda de palabras posibles y el procedimiento seguido por Donald y Betty Harden en el análisis de la primera carta de Zodiac: *(…)"Donald y Betty Harden. Tuvieron la idea de entrar en la psicología de un asesino en serie que, según ellos, debía de tener un ego superdesarrollado. Para ellos, el mensaje debía de comenzar con la letra «I» que en inglés significa «Yo». Luego, la pareja buscó las palabras «kill» y «killing» [matar]." (…)* (Singh 2000),*(p. 140)*

Sam Blake y sus colaboradores para descodificar el segundo de los mensajes de Zodiac.

3.20. Midway – La Batalla de Midway[54]

3.20.1. Resumen y Datos Técnicos

Película norteamericana del año 1976. Fue dirigida por Jack Smight e interpretada en sus principales papeles por Charlton Heston (Capitan Matt Garth), Henry Fonda (Almirante Chester W. Nimitz), Glenn Ford (Vice-almirante Raymond A. Spruance) y Hal Holbrook (Comandante Joseph Rochefort).

Ambientada en la Segunda Guerra mundial y en las operaciones del Pacífico, la acción se centra en los preparativos y la batalla que tuvo lugar en torno al atolón de Midway. Dicha batalla significó, tras el ataque japones a Pearl Harbor, un cambio en el sentido de la guerra en el Pacífico.

3.20.2. Análisis

La importancia que la criptología, en este caso el criptoanálisis y la ruptura del código JN-25 por parte de los norteamericanos, desempeñó en las acciones que tuvieron lugar en el Pacífico y en particular en lo que hace referencia al combate naval que tuvo lugar en los alrededores del atolón de Midway es sin duda capital. Sin este criptoanálisis exitoso y tras la derrota sufrida por los norteamericanos en Pearl Harbor es muy probable que el curso de la guerra en el Pacífico y quizás en Europa hubiese sido diferente, si los norteamericanos hubiesen tenido que dedicar esfuerzos y efectivos extra a la defensa o reconquista del Pacífico, no hubiesen podido contribuir como lo hicieron a la guerra en Europa.

La película, sin entrar en demasiados detalles, muestra con claridad y bastante fidelidad el proceso seguido por la inteligencia naval norteamericana para descifrar, si no totalmente al menos si en los aspectos fundamentales, el plan y objetivos de la incursión japonesa en Midway.

No repetiré aquí los detalles ya descritos en el análisis de la película Tora! Tora! Tora!, que contienen los fundamentos del criptoanálisis de los códigos japoneses llevados a cabo por la inteligencia norteamericana, me limitaré a detallar los aspectos particulares que hacen referencia a la operación que debía llevarse a cabo en Midway.

La mencionada incursión se planifica en un momento en el que Tokio ha sido bombardeada por parte de los norteamericanos y Yamamoto considera imprescindible ampliar el perímetro defensivo de Japón; cree también que el archipiélago de Midway es un excelente punto desde el que los norteamericanos pueden realizar nuevas incursiones. La solución pasaría pues por tomar las islas, de esta forma, se ampliaría el perímetro defensivo, se reduciría la capacidad ofensiva norteamericana sobre

[54] (Heston, y otros 1976)

territorio japones y, si fuese posible, además, se asestaría un golpe a la ya muy mermada flota del pacífico.

Con todo lo anterior e ignorantes de que los norteamericanos eran capaces de descifrar, aunque sea de manera parcial su código JN-25 es cómo se plantea la que sería uno de los enfrentamientos decisivos en la guerra del Pacífico.

En resumen, el equipo del comandante Joseph J. Rochefort[55] había descifrado parcialmente un mensaje en el que se hablaba de *"fuerza de invasión"* y se mencionaba un indicador geográfico *AF*. Una posibilidad real era que AF fuese Midway, pero no se sabía con certeza, a favor de esta opción también se encontraba el Almirante Nimitz.

Era pues preciso determinar con exactitud si la suposición era correcta, en caso contrario otros posibles objetivos podrían quedar desguarnecidos. Se decidió hacer uso de un engaño; toda el agua potable de Midway provenía de una planta desalinizadora, se decidió emplear este hecho para enviar un mensaje falso y sin cifrar en el que se alertaba sobre una avería en dicha planta y posibles problemas en caso de no repararla a tiempo. Dos días después del envío de este mensaje, la estación de Hawái capturó y descifró un nuevo mensaje japonés en el que se mencionaban dichos problemas, con esta treta quedaba pues confirmado que AF era Midway.

Este éxito de inteligencia permitió a los norteamericanos enfrentar con éxito la incursión japonesa en Midway y cambiar el rumbo de la guerra en el Pacífico.

3.21. Resultados

El resumen de los datos que se muestran a continuación se encuentra en las tablas 5 y 6 en el epígrafe correspondiente a las tablas.

Las conclusiones de estos datos, en el apartado correspondiente a conclusiones.

[55] Comandante a cargo de la Unidad de Radio de la Flota del pacífico en Hawái. Curiosamente había llegado a este puesto debido a su afición a los crucigramas.

3.21.1. *Nacionalidad*

La nacionalidad de las películas se distribuye de acuerdo con lo mostrado en el gráfico siguiente.

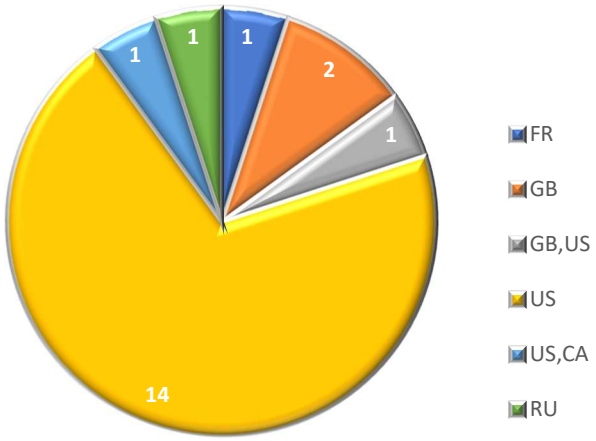


Imagen 29 – Películas por Nacionalidad

3.21.2. *Año de producción*

En cuanto al año de producción de las películas, el resumen se muestra a continuación.

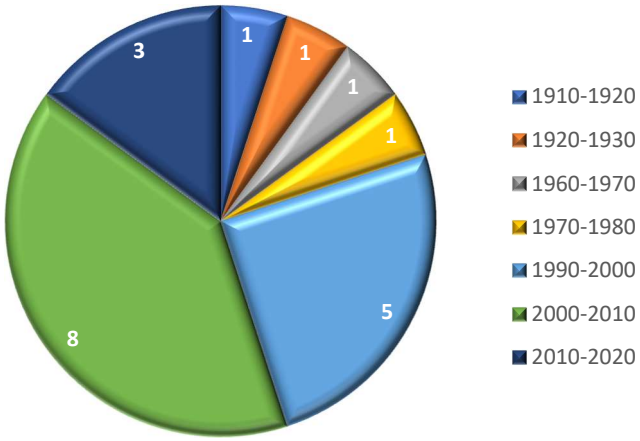


Imagen 30 – Distribución temporal

3.21.3. Papel

En relación con el papel jugado por la criptografía en las diferentes películas, los datos en el gráfico siguiente

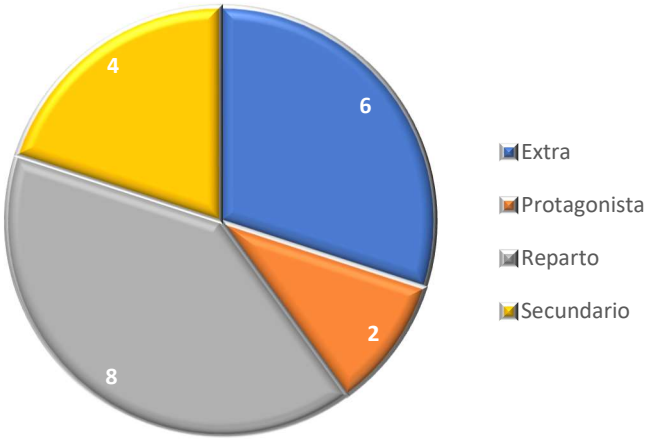


Imagen 31 – Distribución del papel de la Criptografía

3.21.4. Periodo

Los datos relativos al periodo (tipo de procedimiento criptográfico empleado) en el gráfico que sigue.

