Criptografía y cine

Criptografía en el cine bélico

Carlos Domínguez Boiza.

Protocolos criptográficos y aplicaciones de Seguridad.

Nombre Tutor de TF

Rafael Páez Reyes

Profesor/a responsable de la asignatura

Andreu Pere Isern Deyá & Cristina Pérez Solá

Fecha Entrega: Enero 2023

Universitat Oberta de Catalunya

Universitat Oberta de Catalunya uoc.edu

FICHA DEL TRABAJO FINAL

Título del trabajo:	Criptografía en el cine bélico
Nombre del autor:	Carlos Dominguez Boiza
Nombre del consultor/a:	Rafael Páez Reyes
Nombre del PRA:	Cristina Pérez Solá
Fecha de entrega (mm/aaaa):	01/2023
Titulación o programa:	Máster en Ciberseguridad y Privacidad
Área del Trabajo Final:	Protocolos Criptográficos y aplicaciones de Seguridad
Idioma del trabajo:	Castellano
Palabras clave	Cine bélico, criptología, cine, criptografía

Resumen del Trabajo

Desde tiempos inmemoriales el ser humano, al entrar en contienda con otros pueblos, ha tratado de ocultar la información que se transmitía con sus aliados, o entre ellos mismos, frente a las posibles interceptaciones de estos mensajes por parte de sus enemigos. Desde la Scítala espartana en la Antigua Grecia, hasta la máquina Enigma durante la 2ª Guerra mundial, no hay duda en afirmar que todo sistema criptológico ha ocupado un lugar fundamental en el devenir de estas contiendas, incluso ha marcado su destino, y por ende, el de la humanidad, como puede ser el caso del desciframiento de la máquina Enigma en la 2ª Guerra Mundial por parte de científicos polacos e ingleses, lo que provocó la derrota de los alemanes en la guerra.

Por supuesto el cine, al igual que la literatura, se ha hecho eco de la importancia del uso de la criptología durante estos enfrentamientos bélicos, lo que ha llevado a una proliferación de obras que tienen como protagonista de fondo el uso de estos sistemas de ocultación y/o de transformación de la información.

En el presente trabajo, por lo tanto, discutiremos varias de estas obras cinematográficas, explicando el contexto de cada una de ellas, así como el procedimiento de cifrado usado en cada situación.

Abstract

Since inmemorial times, human beings, when entering into a conflict with another human beings, have tried to hide the information that was being transmitted to their allies or among themselves, in order to prevent the enemy know their positions and so, win the war. From the Spartan Scythala, used in Ancient Greece, to the Enigma Machine in the WWII, there is no doubt to claim that every cryptological system has occupied a fundamental place in the course of these conflicts, marking its destiny and so the destiny of the mankind as we can see when Polish and English scientist and mathematicians achieved to break the Enigma machine german army used, causing the allies to win the war.

Cinema, like literature, has echoed the importance or the use of cryptology during these confrontations, which has led to a proliferation of works that has one of their main characters in cryptology, with methods of transformation and hiding of the information.

In the present work, several movies will be discussed, explaining the context of each of them, as well as the encryption procedure used in each situation

Índice

Lista de figuras

Lista de Tablas

1.Introducción

Este primer capítulo tiene como objetivo el realizar una introducción al tema propuesto. Ayuda a poder situarse dentro del contexto del trabajo, explica su porqué y los objetivos que se persiguen, esto es, el alcance del proyecto y la metodología usada para ello.

1.1 Contexto y justificación del Trabajo

Como se puede ver en diversas fuentes [1], se puede decir que la criptología, que comprende tanto las técnicas de encriptado o codificado de la información como las desarrolladas para romper los códigos o criptoanálisis, es hoy en día un campo de investigación propio de las matemáticas. Sin embargo, en el pasado fue considerado un arte donde se hacía alarde de todo el ingenio e imaginación posibles para ocultar y transformar la información considerada vital y poder comunicar determinados secretos que, aunque fuesen interceptados, mantuvieran su integridad en todo momento.

Es sabido que los cambios y los avances científicos y tecnológicos han estado siempre asociados a alguna contienda, es en estos casos de enfrentamiento cuando la información juega un papel fundamental para la supervivencia de cada bando enfrentado. Sin ir más lejos, durante la 2ª Guerra Mundial se produce el verdadero auge de la criptografía, al producirse un salto sustancial tanto en la cantidad como en la calidad exigida a la cifra de las comunicaciones entre los diversos contendientes, lo que obligó al empleo y adaptación de máquinas como Purple, utilizada por Japón y la Enigma utilizada por Alemania.

Como se podría esperar, el cine, sobre todo en su género bélico, ha reflejado el uso de estos sistemas criptográficos en diversas contiendas, poniendo de manifiesto la vital importancia que han jugado en el resultado de éstas y por lo tanto en el destino de los distintos países en lucha.

1.2. Objetivos del Trabajo

El objetivo de este trabajo de máster es el de realizar una revisión del uso de determinados sistemas criptográficos dentro de varias obras cinematográficas de género bélico, examinando y describiendo el procedimiento de cifrado que se describe en cada una de ellas con el objetivo de determinar si se ajustan o a no a la realidad, es decir, a un sistema que podría haberse usado en la vida real, dando respuesta así a la pregunta de si en el cine se refleja fielmente el uso de estos procedimientos criptográficos.

1.3.Enfoque y método seguido

El enfoque que se va a seguir en este trabajo, para llevar a cabo los objetivos descritos en el apartado 1.2, será el de visionar estas películas para poder analizar y detallar los procedimientos criptográficos seguidos en cada de una de ellas y poder conseguir el objetivo descrito, para ello, la presente memoria se acompañará de videos *linkados* y se hará uso de herramientas como "Cyrptool Portal" (https://www.cryptool.org/en/) para una mayor comprensión de estos procedimientos, estos archivos creados con el programa Crytptool serán añadidos en la entrega final del presente trabajo.

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

Como es sabido, existen tres dimensiones que se alinean con los Objetivos de Desarrollo Sostenible (ODS) descritos por la ONU y con los que la UOC se encuentra totalmente comprometida, a saber:

- Sostenibilidad.
- Comportamiento ético y de responsabilidad social.
- Diversidad de género y derechos humanos.

Al ser un trabajo técnico se puede afirmar que tanto ni en el resultado ni durante su desarrollo este trabajo tiene ningún impacto ni negativo ni positivo en aspectos de sostenibilidad medioambiental y/o huella ecológica.

Sí que tiene cierta cabida dentro de una dimensión ética y de responsabilidad social al hacerse eco de la importancia de la salvaguarda de la información que se comparte, de preservar la privacidad y remarcando la importancia de ésta hoy en día y lo importante que es su custodia.

También presenta ciertos aspectos a resaltar dentro de la dimensión de la diversidad, género y derechos humanos, ya que al analizar el uso de sistemas criptológicos en varias obras cinematográficas se obvia, como no podría ser de otra manera, el género y procedencia de sus directores y sus actores, focalizándose tan sólo en los procedimientos criptológicos usados.

1.5.Planificación del Trabajo

En este apartado se tratará de describir los recursos necesarios para implementar el actual trabajo, así como una planificación temporal de cada tarea representada en un diagrama de Gantt. Así, podrán ser destacados los hitos parciales que representan cada una de las PECs de esta asignatura, por lo tanto cada hito está representado por las cuatro Pruebas de Evaluación Continua a entregar, tal y como puede verse a continuación. Se hace notar que también se considerará como hito la propia defensa del trabajo.

1.5.1 Planificación PEC1. Plan de trabajo.

En este primer hito, de 10 días de duración, se realizará un Análisis y concreción del TFM, conjuntamente con una búsqueda de información sobre el material con la compra de recursos teóricos y la elaboración de una lista de películas sobre las que se va a trabajar. Se realizará el primer capítulo de la memoria consistente en explicar el contexto, la justificación y el enfoque que se va a seguir para la realización del trabajo y la planificación temporal que se representa por el actual apartado.

Nombre	Fecha de inicio	Fecha de fin
Planificación PEC1	28/9/22	11/10/22
Análisis y concreción del TFM	28/9/22	29/9/22
Búsqueda y lectura de información	30/9/22	3/10/22
Compra de recursos a utilizar en el trabajo.	4/10/22	5/10/22
Elaboración de lista de películas	6/10/22	6/10/22
Elaboración Estado del Arte	6/10/22	6/10/22
Elaboración Documento PEC1	6/10/22	7/10/22
Entrega PEC1	10/10/22	10/10/22
Revisión y modificaciones PEC1	11/10/22	11/10/22

Figura 1.Planificación PEC1

1.5.2 Planificación PEC2. Entrega de seguimiento.

En esta segunda fase del proyecto, de 20 días de duración, se centrará en el visionado e investigación sobre los diversos procedimientos criptográficos seguidos en cada una de las películas, por lo que la PEC2 tiene una mayor duración que la anterior PEC1 . Se

partirá de la lista elaborada en la anterior PEC1 pero se seguirá revisando, incrementando o reduciendo esta lista según proceda.

Figura 2. Planificación PEC2

1.5.3 Planificación de PEC3. Entrega de seguimiento

Esta PEC se trata de una PEC muy similar a la anterior en tanto que se seguirá visionando y revisando todas los procedimientos criptográficos reseñados en todas las películas de género bélico escogidas previamente, por lo que constará de la tarea de "Visionado de películas y revisión de sistemas criptográficos" y al mismo tiempo se puede realizar la tarea de "Elaboración, comprobación y entrega de PEC3", seguida de una tarea de "Revisión y modificación de PEC3" en caso de que así fuese necesario.

Figura 3. Planificación PEC3

1.5.4 Planificación de PEC4. Memoria final

En esta fase es cuando se unificaran las anteriores PECs y se dará forma a la memoria final del trabajo fin de máster, es por lo tanto la fase que más se prolongará en el tiempo, en concreto desde el 7 de diciembre al 10 de enero aproximadamente en la que se presentarán las tareas de "Redacción final de la memoria" con una duración de 7 días. Después de esta redacción final de la memoria se ha planificado una tarea de "Entrega de PEC4. Mejora continua" por la que se revisarán todos los datos escritos previamente, corrigiendo y añadiendo cualquier información que se considere importante y que no

pueda faltar de la memoria final. Seguidamente se presenta una tarea de “Presentación en vídeo” de 6 días de duración, como se puede ver en la siguiente figura.

