

DE LA LIBRETA DE TURING A LA PANTALLA ¿COMO VE EL CINE LA CRIPTOGRAFÍA?

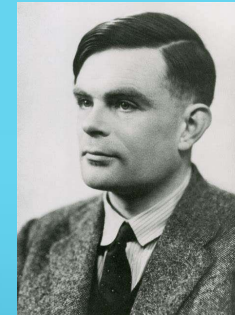


Fig.1

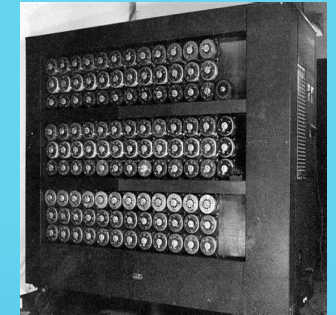


Fig.2



Fig.3

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD Y PRIVACIDAD.

PROTOCOLOS CRIPTOGRÁFICOS Y APLICACIONES DE SEGURIDAD.

AUTOR: ROBERTO MAGÁN PARRO

TUTOR/A DE TFM: RAFAEL PÁEZ REYES

PROFESOR/A RESPONSABLE DE LA ASIGNATURA: ANDREU PERE ISERN DEYÀ

“Arte de escribir con clave secreta o de un modo enigmático”

(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)

Índice

1. Justificación y Contexto

2. Objetivos

3. Enfoque y Método

4. Planificación

5. Análisis

5. Conclusiones y Trabajos futuros

6. Bibliografía y Créditos

Índice

1. Justificación y Contexto

1. Justificación y Contexto

Hace el presente ejercicio una revisión sobre como el cine se acerca a la criptografía y los códigos. Trataré en él de determinar cuan acertada o fallida resulta la representación y si esta última contribuye con mayor o menor protagonismo al desarrollo de la historia que se desarrolla en la pantalla



Índice

1. Justificación y Contexto

2. Objetivos

1. Objetivos

Analizar como algo ajeno y alejado del lenguaje cinematográfico, como lo es la criptografía, puede contribuir en el desarrollo de una historia. Siendo esta contribución significativa en algunos casos

Analizar y mostrar la influencia que una determinada tecnología o la resolución de un problema, pudo tener en el contexto y el momento en el que se desarrolla la acción mostrada en la película.

Como ejemplo de lo anterior, resulta indudable que la ruptura del código ENIGMA resultó crucial en el posterior desarrollo de la batalla de Atlántico y la Segunda Guerra Mundial en general. Sin embargo, no es especialmente significativo que la forma de las ilusiones paranoicas de John Nash fuesen códigos imaginados.

Contribuir a determinar cuan ajustadas y realistas son las representaciones que de la criptografía es capaz de hacer el cine. ¿Es cierto lo mencionado por 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." (Krapp 2019)

Índice

1. Justificación y Contexto

2. Objetivos

3. Enfoque y Método

3. Enfoque y Método. Inventario

En primer lugar, se elaboró el inventario de películas a analizar. El número finalmente incluido de filmes es 20.

Nº	Título	País	Año	IMDB/Filmaffinity
1	The Imitation Game	GB	2014	https://www.filmaffinity.com/es/film617730.html
2	Enigma	GB,US	2001	https://www.imdb.com/title/tt0157583/?ref=fn_al_tt_1
3	Una mente maravillosa	US	2001	https://www.filmaffinity.com/es/film326587.html
4	Contacto	US	1997	https://www.filmaffinity.com/es/film815526.html
5	Sneakers	US	1992	https://www.filmaffinity.com/es/film233071.html
6	National Treasure (La Búsqueda)	US	2004	https://www.filmaffinity.com/es/film721724.html
7	El Código Da Vinci	US	2006	https://www.filmaffinity.com/es/film306442.html
8	Pi	US	1998	https://www.filmaffinity.com/es/film679822.html
9	U-571	US	2000	https://www.imdb.com/title/tt0141926/
10	Les Vampires (Parte 3)	FR	1915	https://www.imdb.com/title/tt0006206/
11	El Topo	GB	2011	https://www.filmaffinity.com/es/film274340.html
12	Aelita	RU	1924	https://www.filmaffinity.com/es/search.php?stext=aelita
13	Operación Swordfish	US	2001	https://www.filmaffinity.com/es/film857439.html
14	Windtalkers	US	2002	https://www.filmaffinity.com/es/film957874.html
15	Jhonny Mnemonic	US	1995	https://www.filmaffinity.com/es/film222381.html
16	Mercury Rising	US	1998	https://www.filmaffinity.com/es/film830550.html
17	Snowden	US,CA	2016	https://www.filmaffinity.com/es/film892502.html
18	Tora! Tora! Tora!	US	1970	https://www.filmaffinity.com/es/film240724.html
19	Zodiac	US	2007	https://www.filmaffinity.com/es/film300908.html
20	La Batalla de Midway	US	1976	https://www.filmaffinity.com/es/film914270.html