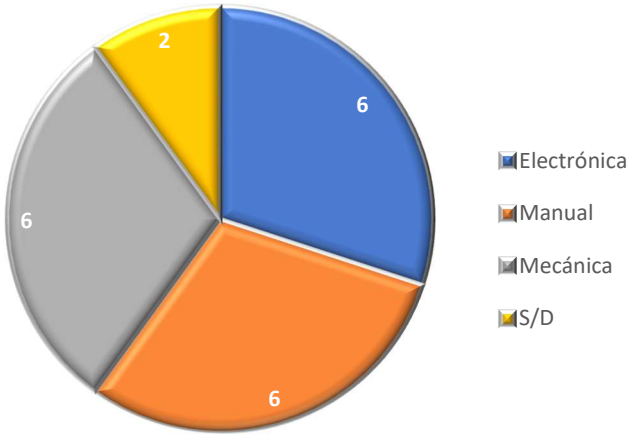


Imagen 32 – Procedimientos criptográficos empleados

3.21.5. Corrección

El número de películas que muestran con corrección las técnicas criptográficas, en el gráfico que sigue.

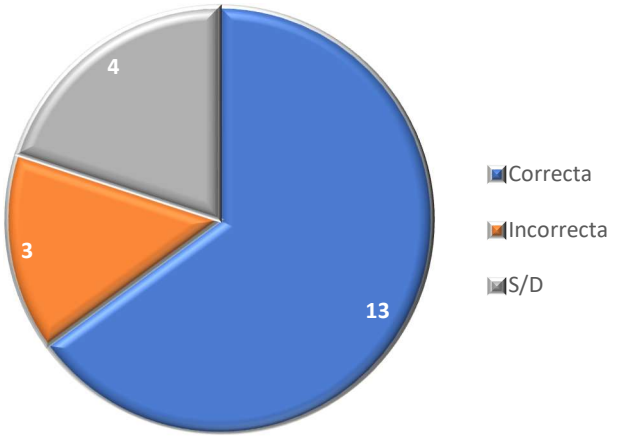


Imagen 33 – Correctas, Incorrectas y S/D

3.21.6. Existencia

¿Existe o existió lo propuesto en la película?

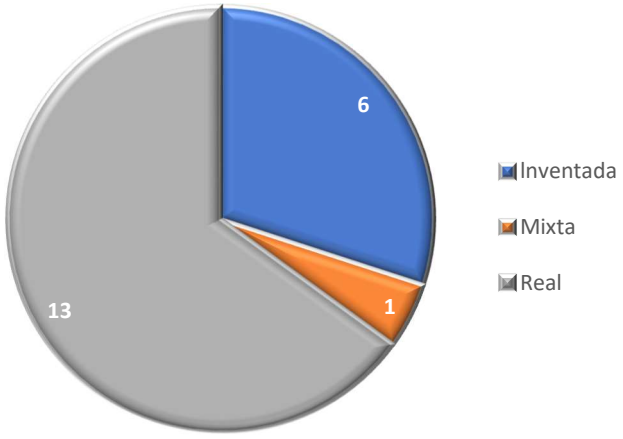


Imagen 34 – ¿Existe o existió lo propuesto?

3.21.7. Importancia

La distribución de los datos en relación a cuan importante resulta lo empleado en la película en el gráfico.

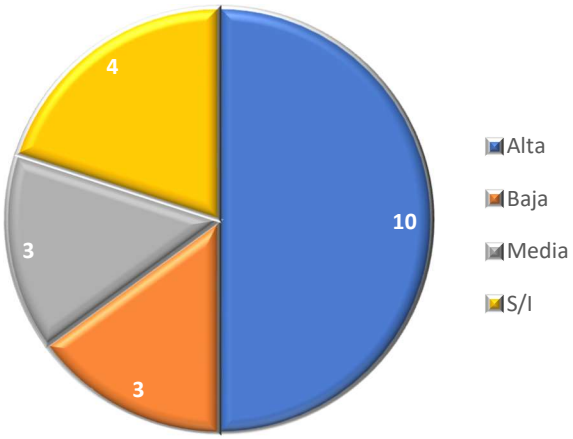


Imagen 35 – Distribución con base en la importancia

El resumen de los resultados obtenidos se incluye en la Tabla 3 al final del presente documento en el epígrafe correspondiente.

4. Conclusiones

Las conclusiones del presente trabajo son las siguientes:

4.1. Nacionalidad

La primera de las conclusiones señala que el inventario seleccionado tiene un fuerte sesgo en cuanto a la nacionalidad de las películas seleccionadas.

El 80% de las películas son norteamericanas, la siguiente nacionalidad con mayor representación es Reino Unido con el 15%, el resto de los representantes son Francia, Rusia y Canadá (en coproducción) con una película cada una de ellas; entre las películas hay dos coproducciones.

Sin desdeñar el hecho seguro de que la industria cinematográfica de los Estados Unidos es con toda probabilidad la más importante a nivel internacional, si me resulta sorprendente la influencia de este sesgo en mi selección. No he localizado o no he considerado lo suficientemente significativas las aportaciones que otras naciones con una industria también pujante: India, Corea, Hong Kong o con una tradición cinematográfica consolidada y de contrastada calidad como Reino Unido y Francia, hayan realizado al aspecto en el que se centra este trabajo.

La limitación en el número de películas analizadas, la poderosa mercadotecnia de la industria norteamericana, el sesgo en los buscadores y bases de datos de películas empleados o la calidad de las búsquedas realizadas también puede haber influido en el resultado obtenido.

Un inventario mucho más amplio que el mío podemos encontrarlo en el trabajo *"Análisis y uso didáctico de la representación de la criptografía en el cine"* de David Fajardo (FAJARDO RODRÍGUEZ 2023) que en su página 166 muestra los datos que incluyo a continuación.

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**

Imagen 36 – Distribución por nacionalidades en el trabajo de David Fajardo

Las tendencias que muestran los datos anteriores, sobre una muestra tres veces más amplía que la mía, no son esencialmente diferentes; la representación norteamericana se reduce al 65%, la británica se mantiene en el 15% y aparecen otras nacionalidades no presentes en mi inventario, pero sólo el 8,4% de las películas pertenecen a naciones fuera del ámbito que podemos llamar occidental (Norteamérica y Europa).

Con los datos anteriores, o bien mis suposiciones son ciertas o el interés por estos aspectos en otras cinematografías es menor[56]

4.2. Fecha de producción

Algo semejante a lo analizado en el punto anterior se repite en esta ocasión con las fechas de producción. En este caso el 80% de las películas han sido producidas desde el año 1990 en adelante y de ellas el 50% a partir del año 2000.

Atribuyo en esta ocasión el sesgo a la falta de información previa, a pesar de haber contado con recomendaciones por parte del tutor que incluían películas anteriores a 1970. Revisando artículos y enlaces, la gran mayoría de obras mencionadas son posteriores a la década de los 60's, lo que contribuye a dirigir la selección en este sentido.