Figura 4. Planificación PEC4

1.6. Análisis de riesgos del trabajo

A continuación se presenta una matriz de riesgos del proyecto con su posible mitigación:

Nombre	Causa	Descripción	Consecuencia	Probabilidad	Impacto	Nivel	Mitigación
Disponibilidad de películas	Dificultad de encontrar películas en internet	Algunas películas, por su antigüedad o porque ya se encuentren descatalogadas son difíciles de encontrar por internet	Imposibilidad de revisar el sistema criptológico usado en ellas	Media	Alto	Alto	Buscar en bibliotecas, comprar la película en tienda o buscar otras películas similares.
Visionar demasiadas películas	Ser demasiados ambiciosos en el número de películas a visionar	Documentar el TFM con un número excesivo de películas .	Se retrasa en exceso la documentación del TFM y por consiguiente, le entrega del proyecto	Bajo	Media	Medio	Ceñirse al número de películas preestablecido y no sobrepasarse.
Explicación excesivamente minuciosa de los sistemas criptológicos usados.	Ser demasiado detallista en cuanto a los sistemas criptológicos usados en cada película.	Extenderse de forma indebida en la descripción de los sistemas criptológicos usados en cada una de las obras.	Esta extensión provocaría un retraso en la entrega del proyecto	Bajo	Media	Medio	Ceñirnos a una explicación que aunque detallada, no sea excesivamente minuciosa, lo que provocaría un retraso en la entrega del proyecto.
Gran número de películas vistas y no tomar notas de las mismas.	Con el afán de ver cuanto más películas mejor, no tomar notas exactas de las mismas.	No tomar notas exactas de los sistemas criptológicos vistos con lo que a la hora de hacer la presentación ésta se retrasa.	Retraso en la entrega del proyecto, ya que se tendría que ver de nuevo la película.	Media	Alto	Alto	Ir documentando de forma concienzuda todas las películas vistas para que esto no pase.

Avería de ordenador	Descuido en el cuidado del ordenador.	Se puede averiar el ordenador por cualquier motivo, caídas, vertido de líquido etc.	Pérdida del trabajo. Imposibilidad de entrega de proyecto	Baja	Muy alto	Muy alto	Realizar copias periódicas en la nube o trabajar directamente en la nube, tener siempre a mano un portátil de repuesto.
Enfermedad o accidente	Enfermedad o accidente sufrido por el estudiante	En ocasiones es inevitable padecer o sufrir una enfermedad o accidente que incapacite de forma temporal al estudiante	Retraso en la entrega del proyecto incluso podría suponer la no entrega del mismo dependiendo del accidente o enfermedad sufrida.	Baja	Muy alto	Muy alto	La mitigación para este contratiempo es difícil de encontrar, ya que la enfermedad pudiera ser totalmente incapacitante, lo mejor es tratar de adelantar todo el trabajo posible, antes de que se presentara esta situación.
Carga de trabajo.	Excesiva carga de trabajo del estudiante entre el proyecto y las cargas laborales externas.	El estudiante, aparte de la entrega de este proyecto, debe hacerse cargo de cargas laborales externas ajenas al proyecto o internas a la Universidad debido a otras asignaturas.	Retraso en las entregas del trabajo, lentitud en la consecución de objetivos.	Media	Alto	Alto	La mejor forma de hacer frente a este problema es utilizar los fines de semana y días libre para poder adelantar trabajoi, así como trabajar todos los días en el trabajo, aunque sea un poco.
Cargas personales	El estudiante de hacerse cargo también de obligaciones de tipo	Las obligaciones de tipo personal o familiar también influirán en los plazos de entrega	Retraso en las entregas del trabajo, lentitud den la consecución de objetivos	Media	Alto	Alto	La mejor forma de mitigar la influencia de las cargas personales es utilizar días

	personal y tipo familiar	de cada una de las partes del trabajo.					libres en cualquier momento para poder ir avanzando trabajo y poder hacer frente a estas cargas de tipo personal.

Tabla 1. Análisis de riesgos del trabajo.

1.7 Estado del Arte

Existen varios obras que han tratado de profundizar en este tema de la Criptografía en el cine como se puede ver en Marcin (2014) [4] en la que se han tratado varias obras cinematográficas como Swordfish, Mercury Rising y Pi, aunque siempre desde una visión a muy alto nivel y sin detallar los procedimientos criptológicos empleados. Es por ello que en este trabajo se pretende explicar un poco más en detalle los aspectos criptográficos un poco más técnicos que tienen lugar.

Otra aproximación al mundo de la criptografía, desde el cine, aunque más centrado en las matemáticas más generales puede verse en Ramesh et al (2019) [5], donde se realiza una aproximación de grandes matemáticos al mundo del cine, examinando cuatro películas en particular: The Imitation Game (2014), Agora (2009), A Beautiful Mind (2001) y The Man who Knew Infinity (2015). La primera de ellas cabe plenamente en el mundo de la criptografía y será discutida en este trabajo.

1.8. Lista de películas a examinar

Tal y como se ha reseñado en capítulos anteriores, se presenta en esta PEC1 una primera versión de lista de películas de cine bélico a examinar. Esta lista se podrá ir modificando a lo largo del trabajo aumentando su tamaño.

1. The Imitation Game (Descifrando a Enigma) (2014)
2. Rendezvous (1935)
3. Windtalkers (2002)
4. La clave está en Rebeca (1985)
5. Midway (1976)
6. La espada de Sharpe (1995)
7. El Topo (2011)
8. All the Queen's Men (2001)
9. Desde Rusia con amor (1963)
10. El puente de los espías (2015)

2. Análisis de lista de películas

En este apartado se documentará los sistemas criptográficos usados en cada una de las películas listadas en el apartado 1.8

2.1 The Imitation Game (2014)

En esta película del 2014, dirigida por Morten Tyldum, se narra el proceso de ruptura de la máquina Enigma utilizada por los alemanes durante la Segunda Guerra Mundial. Esta ruptura se llevará a cabo por parte de un grupo de criptógrafos ingleses, encabezados por el matemático inglés Alan Turing, considerado uno de los padres de la ciencia de la computación.

Es conocido que hasta el final de la 1ª Guerra Mundial, prácticamente todas las comunicaciones entre el personal militar era efectuada o bien a mano o bien por telegrama, por lo que estas comunicaciones se caracterizaban por ser excesivamente lentas. Es a partir de la 2ª Guerra Mundial cuando la radio se convierte en el principal medio de comunicación, convirtiendo a estas comunicaciones en prácticamente instantáneas aunque con la contrapartida importante de que las hacían mucho más fáciles de interceptar [7], con lo que el desarrollo de nuevos códigos de cifrado más robustos era toda una necesidad.

Se puede decir que la máquina Enigma se basa en un cifrado de sustitución, estos métodos de sustitución son aquellos en los que cada letra del texto en claro es sustituida por una o más letras del alfabeto encriptado según un método previamente preestablecido. Existen dos sistemas principales de cifrado por sustitución, monoalfabético y polialfabético. El cifrado por sustitución monoalfabético es aquel en el que existe una asociación biunívoca entre una letra en el texto en claro y una letra en el texto cifrado, por ejemplo en la siguiente figura se puede observar esta asociación entre letra en texto claro y su correspondiente letra cifrada, en la que cada letra del alfabeto en claro es sustituida por la letra tres veces más a la derecha en el alfabeto, lo que es conocido como Cifrado César:

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

Tabla 2. Cifrado Cesar por sustitución monoalfabético

La seguridad de este sistema de cifrado estriba en que, sin esta tabla, el desencriptado se hace relativamente complicado de romper. No obstante, en general todo cifrado monoalfabético, será fácil de quebrar algo en lo que influirá la longitud del texto cifrado. Esta facilidad para romper un cifrado monoalfabético se basa en que este tipo de cifrados adolecen del problema del análisis de las frecuencias, esto se basa en el conocimiento de que, en un idioma determinado, existe una determinada frecuencia en la aparición de letras, por ejemplo, en castellano la letra 'E' es la más frecuente con un 13,68% de aparición, por lo que si una letra en texto claro siempre se corresponde con la misma letra en el código encriptado se tendría un fallo importante que podría provocar la ruptura del código; es conocido que la primera explicación del uso del análisis de frecuencias de las letras como método de criptoanálisis se debe al filósofo árabe AL-Kindi, quien la publicó en su obra *Un manuscrito para el descifrado de mensajes criptográficos* [6].

Para solucionar este problema, surgió el cifrado de sustitución polialfabético, desarrollado por León Battista Alberti en 1466 quien ofreció la posibilidad de utilizar varios alfabetos cifrados para codificar una letra, llevar a cabo una sustitución según una regla y luego, después de un determinado número de sustituciones, cambiar de regla. Para ello desarrolló lo que se ha venido en llamar como "Disco cifrador de Alberti", formado por dos anillos concéntricos, que giran de manera independiente, de tal forma que una vez fijadas sus posiciones relativas, la letras del círculo exterior se sustituirán por las correspondientes letras del círculo interior. El anillo externo fijo representa el texto a cifrar o alfabeto en claro y el anillo interno es un anillo móvil que representará el texto cifrado, tal y como se puede ver en la siguiente figura:

Figura 5. Disco cifrador de Alberti

Una forma sencilla de entender el cifrado polialfabético de Alberti consiste en utilizar dos alfabetos de sustitución, con la regla de que a la hora de llevar a cabo las sustituciones del mensaje original se alterne el uso de ambos alfabetos, a continuación se muestra el alfabeto en claro y dos posibles alfabetos de sustitución:

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

Tabla 3. Cifrado polialfabético

En este ejemplo y en posteriores, se representará el texto claro en letras minúsculas mientras que el texto cifrado se representará en letras mayúsculas, de esta forma se podrá diferenciar un texto del otro.

Por lo que, por ejemplo, si se quiere cifrar la palabra *alba*, de tal forma que se sustituya la primera letra con el primer alfabeto, la segunda con el segundo, la tercera con el primero y la cuarta de nuevo con el primero, se tendría el código *JJMV*, y como podemos observar la letra en claro 'a' se ha sustituido por las letras en código J y V, rompiendo así un posible análisis de frecuencias.

Este disco cifrador de Alberti puede ser considerada como la primera máquina criptográfica, ya que como hemos visto en el ejemplo anterior, la característica principal del disco cifrador de Alberti es que el disco cambia su modo de cifrar durante la codificación [8].

Una evolución más compleja de este disco de cifras fue desarrollado casi 500 años después, en 1918 por los inventores alemanes Arthur Scherbius y Richard Ritter, cuya principal misión fue la de cambiar las cifras de "lápiz y papel" por una forma de codificación que aprovechara las tecnologías del siglo XX, este invento de Scherbius y Ritter, conocido como Enigma se puede ver como una versión electromecánica del disco de Alberti y se puede considerar ya como el más temible y famoso sistema de codificación de la historia. Una imagen de una máquina Enigma se puede ver en la siguiente figura:

Figura 6. Máquina Enigma

Estas máquinas contaban con tres elementos: un teclado, similar al actual teclado QWERTZ, distribución de teclado propia de países germanohablantes, donde se escribía el teclado a cifrar, un panel de lámparas en el que se iluminaba la letra que cifraba cada una de las letras del mensaje en claro, y sobre este panel de lámparas se encontraban el mecanismo que realizaba el cifrado propiamente dicho, el cual constaba de al menos tres rotores, cada uno con 26 contactos conectados entre sí, correspondientes a las 26 letras del alfabeto. En la figura de arriba se puede observar que se trata de una máquina Enigma de cuatro rotores, y por lo tanto usada por la Kriegsmarine, alguno de los mensajes cifrados por dicha máquina, de cuatro rotores, no han sido descifrados hasta fecha muy reciente como puede verse en [9].