3. Enfoque y Método. Análisis. Criterios

- *Sobre cada una de las películas he realizado una pequeña tarea de investigación y análisis, principalmente de los mecanismos criptográficos incluidos.*
- *He escogido un conjunto de criterios que permita valorar cada una de las películas de acuerdo a los objetivos mencionados en el apartado anterior. Estos criterios son:*

Papel

- Protagonista
- Secundario
- Reparto
- Extra

Clasificación

- Técnica
 - Manual
 - Mecánica
 - Electrónica
 - Futura
- Existencia
 - Si
 - No
- Corrección
 - Correcta
 - Incorrecta
 - Imp. Deter.

Importancia

- Alta
- Media
- Baja
- Sin Importancia

3. Enfoque y Método. Análisis. Cryptool2

- En alguna de las películas analizadas y con el objetivo de mostrar de una manera más dinámica el funcionamiento del mecanismo criptográfico analizado, he hecho uso de la herramienta Cryptool2.

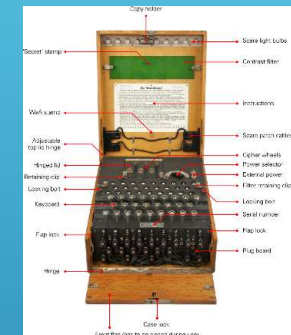
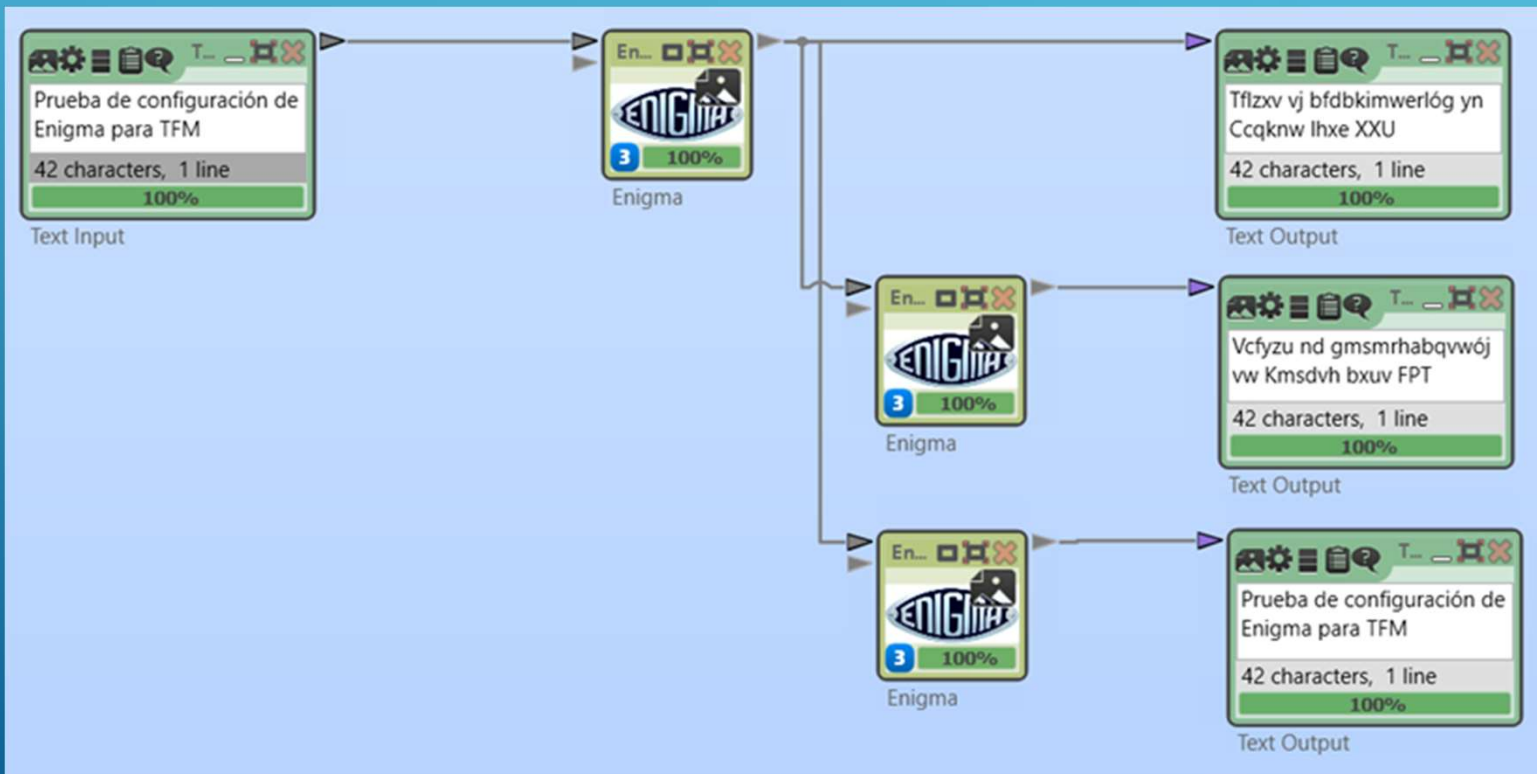