Recurriendo de nuevo a la muestra de David Fajardo mencionada en el punto anterior; en este aspecto los datos son:

[56] Al hilo de lo aquí expuesto, destacaría también que, más allá de las dificultades del idioma, los libros y enlaces empleados son mayoritariamente occidentales y la práctica totalidad de los mecanismos criptográficos empleados o incluidos en la cronología también lo son. Parecería pues que el interés por esta disciplina, al menos hasta tiempos recientes, o bien ha sido más occidental o bien no estamos manejando información suficiente de otros usos y culturas.

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**

Imagen 37 – Distribución por año de producción en el trabajo de David Fajardo

Que no difieren de manera significativa de los obtenidos en mi caso.

Además del sesgo atribuible a los defectos o carencias en la búsqueda de información y referencias, se me ocurre que parte de este desequilibrio hacía fechas recientes tenga que ver, por una parte con la creciente e imparable influencia que la tecnología tiene en nuestro entorno, influencia a la que no escaparían las expresiones artísticas como el cine y por otra una tendencia a la revisión de momentos y personajes históricos, bien con la intención de mirarlos desde puntos de vista novedosos, como homenaje o como exaltación de lo acontecido.

4.3. Papel

En este caso, he atribuido el papel protagonista sólo en dos ocasiones: Enigma y Pi, por motivos diferentes, en el primer caso, no cabe duda de ENIGMA es el oponente, la némesis que a través del contraste sirve para destacar aún más la figura de Turing, sólo una mente genial podría imponerse a un oponente formidable.

En el segundo caso, Pi, el protagonismo sería de la obsesión, representada esta como el código que debe servir para interpretar lo oculto, no sólo la bolsa, el verdadero nombre de dios incluso.

En el resto de las películas y, como ya he mencionado en alguna ocasión anterior, la clasificación no puede ser sino subjetiva y allí donde yo veo secundarios otros podrían encontrar protagonistas o meros comparsas.

Entre los secundarios si me gustaría destacar el papel desarrollado por *"la caja negra"* en el caso de *Sneakers* y los criptogramas en el caso de Zodiac, en ambos casos se trataría de secundarios de lujo y que en algunos momentos compiten con otros protagonistas, pero no creo que sea suficiente para incluirlos entre los motores principales de la historia.

Señalaré también, como ya indicaba en los primeros apartados de esta exposición, que en el caso de las paranoias de John Nash son, sin ningún género de dudas, importantes, pero podrían haberse desarrollado de cualquier otra forma. Si lo hicieron en forma de códigos y patrones, tiene más que ver con la mente que las alumbró que con la importancia de estas.

En todas las películas desarrolladas en un entorno bélico, el papel que he atribuido a la encriptación, salvo el protagonista de *"Descifrando Enigma"*, es de reparto y todo ello a pesar de la importancia que el uso y ruptura de los códigos tuvo en este contexto, así lo reflejo en el apartado correspondiente a la Importancia; el papel de estos códigos no veo que deba ser diferente al de tantos hombres y mujeres sin nombre que desempeñaron este modesto, visto individualmente, pero crucial papel en la formidable tragedia que fue este conflicto.

4.4. Periodo

Poco hay que señalar en este punto, las técnicas empleadas se corresponden a lo que se encontraba en uso en las películas basadas en sucesos reales y en aquellas que no es así, como mencionaremos en varias ocasiones, la tendencia es a emplear técnicas sencillas de reproducir y que no precisen de explicaciones enrevesadas y complejas, no sería el caso de Pi que representó serias dificultades de interpretación, en mi caso al menos.

4.5. Corrección

Parto en este punto, de lo recogido al comienzo de esta exposición y expresado por Robert Krapp en su artículo *"Beyond schlock on screen…": "The problem with audiovisual representations of cybersecurity in particular and computer networks in general is that they are all too often turned into ludicrous caricatures on screen."* [57] (Krapp 2019)

Afortunadamente y una vez revisadas las películas incluidas en el catálogo, puedo afirmar que la corrección con la que son tratados los elementos criptográficos en las obras revisadas no han resultado ser las ridículas caricaturas que Krapp anunciaba; por supuesto, existen excepciones, la más destacada sería Operación Swordfish, pero incluso en este caso hay ciertos visos de realidad y corrección en lo expuesto, que la exposición misma resulte estrambótica, excesiva e irreal tampoco desentona con el tono general de la película, tal vez en este caso no podamos exigir rigor en este aspecto cuando casi todo lo mostrado carecen de él.

Algún otro caso he encontrado como Mercury Rising, pero tampoco cabría esperar más de lo allí mostrado.

En general la tendencia es hacía una mayor cuidado y corrección cuando el argumento de las películas hace referencia a personajes o hechos reales (episodios bélicos, biografías o películas como Zodiac) y esta tendencia se relaja en proporción inversa a la cantidad de acción que contenga el film, a mayor acción menor cuidado en los detalles; también parece lógico pensarlo así, si tu intención es que todo estalle entre fuegos de artificio, el espectador estará demasiado ocupado entre los estampidos y el humo como para fijarse en detalles nimios, de nuevo Operación Swordfish sería el mejor ejemplo.

[57] El problema con las representaciones audiovisuales de Ciberseguridad en particular y redes informáticas en general es que con demasiada frecuencia se convierten en la pantalla en ridículas caricaturas"

No me parece descabellado pensar que el esfuerzo de los guionistas, productores y directores por reflejar la realidad en el primero de los casos mencionados, se extienda de manera natural a los mecanismos criptográficos empleados, mientras que en el segundo caso, el foco se centra en la acción y el empleo de la criptografía no es más que un recurso adicional para mantener una elevada tensión sin importar por tanto cuan correcta o incorrecta resulte; no se diferencia en este caso el tratamiento que recibe este recurso del que recibe en los mismas películas una persecución imposible o la supervivencia del protagonista a una caída o actividad particularmente peligrosa.

Señalar por último que, también de acuerdo con lo supuesto el comienzo del presente trabajo, resulta más sencillo ser preciso con técnicas y algoritmos más fáciles (cifrados de sustitución, etc.) que serlo cuando se habla de un dispositivo tan complejo como lo fue ENIGMA o se presupone que debería serlo la *caja negra* de *Sneakers.*

4.6. Existencia

Este punto resulta claro en aquellos casos en los que lo mostrado en la pantalla corresponde a dispositivos, algoritmos, procesos u operaciones que tuvieron existencia real y sucedieron, libertad creativa aparte, de una forma aproximada a como se nos muestra en la pantalla. Entrarían en esta categoría todas las películas en las que aparece ENIGMA, de una u otra forma, o las que mencionan PÚRPURA, también entraría en esta categoría Zodiac.

En el resto de las películas, hay de los dos tipos: reales e inventadas. Sólo considero destacables de entre ellas: *Pi* por la complejidad de lo expuesto y *Sneakers* por tratarse de una predicción que, en nuestros días, está cercana a cumplirse, al menos en lo que respecta a los mecanismos criptográficos actualmente en uso.

4.7. Importancia

Entendiendo este apartado tal y como lo expresé al comienzo de este trabajo: el mecanismo mostrado resultará importante o no siempre en relación con la historia que se cuenta en pantalla, no añadiré aquí conclusiones adicionales a las ya incluidas en cada uno de los análisis individuales.

4.8. Otras conclusiones

4.8.1. Crucigramas

Resulta interesante que, en al menos cinco de las películas revisadas, una más si consideramos lo que mencionaremos más adelante sobre Mercury Rising, aparecen, de una u otra forma, los crucigramas en el desarrollo de la acción. A lo anterior, podemos además añadir que al menos en un caso, el de Joseph J. Rochefort responsable del criptoanálisis del código JN-25 en la estación HYPO (PRIETO 2020), p.236, uno de los protagonistas alcanzó

el puesto que se representa a consecuencia de su afición a estos pasatiempos.