Este mecanismo de rotores es el que le confería el mecanismo de cifrado de forma similar a como lo hacía el disco de Alberti. Hay que tener en cuenta que estos rotores son discos gruesos con conexiones que van de izquierda a derecha, siendo las conexiones de entrada, de más a la izquierda, las entradas introducidas por teclado y las conexiones de más a la derecha las conexiones que se verán por el tablero de lámparas, por lo tanto hay 26 puntos de entrada y 26 puntos de salida correspondientes al texto en claro y al texto cifrado respectivamente. Como ya se ha comentado básicamente cada rotor ejecutará un cifrado de sustitución.

Para clarificar el funcionamiento se puede ver el funcionamiento en una versión simplificada de un único rotor con un alfabeto limitado de 6 letras en la siguiente figura:

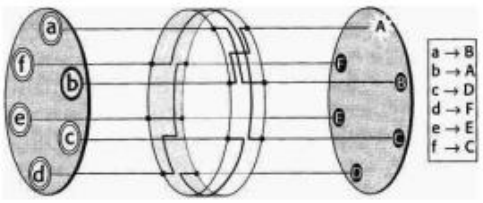


Figura 7. Versión simplificada de máquina Enigma con un rotor[7]

En la figura de arriba se puede ver que las siguientes conexiones efectuadas, una letra *b* en el teclado se cifrará como una *A*, la letra *e* irá directamente a ser cifrada como *E* y la letra *d* se cifrará como una *F*. Sin embargo, Scherbius ya sabía de la existencia de métodos de criptoanálisis que pueden romper un cifrado de sustitución como el descrito, con el ya citado análisis de frecuencias, por lo que se tuvo que buscar una forma de implementar un sistema de cifrado de sustitución múltiple. Esto se logró haciendo que el rotor girase cada vez que un impulso eléctrico pasara a través de él, es decir, cada vez que se pulsara una tecla en el teclado, cambiando la configuración de las conexiones y obteniendo así un sistema de sustitución polialfabética con un total de 26 posibles alfabetos, uno por cada letra.

Esta rotación de los rotores es un aspecto sumamente importante y es lo que le confiere a la máquina Enigma su robustez, no obstante hay una falla importante y es que cada 26 pulsaciones de teclado se volvería a la configuración inicial, provocando que haya cierta repetición en el texto cifrado y que, por consiguiente, éste sea más fácil de romper, es por ello por lo que una máquina Enigma tradicional tiene al menos tres rotores, como se muestra en la siguiente figura:

Figura 8. Esquema de tres rotores de máquina Enigma

Como se muestra en la figura de arriba la configuración inicial de los rotores es VLE, este es un aspecto esencial a la hora de poder desencriptar un mensaje. Cada vez que se pulsa una tecla el rotor más a la derecha, o rotor rápido, girará un intervalo, tal y como se explicó anteriormente, y cuando haya girado 26 veces, hará que el rotor del medio gire a su vez un intervalo, es el rotor a media velocidad y cuando éste haya girado a su vez 26 veces provocará que el rotor de más a la izquierda, o rotor lento, gire a su vez, por lo tanto se volverá a la configuración inicial después de 26x26x26=17.567 pulsaciones en el teclado

y no sólo de 26 como antes, lo que ayuda a que el código no sea tan regular y sea mucho más seguro.

El ejército alemán incluyó incluso un rotor adicional, denominado reflector, el cual se mantenía siempre estático, y su propósito era conectar un par de letras, lo que provocaba que el desciframiento fuera mucho más fácil, siendo ésta su mayor ventaja. Adicionalmente Sherbius añadió otra característica que sí que provocaba un complejidad adicional a la encriptación que fue un panel delantero en el que se conectaban cables conectando dos letras entre sí, de tal forma que si se conectaban entre sí la 'a' y la 'c' cuando el operador presionaba la 'a' en texto claro es como si hubiera presionado una 'c' con lo que la codificación se volvía mucho más compleja. Este panel de clavijas puede verse en la siguiente figura:

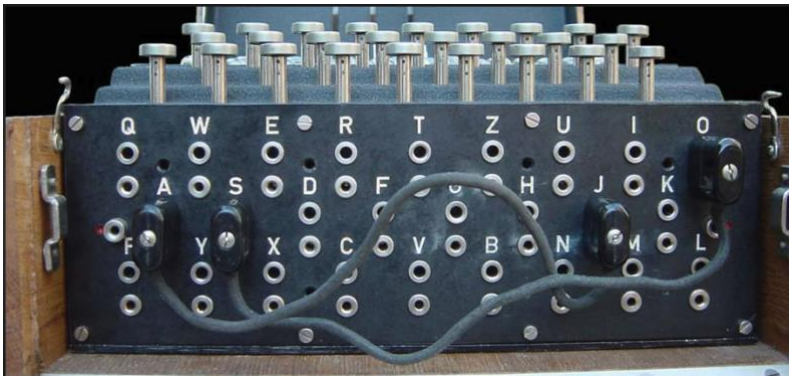


Figura 9. Panel de clavijas en máquina Enigma [10]

Para una transmisión y una recepción idóneas tanto emisor como receptor tenían que conocer previamente qué reflector usar y en qué posición debían conectarse los rotores, es decir debían intercambiarse las claves, para ello los operadores de Enigma disponían de un libro de claves que cambiaba normalmente cada mes, en este libro se mostraba qué reflector utilizar para cada día del mes, la posición de los rotores, qué posición colocar estos rotores y qué letras conectar en el clavijero.

Esto se puede ver en la siguiente figura, donde Tag es el día en el que se usará esta configuración, UKW es el reflector a usar, que casi siempre era el B, Walzenlage eran los rotores a usar, se utilizaban tres rotores de cinco posibles al principio de la 2ª Guerra Mundial mientras que al final se podían utilizar tres de ocho posibles rotores. Seguidamente se tiene la configuración de los rotores y por último Steckerverbindungen expone la unión de letras en el clavijero, como se ve, son diez conexiones ya que se vio que con diez aumentaba la complejidad ante una posible ruptura del código [14]

Tag	UKW	Walzenlage	Ringstellung	---- Steckerverbindungen ----
31	B	I IV III	16 26 08	AD CN ET FL GI JV KZ PU QY WX
30	B	II V I	18 24 11	BN DZ EP FX GT HW IY OU QV RS
29	B	III I IV	01 17 22	AH BL CX DI ER FK GU NP OQ TY

Figura 10. Ejemplo de intercambio de claves para Enigma

En la película *Descifrando Enigma* se muestra cómo Alan Turing para descifrar las comunicaciones construye una máquina, que él denomina *Christopher*, en recuerdo a un amigo suyo, aunque en realidad, esta máquina fue llamada la Bomba, en honor a la máquina electromecánica construida en 1938 por el polaco Marian Rejewsk, que fue llamada de la misma forma por el ruido que hacía. En la siguiente imagen se puede ver un fotograma de la película con la máquina construida por Turing:

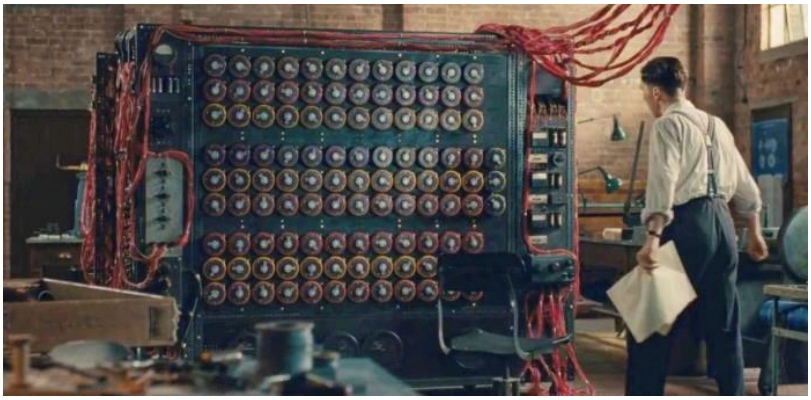


Figura 11. La bomba de Alan Turing en *Descifrando a Enigma* [12]

Muy similar a la máquina original como se puede ver en esta fotografía tomada en tiempos de guerra:

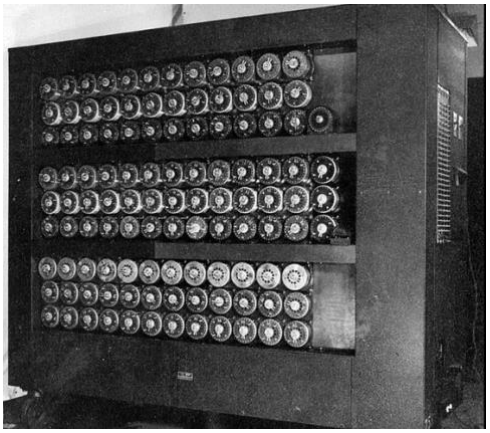


Figura 12. Fotografía de la Bomba tomada en tiempos de guerra [13]

Esta máquina utilizaba la fuerza bruta, con cada uno de los rotores de la máquina simulando un rotor de la máquina Enigma, aunque el número de combinaciones era enorme sobre todo gracias al clavijero ya que, como se ha indicado los alemanes se dieron cuenta que el número de parejas que aumentaba la dificultad eran de 10 parejas de letras [14] .El funcionamiento de esta máquina era la "criba" esto es, intuir que una palabra o una frase formaba parte del texto plano, sabiendo también que no podían coincidir la misma letra del texto cifrado con la misma letra del texto en claro, de esta forma, con palabras como "tiempo" o "Heil Hitler" que se utilizaban con frecuencia en los mensajes transmitidos, por la mañana en los informes del meteorológicos, fueron clave para que la Bomba pudiera romper el código Enigma tal y como como se puede ver en el siguiente video [52]

Mediante Cryptool 2 podemos observar el encriptado del mensaje “Estamos bajo ataque, se necesitan refuerzos PEC2 TFM”.