Fig.4

3. Enfoque y Método. Análisis. Documentación y Referencias.

Los datos recogidos en la memoria son el producto de la revisión y consulta de múltiples referencias y documentos. No es este el lugar para incluir un inventario exhaustivo de todas ellas, pero si quisiera incluir a continuación algunas que considero especialmente interesantes.

Estado del Arte

- Fajardo Rodriguez, David. Criptografía y cine. Análisis y uso didáctico de la representación de la criptografía en el cine
- Domínguez Boiza, Carlos. Criptografía y cine: criptografía en el cine bélico.
- Bomfim, Fabiana de Souza. História da Matemática e Cinema: O caso da criptografia na introdução do ensino de Álgebra
- Krapp, Peter. Beyond schlock on screen: Teaching the history of cryptology through media representations of secret communications.
- Sarnek, Marcin. "Cryptographer-Magician" and other modes of presence of cryptography in contemporary American cinema.

Buscadores

- **Cinematográficos**
 - <https://www.justwatch.com/es>
 - <https://www.filmaffinity.com/>
 - <https://www.imdb.com/>
- **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/>
- **Generalistas**
 - www.Google.com
 - www.Bing.com

Bibliografía

- Blake, Sam. «The Solution of the Zodiac Killer's 340 Character Cipher.»
- Kahn, David. Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939-1943.
- Lehning, Hervé. La Biblia de los Códigos Secretos.
- PRIETO, Manuel J. «Historia de la criptografía. Cifras, códigos y secretos, de la antigua Grecia a la Guerra Fría.»
- Singh, Simon. Los Códigos Secretos.