En el caso de "Enigma" y "Descifrando Enigma", la presencia de crucigramas es destacada ya que, en ambas, la selección de parte del personal que deberá trabajar en la tarea de romper *Enigma* es seleccionada en primera instancia a través de un concurso publicado en un conocido diario británico y asociado a la resolución de un crucigrama particularmente complejo[58].

Además de en las películas mencionadas en el párrafo anterior, contamos con la presencia de crucigrama en, al menos, las películas siguientes:

- Una Mente Maravillosa
- Contacto
- Sneakers

Un pasatiempo algo diferente y parecido a una sopa de letras se revela de importancia en otro de las películas analizadas, en este caso Mercury Rising.

Pero ¿existe una relación entre los crucigramas y la criptografía? y si existe ¿cuál es?

En este sentido, en el artículo *Taller de criptomatemáticas para jóvenes (y adultos)* (Hernández Encinas 2000), en la primera página encontramos la nota siguiente: *"(…) mientras que el criptoanálisis es el "Arte de descifrar criptogramas", siendo un criptograma una "Especie de crucigrama en el que, propuesta una serie de conceptos, se han de substituir por palabras que los signifiquen, cuyas letras, trasladadas a un casillero, componen una frase.""*

También puedo afirmar que un crucigrama es una forma eficiente de ocultar información "secreta" a la vista de todos, sólo quién conozca la clave (3 horizontal, p.e.) sería capaz de desentrañar el mensaje secreto enviado y, desde este punto de vista, podríamos encontrarnos ante un cifrado Ottendorf. En este punto y como curiosidad, podemos mencionar la detención del profesor Leonard Dawe por parte de agentes del MI5 británico en los días anteriores al desembarco de Normandía para investigar la posibilidad de que algunos de los crucigramas elaborados por él y publicados en el diario británico *The Telegraph* incluyesen información sensible sobre el desembarco entre sus soluciones (Lara 2018).

Parece pues que dicha relación existe y su uso en algunos de los filmes analizados refuerza la conexión entre criptografía y la historia narrada.

4.8.2. Importancia de los errores en la ruptura de códigos.

En varias de las películas analizadas se muestra la importancia, en la ruptura de los códigos, de los descuidos y errores humanos cometidos por sus diseñadores u operadores.

Así por ejemplo en el caso de ENIGMA, se señalan en varias ocasiones la existencia de *cillis*, configuraciones de los rotores repetitivas o previsibles que permitieron a los británicos intuir o suponer posibles

[58] Una copia del original publicado en el Daily Telegraph puede encontrarse en la página 207 del libro de Simon Singh "Códigos Secretos" (Singh 2000)

configuraciones; volviendo al caso de enigma el uso de *pilares*[59], también contribuyo a esta tarea, de la misma forma las limitaciones en el uso del clavijero, disposición de los rotores y otras operaciones semejantes contribuyeron de manera decisiva a la ruptura del código.

Otro ejemplo lo tendríamos en el caso de Mercury Rising, la publicación del código en una revista de pasatiempos tiene el efecto de mostrar las debilidades del código empleado, para una mente particularmente dotada para esta tarea como sería el caso del niño que protagoniza el fime.

Tal vez los diseñadores de algoritmos de encriptación deberían tener en mayor consideración los errores que cometerán aquellos que deban hacer uso de ellos; es mucho el cuidado que se pone en la prevención de errores inherentes al algoritmo, pero no estaría de más dedicar algún tiempo a tratar de protegerlos de la mayor o menor incompetencia de quienes deberán servirse de ellos.

La conclusión podría ser que no existe artefacto ni invento humano resistente a la capacidad de generar errores de aquellos que deberán usarlos.

4.8.3. Inteligencia y otras tareas asociadas.

Si dedicaba el apartado anterior a los errores, en este reflexionaré, aunque sea brevemente sobre la importancia, también mostrada en varias de las películas revisadas, de las tareas de inteligencia en todo lo relativo al uso y ruptura de los códigos.

Disponer de una buena inteligencia facilitará, junto a los errores mencionados en el punto anterior, o provocándolos como veremos algo más adelante en este mismo apartado, la tarea ya de por si compleja de los criptoanalistas.

Volviendo de nuevo a ENIGMA, no fueron pocas las operaciones realizadas con el objetivo de recuperar dispositivos y libros de códigos, todas ellas ayudarían de manera significativa en el descifrado del sistema. Mención aparte merecen las tareas, también vinculadas a inteligencia, que hicieron posible ocultar dicho desciframiento a los alemanes, que en varias ocasiones atribuyeron a la casualidad o la mala fortuna las pérdidas y fracasos directamente atribuibles a unas comunicaciones vulneradas.

Pero no sólo se trataría de ENIGMA, en el caso de PÚRPURA y el código naval japones sucedió algo parecido y la treta empleada por los norteamericanos en Midway no es atribuible a sus criptógrafos, sino más bien a su personal de inteligencia.

Fuera de las películas bélicas, merece especial atención lo mostrado en Sneakers donde las tareas de inteligencia e infiltración resultan entretenidas, divertidas y brillantes.

[59] Palabras conocidas que se suponían incluidas en un lugar específico dentro de un mensaje encriptado con ENIGMA, por ejemplo; tiempo (wetter), Hail, Hitler y otras

5. Trabajos futuros

Han quedado pendientes multitud de películas en las que, de una forma u otra, la criptografía y los códigos tienen presencia. Sin ir más lejos, en este propio trabajo, el número inicial de películas era algo más elevado, de las 25 previstas inicialmente han sido 20 las finalmente revisadas. Este punto me permitiría ampliar la búsqueda para tratar de incluir aquellas nacionalidades que no se han visto representadas en este o, si en caso de haberlo sido, el número ha sido casi insignificante. Lo mismo aplicaría a los años en que estás han sido producidas, merecería la pena sin duda pasar revista, o intentarlo al menos, a la evolución que estas técnicas han tenido a lo largo de la historia del cine.

La representación que iniciativas y tecnologías modernas, como podrían ser la computación cuántica o blockchain, no aparecen y si lo han hecho su presencia ha sido meramente anecdótica o residual; a pesar de ello, el número de películas y documentales en relación con estas no hace más que crecer. Esta sería pues otra vía para ampliar el presente trabajo, aunque en el caso de los documentales sería de esperar que la fidelidad con la que se muestren los mecanismos y usos de las diferentes tecnologías sea más elevada de la encontrada aquí, principalmente debido a que se tratan de formatos que aun siendo audiovisuales son radicalmente diferentes.

Si en el primer caso, blockchain y monedas asociadas, parece que las previsiones iniciales se resisten a verse cumplidas y, con el conocimiento del que dispongo, las monedas tradicionales continúan contando con una *mala* salud de hierro; debemos esperar para ver cómo evoluciona la segunda, computación cuántica, y confirmar si en esta ocasión las previsiones aciertan y se produce el cambio que todos hace ya algún tiempo se apresuraron en anunciar.

De ser así, parece que la criptografía deberá enfrentarse a nuevos retos y reinventarse para afrontarlos. No me cabe duda de que la inventiva y genialidad humana, encontrará la vía para continuar protegiendo aquello que es preciso preservar de las miradas indiscretas. Continuará así la carrera de persecución continua que parece haber regido esta disciplina desde su nacimiento, o tal vez se trate de evolución y no de persecución y los continuos esfuerzos por romper códigos no hagan otra cosa que mejorar los existentes; mientras que estas mejoras, a su vez, sirven de acicate para que los interesados en romperlos no hagan sino mejorar y ambos se encarguen de mantener la rueda girando.

De lo que no me cabe duda es del potencial de ficción que este tipo de tecnologías representará, como muestra basta con asomarse a series como *Devs* y *Mr. Robot*.

Otras posibles vías para continuar con la presente investigación y siempre dentro del ámbito audiovisual serían:

- Series
- Películas de Animación
- Películas Indias, Orientales, españolas

Ampliando el rango, otros caminos para completar el el presente pasan por la revisión de la presencia de criptografía, códigos y cifrados en otros ámbitos de la actividad artística.