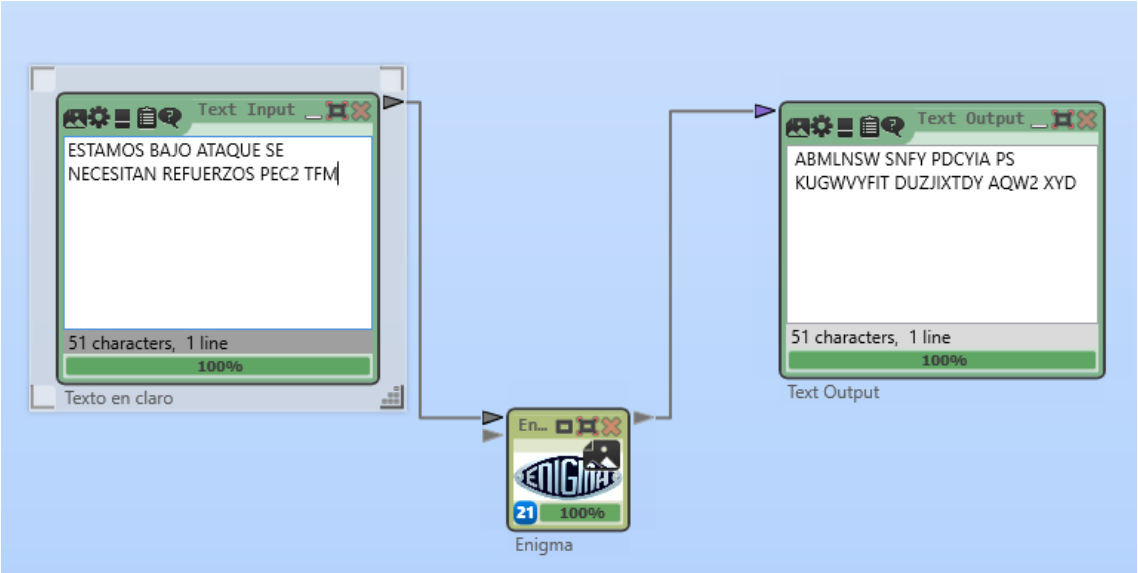


Figura 13.Ejemplo de uso de Enigma en CrypTool 2

En la simulación se han tenido que modificar la configuración de la caja Enigma, para elegir el tipo de máquina Enigma, los tipos de rotores, la posición inicial de los mismos, el reflector usado y las posiciones del clavijero intercambiadas tal y como se muestra a continuación:

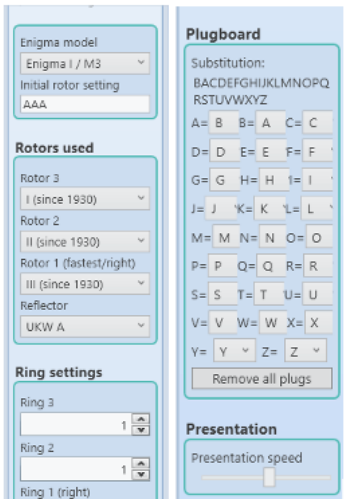


Figura 14. Configuración de Enigma en CrypTool 2

2.2 Rendezvous (1935)

Esta película basa su acción durante la 1ª Guerra Mundial, previa a todos los adelantos tecnológicos que estaban por llegar y, como ya se vio en el apartado anterior, basaba sus métodos criptográficos más en "lápiz y en papel" que en elementos electromecánicos como los utilizados durante la 2ª Guerra Mundial.

En ella se puede observar cómo se envía la información sobre la localización de la zona de reencuentro, o posición *Rendezvous*, de las tropas y provisiones provenientes de Estados Unidos con los destructores británicos cerca de la costa oeste de las islas británicas, las coordenadas de dicha zona de reencuentro no se pasará a los barcos en el mar ni a los destructores británicos, que actuarán como escolta de los primeros hacia el continente europeo, hasta el último día.

Estos datos son transmitidos por telegrafía por lo que irán de cinco en cinco letras y serán muy fáciles de interceptar mediante la antena apropiada, como se muestra en la película. En ésta se puede ver que, una vez interceptado las coordenadas de reencuentro en código, se apuntan en una tarjeta de invitación a una fiesta mediante tinta invisible. Este es un sistema de ocultación de la información que pertenece a una rama de la criptografía, conocida como *esteganografía*, que trata de cómo escribir un mensaje de modo que quede encubierto u oculto. Tal y como se puede leer en [8] hay diversos métodos de aprovisionarse de tinta invisible o tinta simpática, como por ejemplo la "leche" de la planta *Thithymallus* que se vuelve transparente al secarse pero se vuelve marrón al calentarla suavemente, de hecho esto pasa con muchos fluidos orgánicos ricos en carbono, como la orina. Es más, se sabe que espías modernos que no disponen de tinta invisible utilizan su propia orina para lograr esta tinta invisible. Sin ir más lejos los zumos de limón o de cebolla también serían válidos como tinta simpática, como puede leerse en (Carmona,1895), también se sabe que era común que estos mensajes se escriban entre las líneas de una carta realizada con tinta común, para que no llamara la atención una hoja en blanco.
Es posible unir la criptografía y la esteganografía en un único mensaje tal y como se ve en la película al apuntar los códigos con tinta invisible en una tarjeta de invitación a una fiesta en la embajada y así ganar un mayor grado de confidencialidad.

En la película, una vez que el capitán Nieterstein recibe este mensaje en la fiesta de la embajada, trata la carta recibida con los reactivos necesarios para poder desvelar la escritura con tinta invisible y en ella se leen los códigos recibidos en cifras agrupadas de cinco en cinco. Como se sabe "un código se define como una sustitución al nivel de las palabras o las frases, mientras que una cifra se define como una sustitución al nivel de las letras [..] el término cifrar significa ocultar un mensaje utilizando una cifra, mientras que codificar significa ocultar un mensaje utilizando un código. De manera similar, el término descifrar se aplica a la resolución de un mensaje cifrado, es decir, en cifra, y el término descodificar a la resolución de un mensaje codificado" [8], es decir un código es un nivel de sustitución superior a la de la cifra de sustitución ya que mientras que la última se trata de una sustitución en la que cada letra es sustituida por otra letra, número o símbolo diferente, el código trata de la sustitución a nivel de palabras.

A continuación se muestra un esquema de la escritura secreta con la diferenciación entre código y cifra:

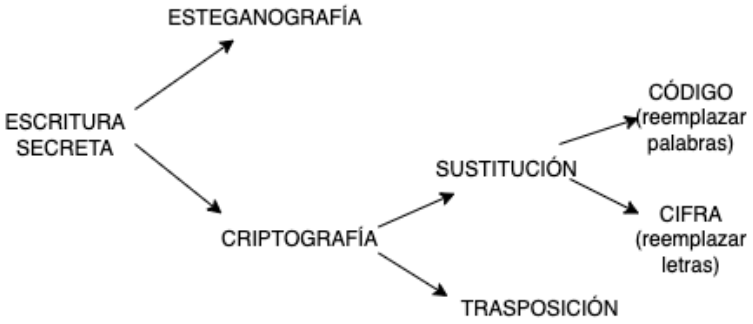


Figura 15 Esquema de la escritura secreta [8]

A primera vista pareciera que la utilización de un código es mucho más seguro que el uso de un cifrado ya que las palabras son mucho menos vulnerables frente a un ataque de análisis de frecuencias que las letras, sin embargo hay que recordar que hay dos defectos principales de un código, el primero es que una vez definido la clave a utilizar en cada una de las 26 letras del alfabeto, tanto el emisor como el receptor pueden comunicar cualquier mensaje, mientras que si se deciden por la utilización de un código se han de limitar a las palabras definidas en dicho código, y redactar un libro de código es una tarea complicada y además ha de repartirse entre todas las partes implicadas en la comunicación, además de tener que esconderse debidamente, ya que la captura del libro de códigos por un enemigo tendría muy graves consecuencias tanto en la ruptura del código por el enemigo como del futuro del espía en sí, de hecho, al final de la película esto es lo que provoca la captura y muerte del capitán Nieterstein.

En la siguiente imagen de la película se puede ver como éste acude a su libro de códigos para descodificar el mensaje que ha recibido:

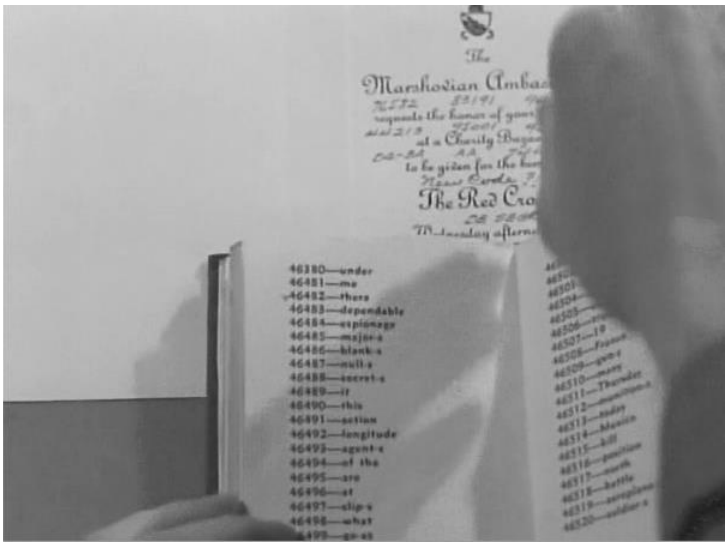


Figura 16. Utilización de libro de códigos en Rendezvous

Mediante la herramienta CrypTool 2 se podrá crear nuestro propio libro de códigos en español tal y como como puede verse en [24], en la siguiente imagen vemos el resultado en código de haber introducido el texto “nos atacan estamos rodeados y estamos haciendo la PEC2”:

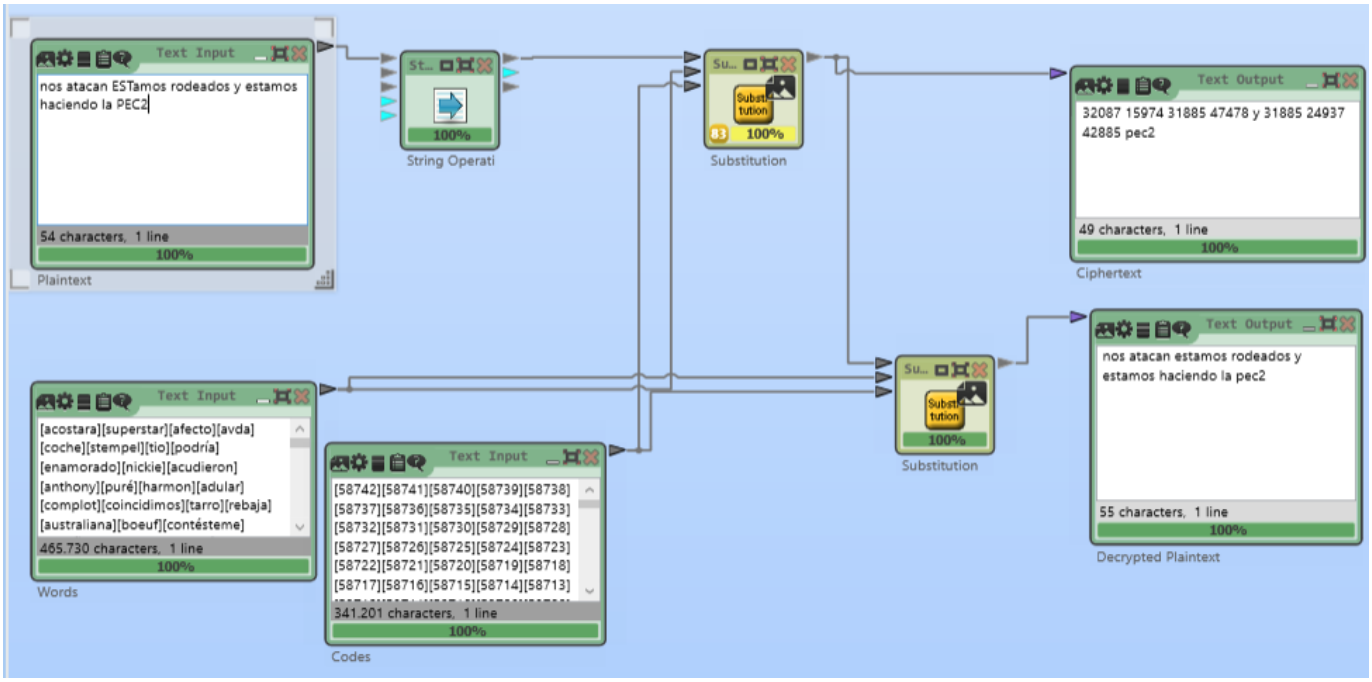


Figura 17. Configuración de libro de códigos en CrypTool 2

Abajo a la izquierda tenemos nuestro diccionario con más de 53.000 palabras en español sacadas de la propia herramienta Cryptool 2, esta caja de denomina *Words*, a su derecha tenemos su correspondencia en código, en la caja denominada *Codes*, antes se ha hecho corresponder cada palabra a un número de cinco cifras y se han organizado de forma aleatoria mediante una hoja Excel tal y como se explica en [24], con el fin de que no haya ninguna correlación que pudiera hacer este código vulnerable. Como se ve, tanto el texto que se introduce “nos atacan estamos rodeados y estamos haciendo la PEC2”, como el diccionario y sus códigos son entrada a una caja de substitución, configurada como encriptación, donde se llevará a cabo esta substitución y se presentará en la caja de salida de *text output* de arriba a la derecha, el código resultante es *32087 15974 31895 47478 Y 31885 24937 42885 PEC2*, como se puede observar si una palabra no está en el diccionario no se podrá codificar, lo que ocurre con pec2 y con la conjunción ‘y’. También se puede observar abajo a la derecha otra caja que desencripta el mensaje y muestra el mensaje en claro introducido previamente.

Este mensaje tiene el mismo formato que el famoso telegrama Zimmerman por el cual Estados Unidos entró en la primera guerra mundial [24], este telegrama como podemos observar en la fuente facilitada, fue descifrado por el llamado Hall40 de la inteligencia británica y propició la entrada de Estados Unidos en la 1ª Guerra Mundial, puesto que desvelaba los planes de Alemania de que, en caso de que los Estados Unidos entraran en guerra, por la campaña de ataques submarinos que Alemania pensaba acometer, México

hiciera una alianza con Japón para atacar los Estados Unidos. A continuación se muestra una fotografía de dicho telegrama:

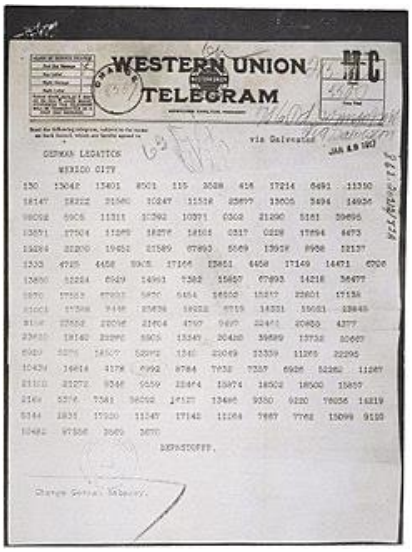


Figura 18. Telegrama Zimmerman

En la película se muestra también cómo se usa del análisis de frecuencias y de las características propias de los idiomas para tratar de descifrar el código, algo propio de descifrar criptogramas codificados con códigos de sustitución monoalfabéticas, como se explicó también en el anterior apartado. Así se puede ver que se descarta que un mensaje interceptado esté en inglés ya que no aparecen e's y, como en español, la 'e' es la letra más frecuente en inglés con un 12,7% de aparición; tampoco podía ser alemán, porque se detectaron múltiples 'q's y en alemán no existe la letra 'q', por lo que la deducción prosigue en que tampoco puede ser el español, puesto que en español toda letra 'q' va seguida de una 'u' y no se ha detectado ninguna, esto muestra el razonamiento seguido en el análisis de frecuencias de un código interceptado.

También se muestra, para el criptoanálisis de un código recibido, se intenta descifrar éste asumiendo que se ha utilizado un código César, así se van probando distintas claves, o distancias, empezando con una clave 1. Se puede ver que también se utiliza, como ayuda, los ya presentados discos de Alberti, con el anillo externo fijo y el interno móvil, como se recordará el anillo externo representaba el texto en claro mientras que el interno representa el texto cifrado. En la siguiente figura se observa un fotograma de la película con la utilización de estos discos:

Figura 19. Discos de Alberti en Rendezvous

En la anterior escena de la película el protagonista iba probando diferentes claves en un cifrado César hasta que encontró que con una distancia igual a 5 hacia delante y hacia atrás repetidamente sobre las letras interceptadas KDWNY se obtenía un texto en claro coherente, *first*, no obstante, si se seguía descifrando de la misma forma no se seguía obteniendo un resultado coherente. Este tipo de sustitución puede determinarse como una sustitución de doble clave, que como se lee en [17] "[...] se trata de un conjunto de substituciones simples que se van aplicando sucesivamente a distintos fragmentos del claro y hay por tanto, dos claves que afectan a cada unidad de cifra: la que determina qué substitución se le aplicará y dicha substitución en sí".

Ante esto, el protagonista deduce que, al ser día uno, *first* en inglés, estas primeras cinco letras, que son las fechas en la que se envía el mensaje, sirven como base para descifrar el resto del criptograma, y mediante los discos de cifrado construye alfabetos en la que cada una de las letras del código interceptado es una 'a' en el texto en claro, como se ve en la siguiente imagen sacada de la película [16]:

Figura 20.Configuración disco de Alberti

Arriba se puede ver que considera la letra ‘F’ descifrada con un sistema de sustitución como la ‘a’ y así con el resto de las cinco letras de *first*, se puede descifrar el resto del mensaje, con la ayuda de los discos cifradores.

En siguientes escenas se describe el uso de tintas simpáticas y los reactivos para hacerlas aparecer, argumentando que cada tinta tiene su propio reactivo, como se puede ver en [18]. El uso de tintas simpáticas o invisibles han tenido y tienen una gran importancia dentro del espionaje y uso en tiempos de guerra, como método esteganográfico, incluso hasta tiempos muy recientes la CIA no ha desclasificado documentos de la I Guerra Mundial haciendo referencia al uso de la tinta invisible durante esta contienda [19]. Como se puede leer en este documento, el hecho de que la desclasificación de estos documentos sobre el uso de tintas invisibles haya sido tan tardía responde al hecho de que algunos de los métodos de fabricación de las respectivas fórmulas de tintas simpáticas eran consideradas como fiables y todavía seguían en uso por esta agencia, por lo tanto, descubrir estos documentos antes de tiempo, conllevaría una gran brecha en la seguridad del país.

Como se relata en [20], “con los avances en química orgánica durante el siglo XIX, la tinta invisible se convirtió en algo mucho más complejo que la carbonización de compuestos orgánicos en zumo de frutas, leche o vino para hacerlas visibles […] no fue hasta la 1ª Guerra Mundial cuando los laboratorios de los distintos gobiernos empezaron a experimentar con la creación y detección de tinta invisible […] las diversas agencias de espionaje del siglo XX desarrollaron sofisticados métodos como el impregnar toda una hoja de papel con un determinado compuesto que, actuando como una especie de papel carbón, se colocaba entre el papel que se escribía y donde se quería escribir el mensaje, apareciendo como una escritura invisible en la hoja inferior. En años posteriores, sobre todo durante la Guerra Fría, se desarrollaron métodos que mediante el uso de catalíticos con tan sólo una minúscula cantidad de compuesto hacían esta tinta mucho más difícil de detectar”. A continuación se muestra la imagen de una fórmula de tinta invisible desarrollada por la Stasi:

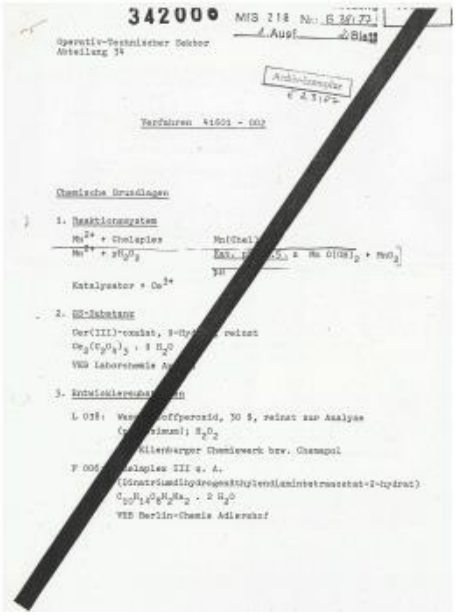

342000 MfS 218 Nr.: 6 367/79
1. Ausf. 2 Bla.
Operativ-Technischer Sektor
Abteilung 34
Archivexemplar
Verfahren 41601 - 001
Chemische Grundlagen
1. Reaktionssystem
Katalysator + Co^{3+}
2. UV-Tabstanz
Cer(III)-oxalat, 9-Hydrat, reinst
$Ce_2(C_2O_4)_3 \cdot 9\ H_2O$
VEB Laborchemie Apolda
3. Entwicklerverbindungen
L 038: Wasserstoffperoxid, 30 %, reinst zur Analyse
(H_2O_2 100 %ig); H_2O_2
Kali-Chemie Aktiengesellschaft Hannover
F 006: Chelaplex III s. A.
(Dinatriumsalz der Hydroxyäthyläthylendiamintriessigsäure-2-hydrat)
$C_{10}H_{14}O_8N_2Na_2 \cdot 2\ H_2O$
VEB Berlin-Chemie Adlershof

Figura 21. Fórmula original de la Stasi para tinta invisible [20]

Se puede decir, sin ningún género de dudas, que todos los apuntes criptográficos reseñados en la película son acertados y próximos a su verdadero uso.

2.3 Windtalkers (2002)

Esta película de 2002, está ambientada también durante la 2ª Guerra Mundial en la campaña del Pacífico, que enfrentó directamente a los Estados Unidos contra Japón. Esta campaña se veía continuamente ralentizada debido a que los japoneses descifraban constantemente los códigos utilizados por los Estados Unidos en sus comunicaciones.