Índice

1. Justificación y Contexto

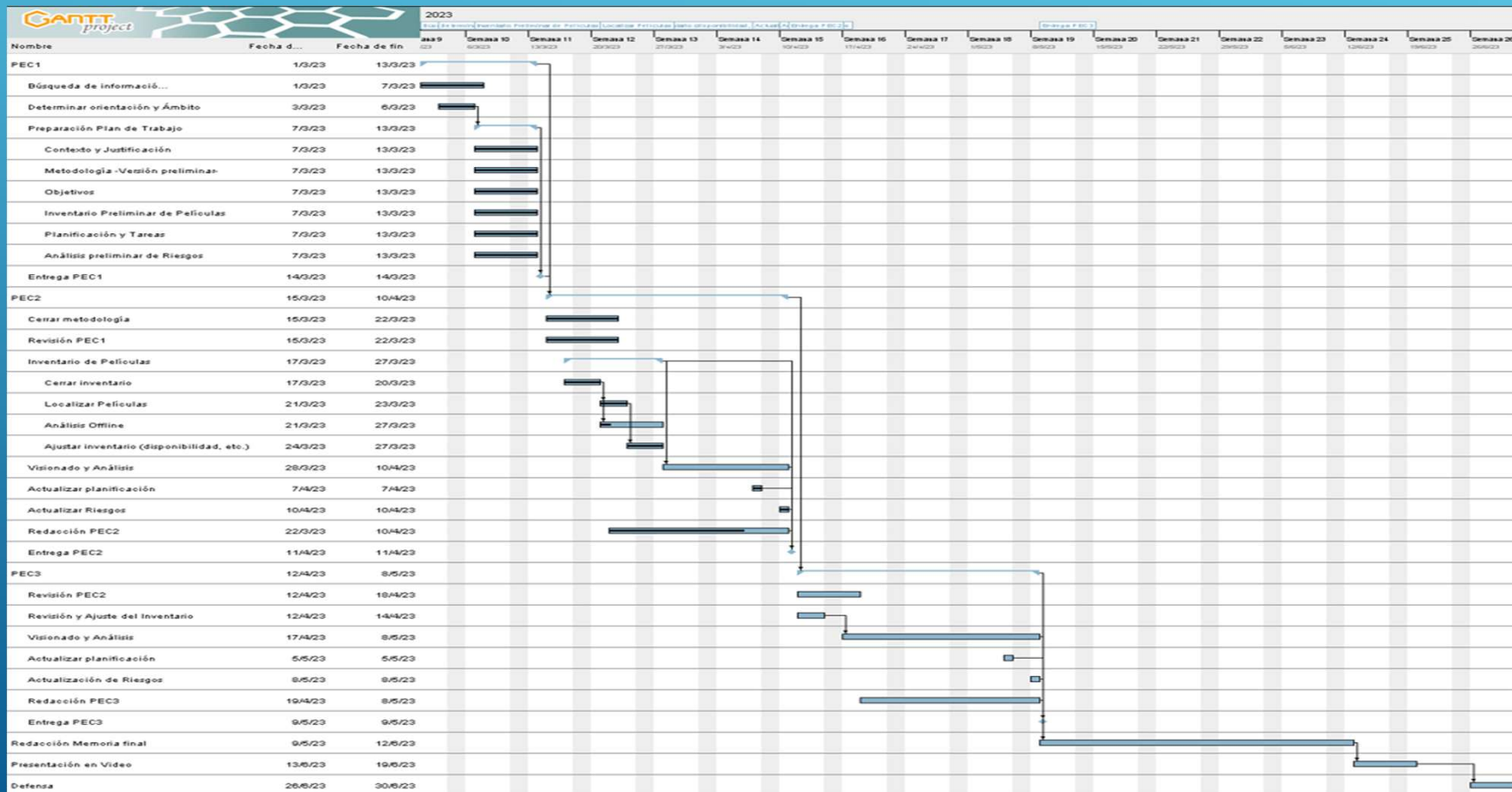
2. Objetivos

3. Enfoque y Método

4. Planificación

4. Planificación

Para realizar lo mencionado, se estableció la planificación que se muestra a continuación.



Índice

1. Justificación y Contexto

2. Objetivos

3. Enfoque y Método

4. Planificación

5. Análisis

5. Análisis.

- *El análisis detallado de cada una de las películas se encuentra recogido en la memoria y contiene, en líneas generales:*
 - *La enumeración y descripción de el o los mecanismos criptográficos que en ella aparecen. Destacaría en este caso los realizados sobre el funcionamiento de ENIGMA y PÚRPURA que aparecen de una u otra forma en al menos cinco de las películas analizadas:*
 - *Descifrando Enigma*
 - *Enigma*
 - *U-571*
 - *La Batalla de Midway*
 - *Tora! Tora! Tora!*
 - *De la misma forma se realiza una descripción de los procesos de criptoanálisis en aquellos casos que son de interés. Remarcar en este caso los llevados a cabo en dos de los filmes analizados*
 - *Descifrando Enigma*
 - *Zodiac*
- *Revisión de los criterios definidos en el apartado correspondiente a Análisis y Métodos. El resultado de dicha revisión se ha consolidado en una tabla de resultados que se encuentra recogida en la memoria y se muestra algo más adelante en esta misma presentación.*