- Literatura
- Pintura
- Música

Parece pues que las posibilidades de continuar realizando análisis análogos al presente son múltiples, sólo restaría encontrar el tiempo

6. Tablas

6.1. Análisis de Riesgos

Nº	*Riesgo*	*Descripción*	*Prob.*	*Impacto*	*Resultado*	*Medidas de Mitigación*
1	Medios no disponibles	Imposibilidad de localizar alguna de las películas incluidas en el inventario y que deba ser considerada	A	A	**A**	En primera instancia, ampliar la búsqueda incluyendo la posibilidad de adquirir o alquilar el filme, visionarlo en idioma original, subscripción a plataformas, etc. En caso de que esta segunda búsqueda o búsqueda ampliada resulte infructuosa se deberá plantear la sustitución del filme por alguna alternativa. En este punto, podría plantearse la existencia de películas de reserva que podrían emplearse en este caso o en algún riesgo que se menciona posteriormente.
2	Falta de documentación y/o referencias	Imposibilidad de localizar referencias que permitan identificar correctamente los mecanismos criptográficos empleados en las diferentes películas analizadas.	B	A	**M**	En este caso se recurrirá al soporte del tutor y en caso de no poder identificarlo con su ayuda, sería posible recurrir a una explicación parcial o eliminar la película del inventario
3	Definición de objetivos poco claros, irreales o en exceso ambiciosos	La definición de objetivos puede caer en el uso de conceptos demasiado amplios o genéricos que desvirtúen el resultado final. También podría darse el caso de que los objetivos planteados resulten irreales o ambiciosos en exceso, desde el punto de vista que los medios y recursos planteados impidan alcanzarlos tal y como han sido planteados	MB	MA	**B**	Los objetivos se han trabajado en esta primera PEC y se revisarán durante la elaboración del trabajo, además serán consensuados con el tutor. Si fuese preciso se buscará la vía para reorientarlos, modificarlos o sustituirlos.
4	Falta de tiempo	Además de la realización del presente trabajo, curso una asignatura adicional; aparte por supuesto de mis obligaciones laborales y familiares. Lo anterior podría resultar en que el tiempo disponible para realizar el presente se viese afectado	B	A	**M**	Buscaría alternativas para aumentar la dedicación al presente, si no resultase posible, se planteará la situación al tutor buscando alternativas, en el peor de los casos se plantearía la opción de reducir el alcance.
5	Falta de conocimiento	Parte del desarrollo del presente se basa en obtener los conocimientos necesarios que permitan identificar los mecanismos criptográficos y determinar si son reales, inventados, correctos o incorrectos.	MB	A	**B**	El mecanismo de mitigación es semejante al expuesto en el punto 2
6	Inventario inadecuado	El inventario de películas que se esboza en esta primera PEC y se definirá en detalle al comienzo de la segunda, podría resulta inadecuado, tanto por contenido como por	MB	M	**MB**	El inventario se consensuará con el tutor, adicionalmente y como ya se ha mencionado en un punto anterior, se plantea ahora incluir en el

Nº	Riesgo	Descripción	Prob.	Impacto	Resultado	Medidas de Mitigación
		extensión, pudiendo ser esta corta o demasiado extensa, influyendo esta última posibilidad varios de los riesgos indicados más arriba				inventario definitivo un conjunto de películas de reserva que podrá emplear en caso de necesidad, bien para sustituir alguno de los filmes incluidos, bien para ampliar el listado en caso de necesidad. Si fuese precisa la reducción, se realizará asegurando que las películas restantes son suficientes para cubrir los objetivos indicados.
7	Imposibilidad de continuar el TFM por causas de fuerza mayor	En este punto se incluyen todas aquellas situaciones que graves e inesperadas dificultarían seriamente la continuidad del proyecto; entre ellas incluyo: enfermedad, acontecimientos familiares o laborales, situaciones externas fuera de control, etc.	MB	MA	**MB**	Se tratará con el tutor para tratar de encontrar una solución.

Tabla 4: Análisis de Riesgos

6.2. *Inventario de Películas*

Nº	Título	País[60]	Año	IMDB/Filmaffinity	Plataforma
1	The Imitation Game	GB	2014	https://www.filmaffinity.com/es/film617730.html	https://tinyurl.com/2a9owdga
2	Enigma	GB,US[61]	2001	https://www.imdb.com/title/tt0157583/?ref_=fn_al_tt_1	Préstamo
3	Una mente maravillosa	US	2001	https://www.filmaffinity.com/es/film326587.html	https://tinyurl.com/2kkeq2np
4	Contacto	US	1997	https://www.filmaffinity.com/es/film815526.html	https://tinyurl.com/2mayfq3l
5	Sneakers	US	1992	https://www.filmaffinity.com/es/film233071.html	https://tinyurl.com/2hnsevc5
6	National Treasure (La Búsqueda)	US	2004	https://www.filmaffinity.com/es/film721724.html	https://tinyurl.com/2p4yyl4a
7	El Código Da Vinci	US	2006	https://www.filmaffinity.com/es/film306442.html	https://tinyurl.com/2ocfxvnp
8	Pi	US	1998	https://www.filmaffinity.com/es/film679822.html	https://tinyurl.com/2mwr8hj5
9	U-571	US	2000	https://www.imdb.com/title/tt0141926/	https://tinyurl.com/2k87rp3o
10	Les Vampires (Parte 3)	FR	1915	https://www.imdb.com/title/tt0006206/	https://tinyurl.com/2p8oxokd
11	El Topo	GB	2011	https://www.filmaffinity.com/es/film274340.html	https://tinyurl.com/2glrhyjt
12	Aelita	RU[62]	1924	https://www.filmaffinity.com/es/search.php?stext=aelita	https://tinyurl.com/2htshadw
13	Operación Swordfish	US	2001	https://www.filmaffinity.com/es/film857439.html	https://tinyurl.com/2mya4wys
14	Windtalkers	US	2002	https://www.filmaffinity.com/es/film957874.html	https://tinyurl.com/2m75pwng
15	Jhonny Mnemonic	US	1995	https://www.filmaffinity.com/es/film222381.html	https://tinyurl.com/2e7v4s77

[60] Para identificar los países de procedencia de las películas, empleo el código ISO obtenido en la web de la Agencia Tributaria (https://tinyurl.com/2arzyrjc) (Tributaria 2022) que también puede consultarse en Wikipedia (https://tinyurl.com/yeooga6s) (Wikipedia 2023)
[61] Se trata de una coproducción entre Reino Unido, Estados Unidos, Alemania y Países Bajos
[62] Se trata de una película de la Unión Soviética (URSS), empleo el código moderno que corresponde a la Federación Rusa.