No fue hasta 1942 cuando Philip Johnston, un ingeniero de Los Ángeles aportó la idea de utilizar la lengua de los indios navajo para las transmisiones secretas, al ser una lengua con ninguna conexión con las lenguas europeas o las asiáticas, esto fue de gran utilidad puesto que el idioma navajo simplificaba enormemente la transmisión. En un principio se creó el siguiente alfabeto completo [2]:

ALFABETO	NAVAJO	INGLÉS	CASTELLANO
A A A	Wol-la-chece Be-la-sa-na Tsenil	Ant Apple Axe	Hormiga Manzana Hacha
B B B	Shush Najash-chid Toisho-lle	Bear Badger Barrel	Oso Tejón Barril
C C C	Moasi Tlallin Bagoshi	Cat Coal Cow	Gato Carbón Vaca
D D D	Be Chindi Llachae	Deer Devil Dog	Ciervo Demonio Perro
E E E	Dzeh Alla Ana	Moose Ear Eye	Alce Oreja Ojo
F F F	Ma-e Chuo Tsaedonin-e	Fox Fir Fly	Zorro Pino Mosca
G	Klizzie	Goat	Cabra
H	Lin	Horse	Caballo
I	Tkin	Ice	Hielo
J	Tkele—cho-gi	Jackass	Burro
K	Klizzie-yazzie	Kid	Cabrito/chaval
L	Dibeh-yazzie	Lamb	Cordero
M	Na-as-tso-i	Mouse	Ratón
N	Nesh-chee	Nut	Nuez

O	Ne-ash-ji	Owl	Buho
P	Bi-sodih	Pig	Cerdo
Q	Ca-yeilth	Quiver	Carcaj
R	Gah	Rabbit	Conejo
S	Dibeh	Sheep	Oveja
T	Than-zie	Turkey	Pavo
U	No-da-ih	Ute	Piel roja/indio
W	Gloe-ih	Weasel	Comadreja
X	Al-keh-di-glini	Victor	Vencedor
Y	Tsah-as-zih	Yucca	Yuca
Z	Besh-do-gliz	Zinz	Zinc

Tabla 4. Alfabeto código navajo [2]

Con la ayuda de la anterior tabla nombres como “Compañía A” o “Compañía Alfa” se cifrarían como “Compañía Hormiga”, “Compañía Manzana” o “Compañía Hacha” lo que se traducía al lenguaje navajo como “Wol-la-chece”, “Be-la-sa-na” o “Tsenil”, esto, a modo de código de sustitución, es una sustitución homofónica que dificultaba enormemente el criptoanálisis por los japoneses, de hecho este código, denominado código navajo, jamás fue descifrado.

Los nombres propios se traducían al navajo y luego se transmitían letra por letra. Con la inicial de cada letra transmitida se formaba el nombre, por ejemplo, Guadalcanal, una de las más decisivas batallas en la campaña del Pacífico, se codificaría con las iniciales del siguiente mensaje [2]:

GIRL, UNCLE, ANT, DEVIL, APPLE, LION, CAT, AXE, NEEDLE, AXE, LAMB

que había sido traducido al inglés del navajo que transmitió el emisor:

ATAD, SHIDA, WOLACHI, CHINDI, BELASANA, NASHDOIETSO, MOUSI, TSENIL, TSA, TSENIL, DIBEYATZIE.

No obstante, el gran inconveniente de este código estribaba en que en el lenguaje navajo no existían términos modernos como tanque, submarino, acorazado etc, por lo que se vio la necesidad de crear un léxico para los términos navajos que no podían traducirse al inglés, algunos de los cuales, referidos a barcos y vehículos militares acuáticos, se pueden ver en la siguiente tabla:

BARCOS	INGLÉS	NAVAJO	CASTELLANO
Acorazado	Whale	Lot-so	Ballena
Destructor	Shark	Ca-lo	Tiburón
Submarino	Iron fish	Be-shio	Pez de hierro
Vehículo anfibio	Frog	Cha	Rana

Tabla 5 Código navajo de vehículos militares acuáticos [2]

De igual forma, los tanques o carros de combate eran codificados como CHAYDAGAHI o “tortugas” y las bombas como A-YE-SHI. Esto se puede ver en el siguiente fotograma sacado de la película:

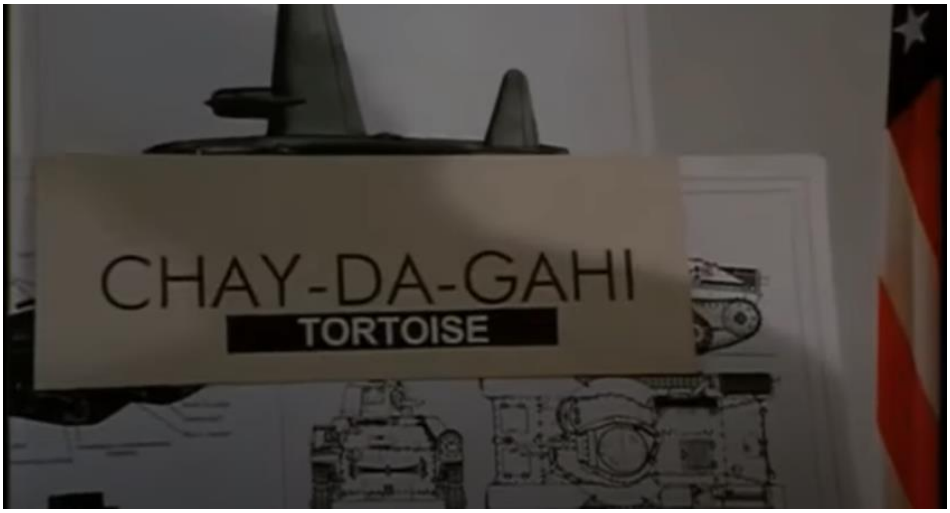


Figura 22. Codificación de tanque en código navajo [21]

Aunque los minutos dedicados a la explicación del código navajo en la película son muy escasos, se puede afirmar que el acercamiento a la explicación de los términos es el correcto como se ve en la anterior imagen, que es un fotograma sacado de la película. El código navajo, forma parte de uno de los pocos códigos en la historia que jamás fue descifrado por el enemigo, de hecho, volvió a ser usado durante la guerra de Corea.

Este código navajo también podrá ser simulado en Cryptool 2, como se puede ver en la figura donde se muestra el “layout” para el uso del código navajo en esta herramienta. Arriba a la izquierda es la caja de plaintext, donde introduciremos nuestro texto a codificar, justo debajo se encuentra el código navajo, con todas las correspondencias anteriormente citadas

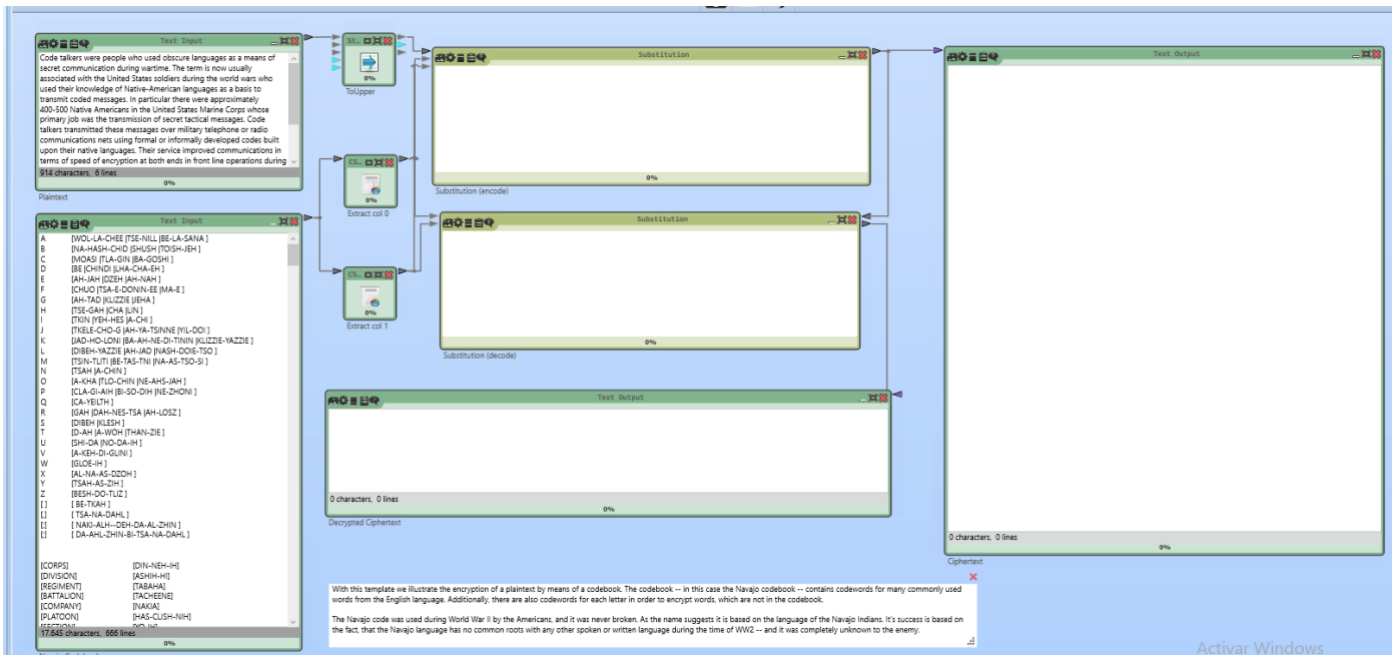
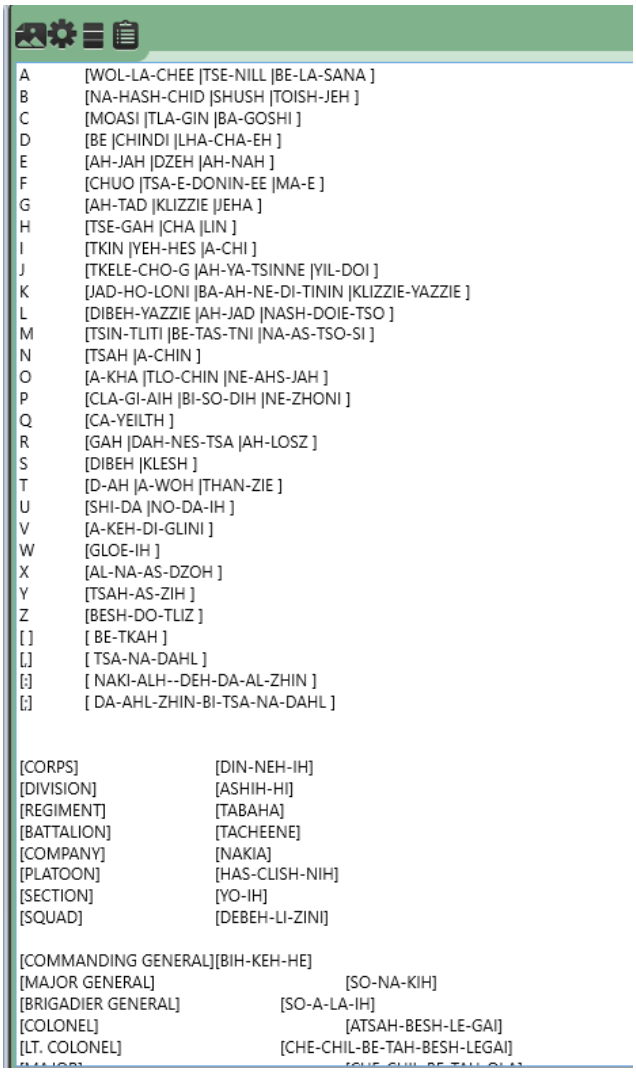