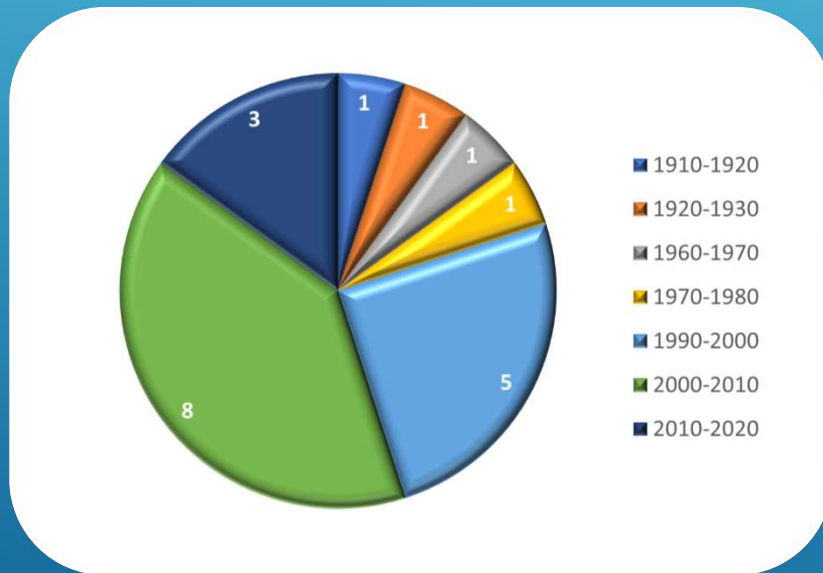
5. Análisis. Resultados. Resumen

Los resultados obtenidos tras el análisis de las diferentes películas se muestran en cada una de ellas y se han consolidado en la tabla que se muestra en la memoria y reproduzco a continuación.

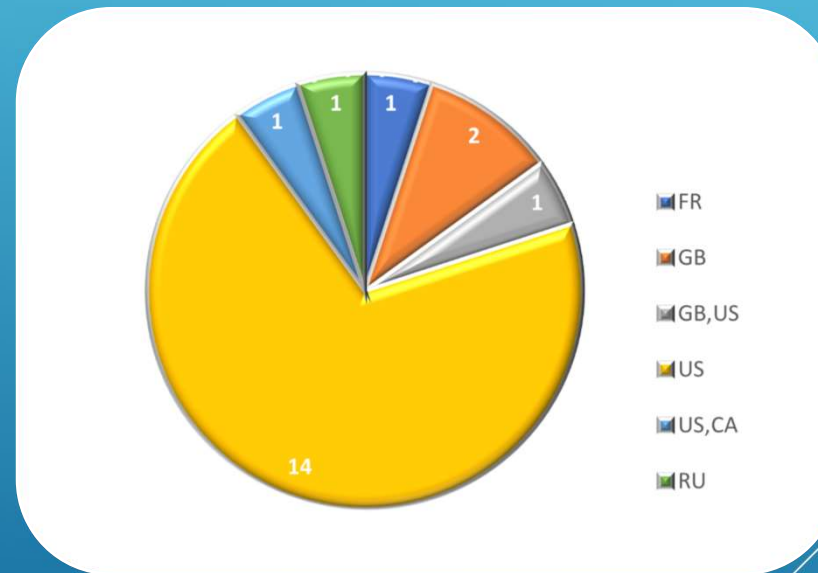
Nº	Título	Papel	Técnica			Importancia
			Periodo	Existencia	Correccion	
1	The Imitation Game (Descifrando Enigma)	Protagonista	Mecánica	Real	Correcta	Alta
2	Enigma	Secundario	Mecánica	Real	Correcta	Alta
3	A Beautiful Mind (Una Mente Maravillosa)	Reparto	S/D	Inventada	Incorrecta	Alta
4	Contact (Contacto)	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	Correcta	S/I
8	Pi	Protagonista	Manual	Inventada	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	Correcta	S/I
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

5. Análisis. Resultados. Nacionalidad y Año.

En cuanto a la nacionalidad y el año de realización de las películas analizadas, el detalle a continuación. Las conclusiones, las detallo en el apartado correspondiente, aunque ya podemos intuir aquí algunos desequilibrios en las distribuciones.