Nº	Título	País[60]	Año	IMDB/Filmaffinity	Plataforma
16	Mercury Rising	US	1998	https://www.filmaffinity.com/es/film830550.html	https://tinyurl.com/2dtju6cl
17	Snowden	US,CA	2016	https://www.filmaffinity.com/es/film892502.html	https://tinyurl.com/2htvj2dj
18	Tora! Tora! Tora!	US	1970	https://www.filmaffinity.com/es/film240724.html	https://tinyurl.com/2oxhsn7v
19	Zodiac	US	2007	https://www.filmaffinity.com/es/film300908.html	https://tinyurl.com/2q2o7mje
20	La Batalla de Midway	US	1976	https://www.filmaffinity.com/es/film914270.html	https://tinyurl.com/22xfdelh

Tabla 5: Inventario de Películas

6.3. *Resultados*

Nº	Título	Papel[63]	Técnica			Importancia[64]
			Periodo[65]	Existencia[66]	Correccion[67]	
1	The Imitation Game (Descrifrando Enigma)	Protagonista	Mecánica	Real	Correcta	Alta
2	Enigma	Secundario	Mecánica	Real[68]	Correcta[69]	Alta
3	A Beautiful Mind (Una Mente Maravillosa)	Reparto	S/D	Inventada	Incorrecta	Alta
4	Contact (Contacto)	Reparto	Electrónica	Real	Correcta	Baja
5	Sneakers	Secundario	Electrónica	Inventada	S/D	Alta
6	National Treasure (La Búsqueda)	Secundario	Manual	Real	Correcta	S/I
7	El Código Da Vinci	Extra	Manual	Mixta[70]	Correcta	S/I
8	Pi	Protagonista	Manual	Inventada[71]	S/D	Alta
9	U-571	Reparto	Mecánica	Real	Correcta	Alta
10	Les Vampires	Extra	Manual	Real	Correcta	Baja
11	El Topo	Extra	Electro-Mecánica	Real	Correcta	Baja
12	Aelita	Extra	S/D	Inventada	Incorrecta	S/I
13	Operación Swordfish	Secundario	Electrónica	Real[72]	Correcta[73]	S/I

[63] Protagonista, Secundario, Reparto, Extra
[64] Alta, Media, Baja, Sin Influencia (S/I)
[65] Manual, Mecánica, Electrónica, Cuántica
[66] Real, Inventada
[67] Correcta, Incorrecta, S/D (Imposible determinarlo)
[68] Es la segunda película del inventario basada en el dispositivo Enigma, sin duda su existencia es real, cosa diferente es el tratamiento que se da en la película a ciertos aspectos; por ejemplo, no he localizado información ni confirmación en relación con el uso de dispositivos TypeX en el descifrado diario de los mensajes de Enigma
[69] Más allá de los errores mencionados en el análisis que hacen referencia más a su uso y procedimiento de empleo y desencriptado que a su funcionamiento.
[70] Señalo que la existencia es Mixta debido a que en la película se mezclan elementos inventados, como el criptex, con elementos con existencia real, aunque no estén directamente conectados con la criptografía.
[71] A pesar de que lo mostrado en la película es, sin duda, inventado, en varios momentos de la película se hace mención a la Gematría, numerología Hebrea que establece una correspondencia entre los símbolos del alfabeto hebreo números.
[72] Hago referencia en este punto a lo analizado en relación con los mecanismos de cifrado y con un criterio amplío. Sin duda el resto de usos y terminología resultan bastante alejados de la realidad.
[73] De nuevo, hago referencia en este punto a todo lo relativo a la criptografía y ateniéndome a lo incluido en el análisis.

Nº	Título	Papel[63]	Técnica			Importancia[64]
			Periodo[65]	Existencia[66]	Correccion[67]	
14	Windtalkers	Reparto	Manual	Real	Correcta	Media
15	Jhonny Mnemonic	Reparto	Electrónica	Inventada	S/D	Alta
16	Mercury Rising	Extra	Electrónica	Inventada	Incorrecta	Media
17	Snowden	Extra	Electrónica	Real	S/D	Alta
18	Tora! Tora! Tora!	Reparto	Mecánica	Real	Correcta	Alta
19	Zodiac	Reparto	Manual	Real	Correcta	Media
20	La Batalla de Midway	Reparto	Mecánica	Real	Correcta	Alta

Tabla 6: Resultados

7. Glosario de Términos

A

Anagrama
Según el diccionario de la R.A.E
Cambio en el orden de las letras de una palabra o frase que da lugar a otra palabra o frase distinta., 38
ataques de fuerza bruta
En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso, 56
Atrezo
Utilería. Conjunto de elementos que se emplean en una película, obra de teatro o representación escénica, para prestar verosimilitud a las escenas que en ellas se desarrollan., 48

B

Beale, cifrado
Véase Cifrado Ottendorf., 21
Biopic
Acrónimo construido con los términos ingleses biographical y picture que traducido al castellano sería Película Biográfica, 21
Bombe, The
Dispositivo electromecánico usado por los criptólogos británicos para ayudar a descifrar las señales cifradas por la máquina alemana ENIGMA durante la Segunda Guerra Mundial, 21

C

CiberPunk
Subgénero de la Ciencia Ficción que muestra un futuro distópico gobernado por megacorporaciones a las que suelen enfrentarse hackers y expertos en tecnologías de la información., 56
Cifrado de sustitución
Mecanismo de cifrado en el que los símbolos o caracteres que se encriptan son sustituidos por otros., 21
Cillis
Claves de mensajes previsibles usados con el sistema ENIGMA alemán., 32
Clave simétrica
Sistema de encriptación basado en una clave común para el encriptado y desencriptado de la información o el mensaje. En el caso de que la clave deba ser compartida entre el emisor y el receptor del mensaje, presenta la dificultad adicional de compartirla de manera segura., 51
Computación Confidencial
El CCC define la computación confidencial como
la protección de los datos en uso mediante la realización de cálculos en un entorno de ejecución de confianza (TEE) basado en hardware., 16
Criptoanálisis
El criptoanálisis (del griego kryptós, 'escondido' y analýein, 'desatar') es la parte de la criptología que se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad sin el conocimiento de información secreta, 8
criptografia
Arte de escribir con clave secreta o de un modo enigmático. (Real Academia Española 2014). Es la parte de la criptología dedicada a la generación de códigos para el encriptado y protección de mensajes e información., ii

D

Departamento / Oficina Naval de Inteligencia
ONI (Office of Naval Intelligence) según su original el Inglés, es un servicio de inteligencia de la marina norteamericana., 37

E

Encriptación Homomórfica
un sistema de cifrado es homomórfico si es capaz de realizar una operación algebraica concreta sobre un texto original, equivalente a otra operación algebraica (no necesariamente la misma) sobre el resultado cifrado de ese texto original, 16

Entrelazamiento Cuántico
El entrelazamiento cuántico es un fenómeno de la mecánica cuántica en el que dos o más partículas se relacionan de tal manera que el estado cuántico de cada una no puede ser descrito de forma independiente del otro, incluso si las partículas están físicamente separadas. En otras palabras, el estado de una partícula está intrínsecamente vinculado al estado de la otra(s) partícula(s), sin importar la distancia que las separe., 16

Esquizofrenia
Grupo de enfermedades mentales correspondientes a la antigua demencia precoz, que se declaran hacia la pubertad y se caracterizan por una disociación específica de las funciones psíquicas, que conduce, en los casos graves, a una demencia incurable. (Real Academia Española 2014), 17

Esteganografía
Técnica que oculta mensajes, imágenes, información u objetos en el interior de otros que reciben el nombre de portadores., 36

F

Fibonacci, espiral de
Se trata de una aproximación a la espiral áurea generada dibujando arcos circulares conectando las esquinas opuestas de los cuadrados ajustados a los valores de la sucesión., 42

Fibonacci, sucesión de
Sucesión numérica en la que cada número puede obtenerse mediante la suma de los dos que le preceden., 42

Foreing Office
Equivalente Británico al Ministerio de Asuntos Exteriores español., 48

G

Gematria
Método de interpretación de nombres, palabras y frases hebreas basada en la asignación de valor numérico a cada carácter del alfabeto hebreo, 42

Guerra Fría
Enfrentamiento político, ideológico, económico y cultural entre los Estados Unidos y la Unión Soviética, que se desarrolló entre 1945 y 1989, 34

H

Hacker
La R.A.E. define hacker como pirata informático en su primera acepción. En la segunda lo define como
" Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora", 37

Heer, 32
Ejército de tierra aleman., 32

K

kriegsmarine
Nombre alemán de la marina de guerra, 45

L

Luftwaffe
Aviación militar alemana, el equivalente al ejército del aire en España, 32

M

Macguffin

Y

8. Bibliografía

Tora! Tora! Tora! Dirigido por Kinji Fukasaku y Toshio Masuda Richard Fleischer. Interpretado por Martin Balsam, Sô Yamamurak, E.G. Marshall y Tatsuya Mihashi. 1970.