Figura 23. Código navajo en Cryptool2

A continuación se muestra un detalle del diccionario para el código navajo utilizado en Cryptool 2:



```
A       [WOL-LA-CHEE |TSE-NILL |BE-LA-SANA ]
B       [NA-HASH-CHID |SHUSH |TOISH-JEH ]
C       [MOASI |TLA-GIN |BA-GOSHI ]
D       [BE |CHINDI |LHA-CHA-EH ]
E       [AH-JAH |DZEH |AH-NAH ]
F       [CHUO |TSA-E-DONIN-EE |MA-E ]
G       [AH-TAD |KLIZZIE |JEHA ]
H       [TSE-GAH |CHA |LIN ]
I       [TKIN |YEH-HES |A-CHI ]
J       [TKELE-CHO-G |AH-YA-TSINNE |YIL-DOI ]
K       [JAD-HO-LONI |BA-AH-NE-DI-TININ |KLIZZIE-YAZZIE ]
L       [DIBEH-YAZZIE |AH-JAD |NASH-DOIE-TSO ]
M       [TSIN-TLITI |BE-TAS-TNI |NA-AS-TSO-SI ]
N       [TSAH |A-CHIN ]
O       [A-KHA |TLO-CHIN |NE-AHS-JAH ]
P       [CLA-GI-AIH |BI-SO-DIH |NE-ZHONI ]
Q       [CA-YEILTH ]
R       [GAH |DAH-NES-TSA |AH-LOSZ ]
S       [DIBEH |KLESH ]
T       [D-AH |A-WOH |THAN-ZIE ]
U       [SHI-DA |NO-DA-IH ]
V       [A-KEH-DI-GLINI ]
W       [GLOE-IH ]
X       [AL-NA-AS-DZOH ]
Y       [TSAH-AS-ZIH ]
Z       [BESH-DO-TLIZ ]
[ ]     [ BE-TKAH ]
[,]     [ TSA-NA-DAHL ]
[:]     [ NAKI-ALH--DEH-DA-AL-ZHIN ]
[;]     [ DA-AHL-ZHIN-BI-TSA-NA-DAHL ]


[CORPS]                 [DIN-NEH-IH]
[DIVISION]              [ASHIH-HI]
[REGIMENT]              [TABAHA]
[BATTALION]             [TACHEENE]
[COMPANY]               [NAKIA]
[PLATOON]               [HAS-CLISH-NIH]
[SECTION]               [YO-IH]
[SQUAD]                 [DEBEH-LI-ZINI]

[COMMANDING GENERAL][BIH-KEH-HE]
[MAJOR GENERAL]                 [SO-NA-KIH]
[BRIGADIER GENERAL]         [SO-A-LA-IH]
[COLONEL]                       [ATSAH-BESH-LE-GAI]
[LT. COLONEL]               [CHE-CHIL-BE-TAH-BESH-LEGAI]
```

Figura 24. Detalle del diccionario utilizado para código navajo utilizado en Cryptool2

Como se puede ver en la anterior figura el diccionario utilizado en Cryptool 2 es el mismo que el presentado con anterioridad, si realizamos una simulación con este código e introducimos " nos atacan major general y estamos haciendo la pec2" se obtiene lo siguiente imagen:

Figura 25. Resultado de encriptación usando código navajo.

Mostramos el detalle de la codificación:

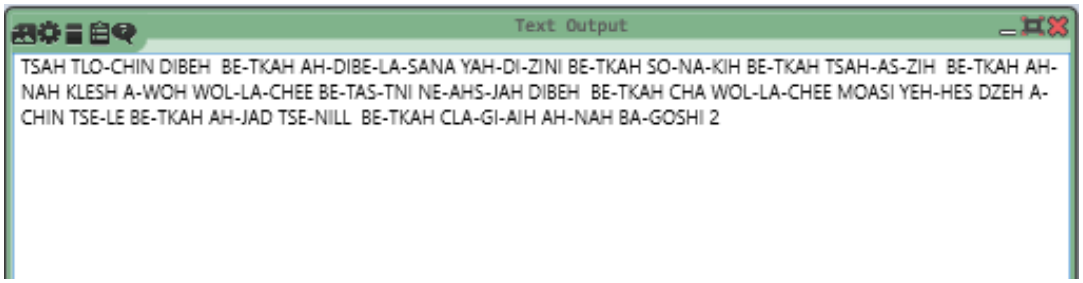


Figura 26. Detalle de codificación navajo

Como se puede observar en la imagen anterior, major general se codificaba como SO-NA-KIH que se puede observar en el resultado de la codificación, los números no eran codificados.

2.4 La clave está en Rebeca (1985)

Esta película, basada en el libro homónimo de Ken Follet, basa su acción durante la campaña de África comandada por el mariscal Erwin Rommel durante la 2ª Guerra Mundial. En ella se describe la acción de un espía nazi infiltrado dentro de la ciudad de El Cairo, en esos momentos colonia inglesa.

Toda la comunicación entre el espía y el ejército alemán, que se encontraba a las puertas de El Cairo, se realiza a través de telégrafo utilizando el método de cifrado por libro o cifrado *Ottendorf*.

Como se puede ver en [23] un cifrado por libro o Cifrado Ottendorf funciona reemplazando palabras del texto claro de un mensaje con la ubicación de estas palabras en el texto del libro, por lo que más que un método de cifra se trataría de un código, aunque si lo que se va a transmitir es la posición de cada letra sí que se puede afirmar que es un cifrado. Como se puede leer en [2], y como se ha explicado en el apartado 2.2, se tiene que recordar que la gran diferencia entre el lenguaje cifrado y el codificado es que con el lenguaje cifrado podemos expresar cualquier mensaje, mientras que con el lenguaje codificado solo se pueden transmitir los símbolos que contiene el diccionario del código de que se trate, por lo que si esta palabra no está en el diccionario no se podría transmitir.

Como ya se ha comentado y se reafirma en [23] una condición indispensable para llevar a cabo un envío de información mediante este método es que, tanto el emisor como el receptor tienen que ser poseedores de exactamente el mismo libro, de la misma edición, esto puede confirmarse en la película ya que se puede ver que tanto el espía como los militares en el frente alemán utilizan la misma edición del libro.

Se puede afirmar también que existen dos aproximaciones o esquemas de encriptación por este método, y que tanto emisor como receptor se tendrán que poner de acuerdo para usar:

1. Codificación letra por letra.

2. Codificación por palabra completa

Al mismo tiempo, el emisor como el receptor también tienen que saber y ponerse de acuerdo de qué es lo que se codifica, si se codifica una página, una línea o una palabra.

Un ejemplo de un **esquema de codificación letra por letra** se puede dar, por ejemplo, si tomamos los siguientes versos de un poema de Antonio Machado como clave [2]:

La primavera besaba
suavemente la arboleda
el verde nuevo brotaba
como una verde humareda

si queremos transmitir cifrada la palabra *corre* nos fijaremos en que la primera letra se encuentra en la línea 4 y es la letra 1 de esta línea, por tanto esta letra se podría cifrar como 1/4. La segunda letra la podemos tomar de donde queramos, si la tomamos de la segunda línea, cifraríamos entonces como 16/2. La tercera letra, la podemos tomar de la primera línea como 4/1, la segunda 'r' se podría utilizar la misma, pero para disminuir cifrados repetidos se podría tomar la 'r' de la tercera línea como 5/3, y por último, la letra 'e' podrá ser 1/3 por lo que entonces la palabra *corre* podría cifrarse como *1/4 16/2 4/1 5/3 1/3*. Con un libro se podría también añadir el número de página de donde se toman las letras para una mayor claridad en el mensaje.

Otra aproximación para un esquema de codificación por letra sería el de escribir la posición de una palabra en el texto que empiece por esa misma letra, en el caso anterior si queremos transmitir *corre*, vemos que no hay palabras en el texto que empiecen por 'o' o por 'r' por lo cual esta aproximación a la codificación letra por letra no puede ser usada.

Sin embargo, si elegimos como texto a usar los siguientes versos de José de Espronceda sacados de "El estudiante de Salamanca":

Que el alma virgen que halagó un encanto
Con nacarado sueño en su pureza,
Todo lo juzga verdadero y santo
Presta a todo virtud, presta belleza.
Del cielo azul al tachonado manto,
Del sol radiante a la inmortal riqueza,
Al aire, al campo, a la fragantes flores,
Ella añade esplendor, vida y colores.

Cifró en don Félix la infeliz doncella
Toda su dicha, de su amor perdida;
Fueron sus ojos a los ojos de ella
Astros de gloria, manantial de vida.
Cuando sus labios con sus labios sella
Cuando su voz escucha embebecida

Y se quiere seguir la aproximación anterior con la palabra a enviar *corre* bastaría con haber sido cifrada como 9 70 35 35 48, en el texto se marcan en colores las posiciones de la palabras que empiezan con las letras para una mayor claridad. En este caso, el utilizar dos veces la cifra 35 puede ser peligroso desde el punto de vista del criptoanálisis, ya que si el que intenta romper el código sabe que el idioma que se está usando es el español, sabrá que hay pocas letras en este idioma que se puedan repetir en una misma palabra, tan sólo la 'll' y 'rr' por lo que sin duda estaríamos facilitando mucho la ruptura de la cifra.