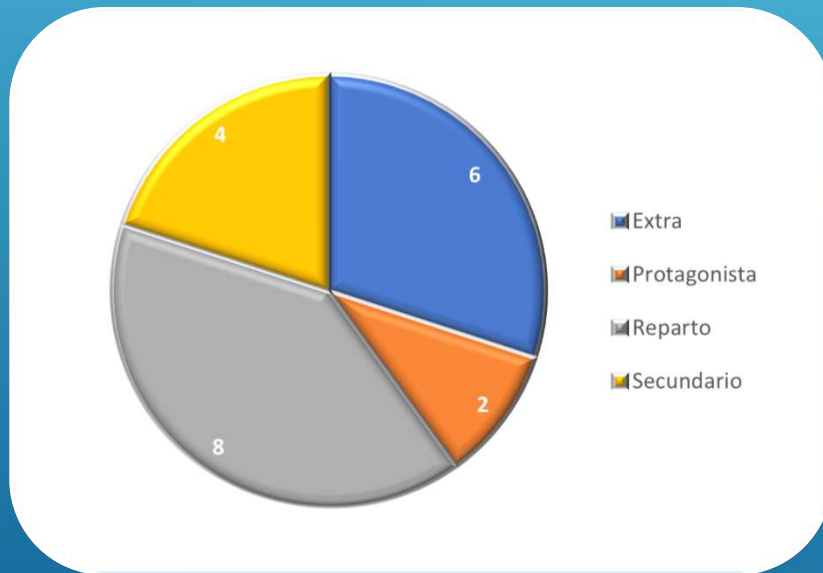
Año de Producción



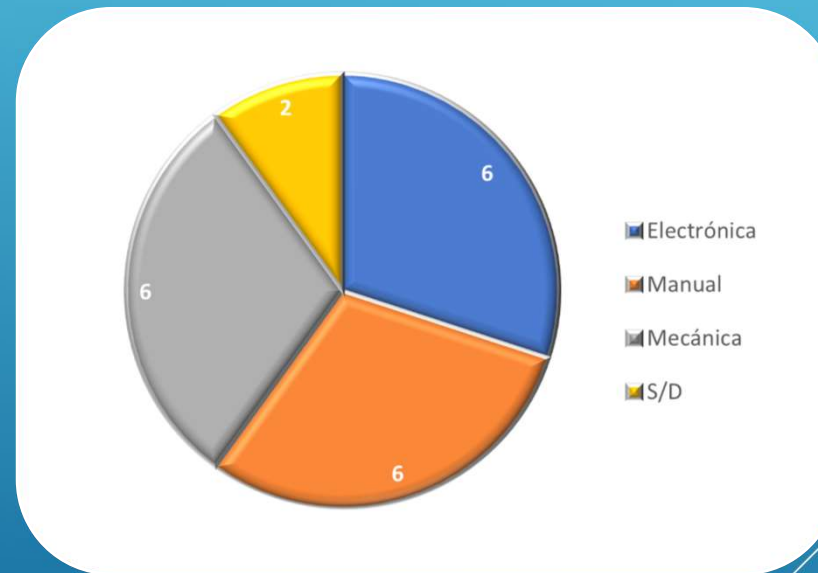
Nacionalidad

5. Análisis. Resultados. Papel y Periodo.

Seguimos con los datos correspondientes al Papel desempeñado por la criptografía en la película y el tipo de técnica empleada