Barro Ordovás, Antonio. «La clave Enigma.» Revista general de la marina, 2017: 233-247.

Bill, Valentine Tschebotarioff. Chekhov, The silent voice of freedom. Nueva York: Philosophical Library, 1987.

Blake, Sam. «The Solution of the Zodiac Killer's 340 Character Cipher.» Blog Wolfram. 24 de Marzo de 2021. https://blog.wolfram.com/2021/03/24/the-solution-of-the-zodiac-killers-340-character-cipher/ (último acceso: 29 de Mayo de 2023).

BOMFIM, Fabiana de Souza. «História da Matemática e Cinema: O caso da criptografia na introdução do ensino de Álgebra.» Tesis Doctoral, Universidade de São Paulo, 2017.

BUCHMANN, Johannes A., Denis BUTIN, Florian GÖPFERT, y Albrecht PETZOLDT. «Post-Quantum Cryptography: State of the Art.» En The New Codebreakers, editado por Peter Y.A. RYAN, David NACCACHE y Jean-Jacques QUISQUATER, 106-133. Springer-Verlag, 2016.

Windtalkers. Dirigido por John Woo. Interpretado por Nicolas Cage, Adam Beach, Christian Slater y Mark Ruffalo. 2002.

National Treasure (La Búsqueda). Dirigido por Jon Turteltaub. Interpretado por Nicolas Cage y Diane Kruger. 2004.

COHEN, Fred. 1990-1995. http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf (último acceso: 07 de Abril de 2023).

A Beautiful Mind - Una Mente Maravillosa. Dirigido por Ron Howard. Interpretado por Russell Crowe, Jennifer Connelly y Ed Harris. 2001.

Cuevas, A., y otros. «Long-distance distribution of genuine energy-time entanglement.» Nature Communications 4, nº 1 (2013): 2871.

The Imitation Game. Dirigido por Morten Tyldum. Interpretado por Benedict Cumberbatch, Keira Knightley, Charles Dance y Mark Strong. 2014.

Dictionary.com. «Gematria.» Dictionary.com. s.f. https://www.dictionary.com/browse/gematria (último acceso: 15 de Mayo de 2023).

DOMÍNGUEZ BOIZA, Carlos. «Criptografía y cine: criptografía en el cine bélico.» Trabajo Fin de Master, Universitat Oberta de Catalunya (UOC), 2023.

Easter, David. «Protecting secrets: British diplomatic cipher machines in the early Cold War, 1945–1970.» Intelligence and National Security, 2019: 157-169.

EPIC. «Carnivore.» Electronic Privacy Information Center. 19 de Junio de 2005. https://archive.epic.org/privacy/carnivore/ (último acceso: 31 de Mayo de 2023).

EuropaPress. «europapress/cienciaplus/laboratorio.» Científicos españoles logran comunicaciones cuánticas seguras por primera vez en el rango de las microondas. 19 de Junio de 2019. https://tinyurl.com/2mh7t6ls (último acceso: 03 de Abril de 2023).

FAJARDO RODRÍGUEZ, David. «Criptografía y cine. Análisis y uso didáctico de la representación de la criptografía en el cine.» Protocolos Criptográficos y Aplicaciones de Seguridad, Universitat Oberta de Catalunya (UOC), 2023.

Featherly, Kevin. «Carnivore.» Encyclopaedia Britannica. 28 de Septiembre de 2015. https://www.britannica.com/technology/Carnivore-software (último acceso: 31 de Mayo de 2023).

Contact. Dirigido por Robert Zemeckis. Interpretado por Jodie Foster, Matthew McConaughey, John Hurt y William Fichtner. 1997.

GARISTO, Dan. «spectrum.ieee.org.» What Is the Future of Quantum-Proof Encryption? 08 de Julio de 2022. https://tinyurl.com/2mpq7k7n (último acceso: 03 de Abril de 2023).

GILLIS, Alexander S. «TechTarget Security.» Definition quantum key distribution (QKD). Noviembre de 2022. https://tinyurl.com/2gsge969 (último acceso: 03 de Abril de 2023).

Goldberg, Leah. «Russian Literature in the Nineteenth Century: Essays.» 163. The Hebrew University Press, 1976.

Snowden. Dirigido por Oliver Stone. Interpretado por Joseph Gordon-Levitt y Melissa Leo. 2016.

GRUSKA, Jozef. «Faculty of Informatics, Masaryk University - IV054 Codes, Cryptography and Cryptographical Protocols - 2019.» CHAPTER 14: MACHINES and HISTORY of CRYPTOGRAPHY. 2019. https://tinyurl.com/2ce2cdch (último acceso: 07 de Abril de 2023).

Pi: Faith in Chaos - Pi, Fe en el Caos. Dirigido por Darren Aronofsky. Interpretado por Sean Gullete, Mark Margolis, Pamela Hart y Ben Shenkman. 1998.

Zodiac. Dirigido por David Fincher. Interpretado por Jake Gyllenhaal, Robert Downey Jr. y Mark Ruffalo. 2007.
The Da Vinci Code - El Código Da Vinci. Dirigido por Ron Howard. Interpretado por Tom Hanks, Audrey Tautou, Jean Reno, Ian McKellen y Paul Bettany. 2006.
The Da Vinci Code (El Código Da Vinci). Dirigido por Ron Howard. Interpretado por Tom Hanks y Audrey Tautou. 2006.
Hernández Encinas, Luis. «Taller de criptomatemáticas para jóvenes (y adultos).» Suma, 2000: 45-58.
Midway. Dirigido por Jack Smight. Interpretado por Charlton Heston, Henry Fonda, Toshirô Mifune y Hal Holbrook. 1976.
Hosch, William L. «Leonard M. Adleman.» Encyclopedia Britannica. 27 de Diciembre de 2022. https://www.britannica.com/biography/Leonard-M-Adleman (último acceso: 04 de Junio de 2023).
IBM. «IBM Explores the Future of Cryptography.» 15 de Marzo de 2021. https://tinyurl.com/2m27x77l (último acceso: 03 de Abril de 2023).
Swordfish - Operación Swordfish. Dirigido por Dominic Sena. Interpretado por Hugh Jackman, Halle Berry, John Travolta y Don Cheadle. 2001.
JULIÁN, Guillermo. «Xataka.» Así es el futuro de la criptografía: física cuántica. 25 de Marzo de 2015. https://tinyurl.com/2nuc78oq (último acceso: 03 de Abril de 2023).
Kahn, David. Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939-1943. Houghton Mifflin Harcourt, 1991.
KOTAS, William August. A Brief History of Cryptography. Supervised Undergraduate Student Research, Knoxville: Chancellor's Honors Program Projects - University of Tennessee, 2000.
Krapp, Peter. «Beyond schlock on screen: Teaching the history of cryptology through media representations of secret communications.» Proceedings of the 2nd international conference on historical cryptology. Linköping, Sweden: Linköping University Electronic Press, 2019. 79-87.
Lara, Vonne. «La soprendente historia del autor de crucigramas que puso en riesgo el desembarco de Normandía.» Hipertextual. 19 de Abril de 2018. https://hipertextual.com/2018/04/desembarco-normandia-crucigramas (último acceso: 08 de Mayo de 2023).
Lehning, Hervé. La Biblia de los Códigos Secretos. Planeta, 2022.
Macaskill, Ewen, y Grabriel Dance. «NSA FIles Decoded.» The Guardian, 1 de Noviembre de 2013.
Madridejos, Mateo. «Ni rojo, ni teléfono. La leyenda de la guerra fría.» El Periodico, 2 de Septiembre de 2023.
U-571. Dirigido por Jonathan Mostow. Interpretado por Matthew McConaughey, Bill Paxton y Harvey Keitel. 2000.
Les Vampires. Dirigido por Louis Feuillade. Interpretado por Musidora, Edouard Malthé y Marcel Lévesque. 1915.
N.S.A. National Security Agency / Central Security Service. s.f. https://www.nsa.gov/About/Mission-Combat-Support/ (último acceso: 04 de Junio de 2023).
Nash, John. «Non-Cooperative Games.» Editado por Mathematics Department. Princeton University. Annals of Mathematics 54, nº 2 (1951): 286-295.
National Museum of the United States Air Force. «National Museum of the United States Air Force.» War of Secrets: Cryptology in WWII. s.f. https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196193/war-of-secrets-cryptology-in-wwii/ (último acceso: 19 de Mayo de 2023).
Tinker, Tailor, Soldier, Spy. Dirigido por Tomas Alfredson. Interpretado por Gary Oldman, Colin Firth, Mark Strong, Benedict Cumberbatch y John Hurt. 2011.
O'Neill, Patrick Howell. «Criptografía reticular, el cifrado a prueba de ordenadores cuánticos.» MIT Technology Review. 07 de Agosto de 2020. https://www.technologyreview.es/s/12484/criptografia-reticular-el-cifrado-prueba-de-ordenadores-cuanticos (último acceso: 03 de Junio de 2023).
Ordenadores y Portátiles. «Carnivore.» Ordenadores y Portátiles. s.f. https://ordenadores-y-portatiles.com/carnivore/ (último acceso: 31 de Mayo de 2023).

PEDERSEN, Torben Pryds. «www.coindesk.com.» The Future of Cryptographic Security in the Age of Quantum. 06 de Enero de 2021. https://tinyurl.com/2l8fgney (último acceso: 03 de Abril de 2023).
Películas de Culto. «Sneakers (Los fisgones).» Películas de Culto. 08 de Diciembre de 2013. http://peliculasdeculto.blogspot.com/2013/12/sneakers-los-fisgones.html (último acceso: 04 de Junio de 2023).
Pérez-Desoy i Fages, Carles. «Conectando el 'teléfono rojo'.» cperezdesoy.files.wordpress.com. 26 de Diciembre de 2013. https://cperezdesoy.files.wordpress.com/2022/01/esglobal_-_conectando_el_telfono_rojo_-_2013-12-30.pdf (último acceso: 19 de Mayo de 2023).
PRIETO, Manuel J. «Historia de la criptografía. Cifras, códigos y secretos, de la antigua Grecia a la Guerra Fría.» De Manuel J. Prieto, 269-272. 2020.
Proton Mail. Proton Mail. s.f. https://account.proton.me/login (último acceso: 19 de Mayo de 2023).
Quirantes, Arturo. «Descifrando el último mensaje de Zodiac.» El Profe de Física. 29 de Marzo de 2021. https://elprofedefisica.naukas.com/2021/03/29/descifrado-el-ultimo-mensaje-de-zodiac/ (último acceso: 25 de Mayo de 2023).
Real Academia Española. Diccionario de la lengua española (23.a ed.). Real Academia Española, 2014.
Sneakers. Dirigido por Phil Alden Robinson. Interpretado por Robert Redford, Dan Aykroyd y Sidney Poitier. 1992.
Sneakers - Los Fisgones. Dirigido por Phil Alden Robinson. Interpretado por Robert Redford, Sidney Poitier, Mary McDonnell, Dan Aykroyd y David Strathairn. 1992.
Johnny Mnemonic. Dirigido por Robert Longo. Interpretado por Keanu Reeves y Dina Meyer. 1995.
SARNEK, Marcin. «"Cryptographer-Magician" and other modes of presence of cryptography in contemporary American cinema.» Artículo, University of Silesi, Katowice, 2014.
Schechter, Solomon, y Caspar Levias. «Gematria.» Jewish Encyclopedia. s.f. https://www.jewishencyclopedia.com/articles/6571-gematria (último acceso: 10 de Mayo de 2023).
SHANNON, C.E. «A mathematical theory of communication.» Editado por Nokia Bell Labs. The Bell System Technical Journal 27, nº 3 (Julio 1948): 379 - 423.
Shannon, C.E. «Communication theory of secrecy systems.» The Bell System Technical Journal 28, nº 4 (1949): 656-715.
SIMMONS, Gustavus J. «Encyclopedia Britannica - Britannica.» History of cryptology. 02 de Agosto de 2022. https://www.britannica.com/topic/cryptology/History-of-cryptology (último acceso: 07 de Abril de 2023).
SINGH, K. John, y R. MANIMEGALAI. «Evolution of Encryption Techniques and Data Security Mechanisms.» World Applied Sciences Journal 33, 2015: 1597-1613.
Singh, Simon. Los Códigos Secretos. Debate, 2000.
Аэлита - Aelita, Reina de Marte. Dirigido por Yakov Protazanov. Interpretado por Yuliya Sointeva, Igor Ilyinsky, Nikolai Tsereteli y Vera Orlova. 1924.
Enigma. Dirigido por Michael Apted. Interpretado por Tom Stoppard, Kate Winslet, Saffron Burrows y Jeremy Northam. 2001.
Subalemanes2. «El U-505, captura.» 19 de Marzo de 2013. https://subalemanes2.blogspot.com/2013/03/el-u-505-captura.html (último acceso: 28 de Mayo de 2023).
The Washington Post. «NSA slides explain the PRISM data-collection program.» The Washington Post, 10 de Julio de 2013.
Tributaria, Agencia. Agencia Tributaria. 11 de Mayo de 2022. https://tinyurl.com/2arzyrjc (último acceso: 10 de Abril de 2023).
Wikipedia. «Cábala.» Wikipedia, La enciclopedia libre. 5 de Mayo de 2023. https://es.wikipedia.org/w/index.php?title=C%C3%A1bala&oldid=150966498 (último acceso: 15 de Mayo de 2023).
—. «Carnivore.» Wikipedia, La enciclopedia libre. 23 de Octubre de 2022. https://es.wikipedia.org/w/index.php?title=Carnivore_(software)&oldid=146849407 (último acceso: 31 de Mayo de 2023).
—. «Criptografía.» Wikipedia, La enciclopedia libre. 21 de Febrero de 2023. https://tinyurl.com/2glqczu7 (último acceso: 14 de Marzo de 2023).

—. «Gematria.» Wikipedia, La enciclopedia Libre. 26 de Enero de 2023. https://es.wikipedia.org/w/index.php?title=Gematr%C3%ADa&oldid=148856836 (último acceso: 10 de Mayo de 2023).
—. «ISO 3166-1.» Wikipedia, La enciclopedia libre. 03 de Abril de 2023. https://es.wikipedia.org/w/index.php?title=ISO_3166-1&oldid=150308566 (último acceso: 10 de Abril de 2023).
—. «Macguffin.» Wikipedia, La enciclopedia libre. 9 de Abril de 2023. https://es.wikipedia.org/w/index.php?title=Macguffin&oldid=150434918 (último acceso: 19 de Mayo de 2023).
—. «Short Weather Cipher.» Wikipedia, La enciclopedia libre. 31 de Octubre de 2022. https://en.wikipedia.org/w/index.php?title=Short_Weather_Cipher&oldid=1119254919 (último acceso: 03 de Junio de 2023).
Mercury Rising - Al Rojo Vivo. Dirigido por Harold Becker. Interpretado por Bruce Willis, Kim Dickens y Alec Baldwin. 1998.
Zúñiga Azcue, Alfonso Manso de. «La máquina "Enigma".» U-historia. s.f. https://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm (último acceso: 10 de Junio de 2023).
Zurdo, David. «La gematría, numerología hebrea.» Manual formativo de ACTA, nº 48 (2008): 56-60.