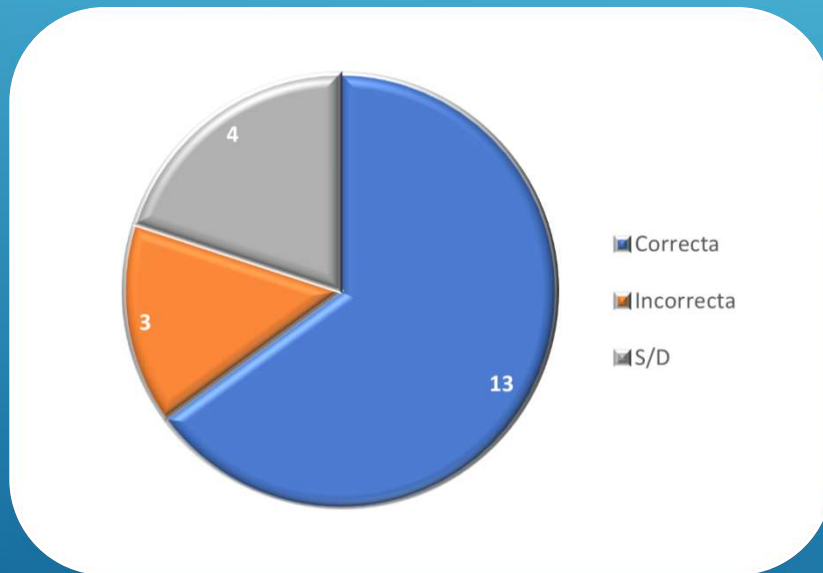
Papel



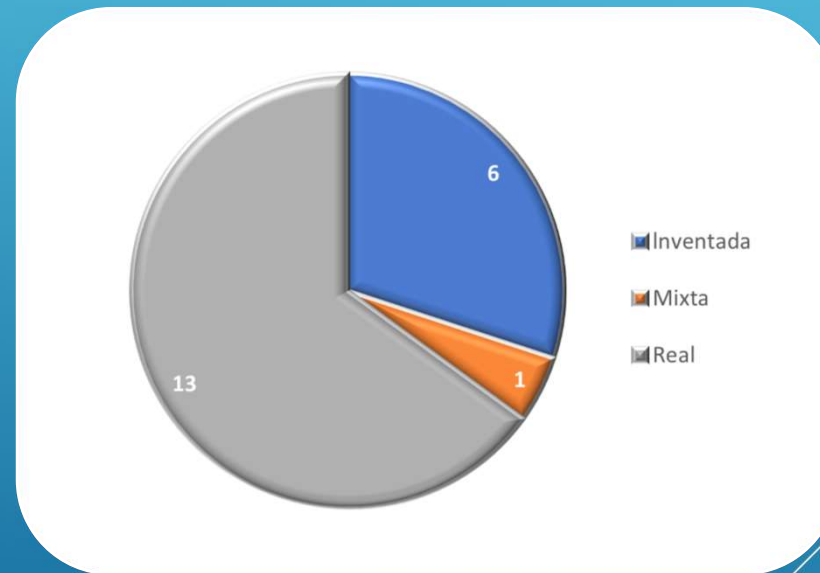
Periodo

5. Análisis. Resultados. Corrección y Existencia.

De los criterios pendientes, a continuación, los datos correspondientes a cuan correcta es la representación y si los mecanismos tienen existencia real o no.



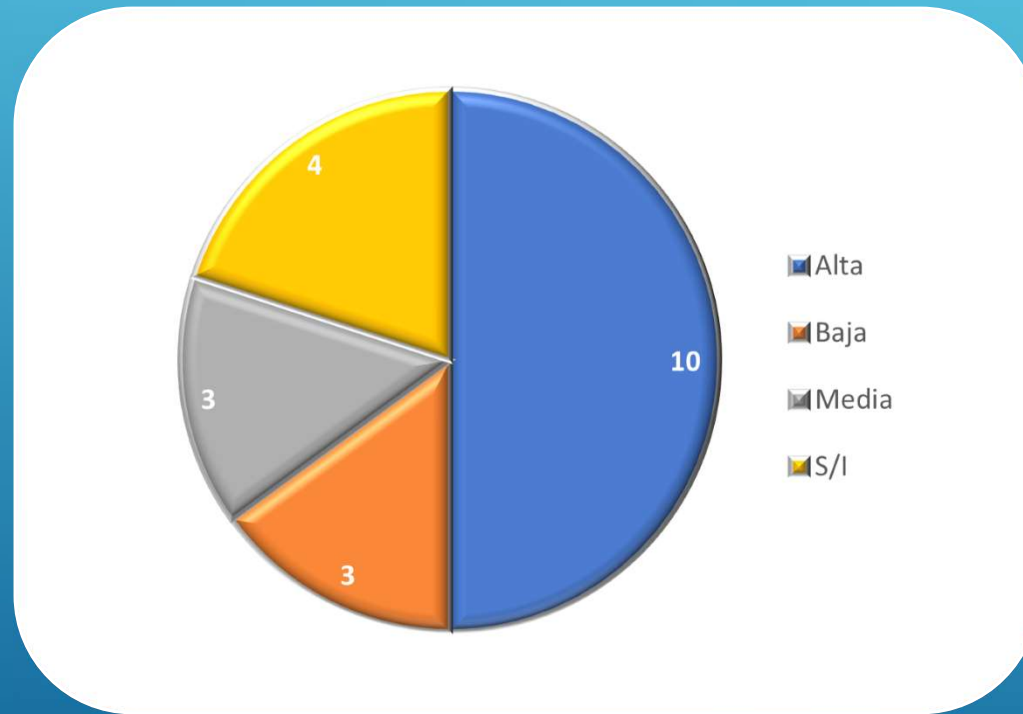
Corrección



Existencia

5. Análisis. Resultados. Importancia.

Para finalizar, el resumen de cuan importantes son los mecanismos criptográficos mostrados



Importancia

Índice

1. Justificación y Contexto

2. Objetivos

3. Enfoque y Método

4. Planificación

5. Análisis

5. Conclusiones y Trabajos futuros

5. Conclusiones y Trabajos Futuros. Conclusiones (I)

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

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

En cuanto al papel, aunque sólo en dos ocasiones he atribuido la condición de protagonista a los códigos y encriptaciones y el de secundario en cuatro, en más del 65% de los filmes analizados lo analizado tiene influencia en el desarrollo de la historia.

Si del periodo hablamos, sólo en un 10% de las ocasiones no he sido capaz de atribuir el mecanismo. En el resto de los casos, los porcentajes son iguales, un 30% para cada uno de ellos.

5. Conclusiones y Trabajos Futuros. Conclusiones (II)

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

En general la tendencia es hacia 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

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.

5. Conclusiones y Trabajos Futuros. Conclusiones (III)

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

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.

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

Destacar en este último punto que disponer de un buen servicio de inteligencia; facilitará, junto a los errores mencionados en el punto anterior, o provocándolos como se puede en alguna de las películas analizadas, la tarea ya de por si compleja de los criptoanalistas y sin ella, tal vez esta tarea acabe resultando infructuosa.

5. Conclusiones y Trabajos Futuros. Trabajos Futuros

Han quedado pendientes multitud de películas en las que, de una forma u otra, la criptografía y los códigos tienen presencia. Se trata esta de una oportunidad para incluir nacionalidades y años no revisados en esta ocasión.

Sólo algunos de los mecanismos de encriptación empleados podrían considerarse entre los que podemos llamar modernos (electrónica, claves asimétricas, etc.) Tratar de localizar y revisar estos mecanismos es, también, una posible ampliación del presente

Sin salir del ámbito audiovisual, han quedado por revisar opciones como serían las series, películas de animación y documentales.

Fuera del ámbito audiovisual y sin mencionar la literatura que, sin duda, tiene muchas y muy variadas representaciones de esta disciplina, la posibilidad de explorar su presencia en otros ámbitos artísticos resulta muy atractiva (música, pintura, etc.)

Índice

1. Justificación y Contexto

2. Objetivos

3. Enfoque y Método

4. Planificación

5. Análisis

5. Conclusiones y Trabajos futuros

6. Bibliografía y Créditos

3. Bibliografía y Créditos

- 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.
- DOMÍNGUEZ BOIZA, Carlos. «Criptografía y cine: criptografía en el cine bélico.» Trabajo Fin de Master, Universitat Oberta de Catalunya (UOC), 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.
- Kahn, David. *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939-1943.* Houghton Mifflin Harcourt, 1991.
- 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.
- Lehning, Hervé. *La Biblia de los Códigos Secretos.* Planeta, 2022.
- 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.
- Real Academia Española. *Diccionario de la lengua española (23.a ed.).* Real Academia Española, 2014.
- SARNEK, Marcin. «"Cryptographer-Magician" and other modes of presence of cryptography in contemporary American cinema.» Artículo, University of Silesi, Katowice, 2014.
- Singh, Simon. *Los Códigos Secretos.* Debate, 2000.
- Wikipedia. «Criptografía.» Wikipedia, La enciclopedia libre.
- Fig.1 Granger/REX/Shutterstock
- Fig.2 Set of wartime photos of GC&CS at Bletchley Park. Dominio Público
- Fig.3 Cartel de promoción de la película *The Imitation Game (Descifrando Enigma)*
- Fig.4 <https://www.cryptomuseum.com/crypto/enigma/i/>
- Fig.5 (The End) <https://pixabay.com/illustrations/the-end-guy-cinema-strip-movie-139848/>

A graphic of a film strip with a dark, textured background. The words "The End" are written in a white, elegant cursive font, centered on the strip. The film strip has perforations on the left and right sides and a white border at the top and bottom.

The End