Si se quiere seguir un **esquema de codificación por palabra**, se tiene que enviar la posición de la palabra que se quiere enviar dentro del libro o texto elegido, esta aproximación consiste en buscar la palabra exacta que se quiere mandar dentro del texto elegido y anotar la posición de la palabra dentro de este texto. Lógicamente si la palabra no se encuentra en el texto ésta no podrá ser encriptada, como pasa con la palabra corre que no puede ser codificada con este método y este texto. Por ejemplo con los anteriores

versos de Espronceda si queremos encriptar *amor escucha*, se podrá mandar la posición de estas palabras en el texto:

amor escucha ->66 92

También se podría haber enviado la línea y la posición de la palabra en esa línea, por ejemplos *amor* es la sexta palabra de la línea diez y *escucha* es la cuarta palabra de la línea catorce:

amor escucha -> 1006 1404

Si volvemos a la película, en las escenas en las que el espía retransmite las posiciones del ejercito inglés, vemos que éste cuenta letras sobre el libro *Rebeca*, por lo cual se puede asumir que está contando la posición de las letras en el libro para poder retransmitirlas por telégrafo, para formar lo que quiere retransmitir, como se puede ver en al siguiente imagen sacada de la película:

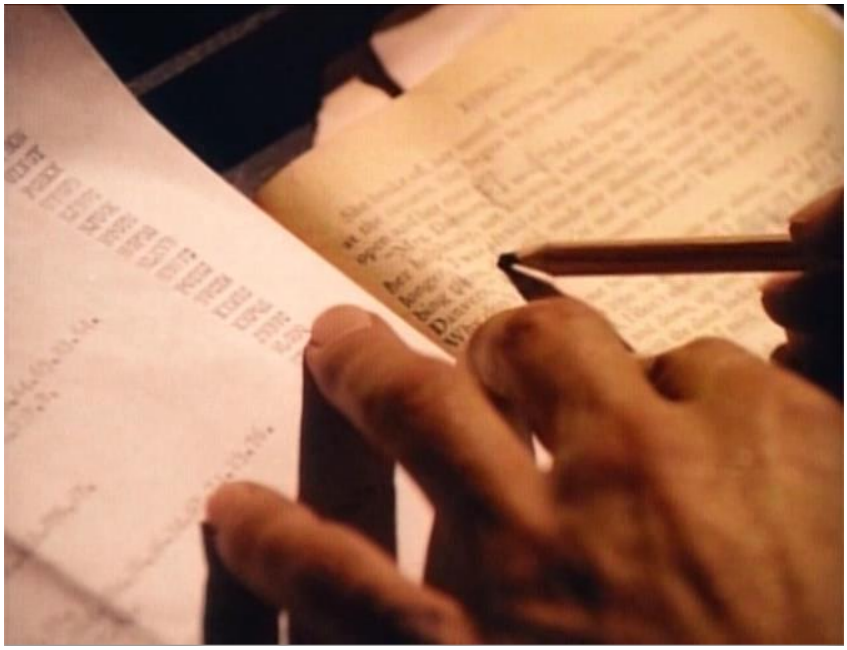
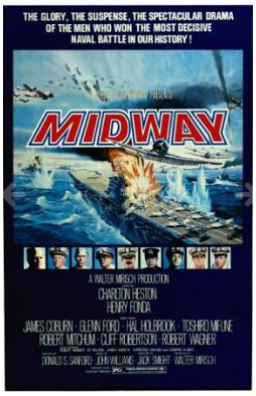


Figura 27. Conteo de letras en "La clave está en Rebeca" [22]

Por lo que se puede asumir, por esta escena, que la representación de la codificación por cifrado de libro o método Ottendorf es la correcta.

En este caso se puede reseñar que es mucho más seguro para el espía el utilizar esta método de cifrado por libro que el utilizar un libro de códigos. Un libro, como una novela, no despierta sospecha ninguna, sin embargo un libro de códigos supondría poner en peligro todas las comunicaciones y el castigo al poseedor.

2.5 La batalla de Midway (1976)



Esta película de 1976, basa su historia durante la 2ª Guerra Mundial, durante la campaña del Pacífico que enfrentó a Estados Unidos y Japón.
Después del ataque a Pearl Harbour los americanos pudieron bombardear el mismo Tokyo, por lo que era de esperar una acción inminente por parte del almirante Yamamoto, comandante en jefe de la Flota Combinada de la Armada Imperial Japonesa durante la Segunda Guerra Mundial.

En la película se ve como el ejército americano capta como un avión enemigo sobrevuela un territorio que es telegrafiado por los japoneses como *AF*, por su ruta y trayectoria el ejército americano intuye que AF es la isla de Midway. Utilizando un engaño, los americanos indican que Midway sufre de problemas de abastecimiento de agua, a lo que los japoneses telegrafiaron a su comandancia que AF sufría problemas de abastecimiento de agua, por lo que los americanos pudieron confirmar sus sospechas de que Midway iba a ser atacada.

En la misma película se narra como, aunque el ejército americano conoce la clave del cifrado JN-25 usado por Japón, sólo podían descifrar un 10% de las comunicaciones japonesas. Una de las formas, por las que el ejército americano pudo saber que el ejército japonés tramaba algo después del ataque a Tokyo, fue por el aumento de las comunicaciones emitidas por los japoneses, lo que no deja de ser una forma de detectar un ataque basado en anomalías, al igual que en el caso de la ciberseguridad informática tal y como se puede leer en [26] "[…] hay una gran probabilidad de que si el sistema ha sido hackeado, se note uno o más de los siguientes comportamientos: Tráfico de red altamente sospechoso […] aumento de la actividad del disco […] gran número de paquetes que provienen de una única dirección[…]" y también en [27] "Anomaly detection is an important data analysis task that detects anomalous or abnormal data from a given dataset […] an unusual traffic pattern in a network could mean that a computer has been hacked and data is transmitted to unauthorized destinations […]" se puede ver la similitud de detectar un ciberataque en un equipo Windows o Unix a como el ejército estadounidense pudo prever que se produciría un ataque del ejército japonés.

En otro fragmento de la película se hace observar que los japoneses han cambiado la clave de su código JN-25, por medio de la cual los americanos se enteraban de los planes de Yamamoto Este código JN-25 fue un código desarrollado por la Armada Imperial Japonesa durante la 1ª Guerra Mundial [27] de ahí el nombre dado por el ejército americano *Japanese Navy 25*, este código no utilizaba ningún sistema electromecánico, al contrario de la máquina Enigma, sino que era más bien un sistema manual que consistía de dos partes, un diccionario de 33.333 letras, palabras y frases, que tenían asignadas un número de cinco dígitos, algo muy similar al sistema utilizado con el telegrama Zimmerman como se vio en el apartado 2.2 y también desarrollado durante la 1ª Guerra Mundial. Cabe destacar que para las palabras que no estaban incluidas en el diccionario, se empleaba el silabario kana, también usando un número de cinco dígitos por cada carácter japonés. "La segunda parte la componía unas tablas sumatorias numeradas, con números aleatorios alineados en líneas y columnas también identificadas con números que por razones de seguridad se reemplazaban cada seis meses. A continuación se puede observar, una parte del diccionario usado en esta cifra JN-25:

Figura 28. Diccionario JN-25

Un ejemplo de mensaje interceptado por el ejército americano en junio de 1939, cifrado con este sistema de cifrado JN-25, puede verse en la siguiente figura:

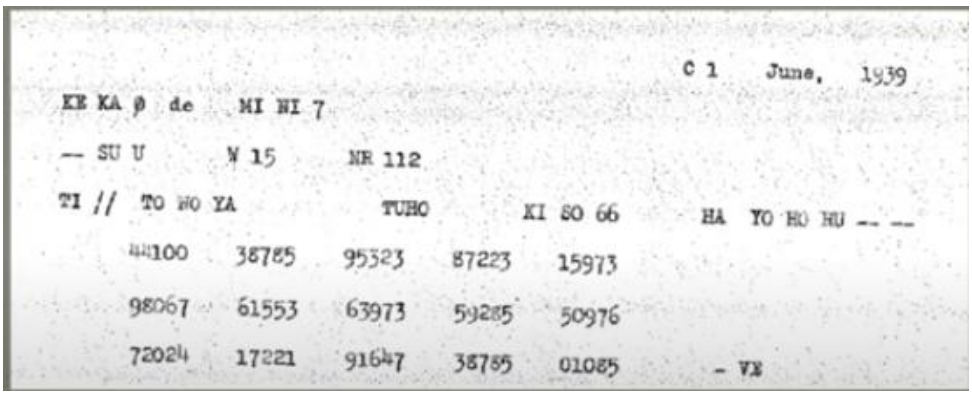
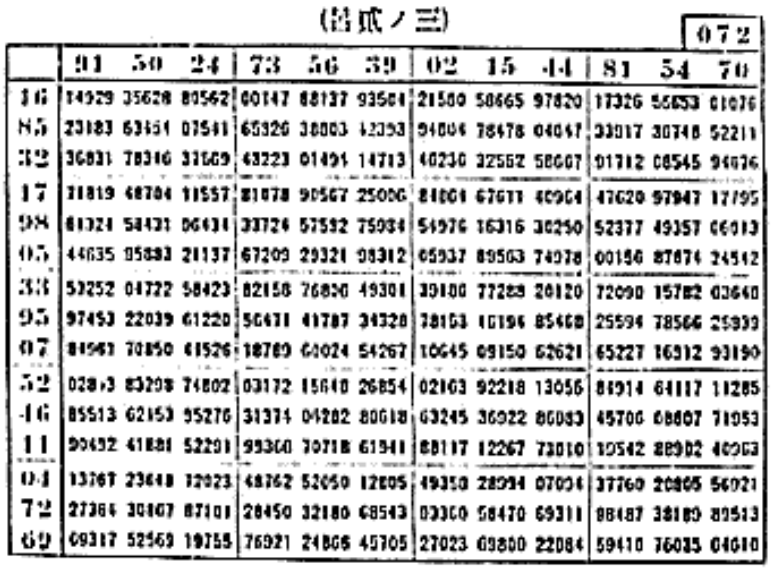


Figura 29. Mensaje interceptado en cifra JN25

Como se puede ver arriba y como ya se ha reseñado éste era un código que producía grupos de cinco números para la transmisión, aunque se introducían de vez en cuando nuevos libros de códigos y libros de supercifrado y con cada nueva versión se requería otro ataque de criptoanálisis distinto. John Tiltman, con la ayuda de Alan Turing, descubrió que se trataba de un cifrado por libro de código al que se sumaba otro libro "aditivo" que el emisor agregaba a los números originales, aunque saber esto sólo, no

ayudó a leer un solo mensaje ya que como se reseña en la película, a principios de 1942 sólo era legible un 20% de los mensajes interceptados, siendo el análisis de tráfico mucho más útil [30]. Tiltman pudo idear un método para romper este código basado en quebrarlo, ya que pudo darse cuenta de que todos los números en el libro de códigos se podían dividir por tres. Para codificar un mensaje, las palabras del texto en claro se codificaban mediante el libro código, al que se sumaban los números correspondientes de una tabla sumatoria o aditiva, tal y como se puede ver en la siguiente imagen:



(昭式ノ三)

072

	91	50	24	73	56	39	02	15	44	81	54	70
16	14929	35628	80562	60147	88137	93561	21500	58665	97820	17326	56853	01076
85	23183	63151	07541	65326	38003	42353	94004	78478	04047	33017	30748	52211
32	36831	78346	33669	43223	01491	14713	40230	32552	58607	01712	08545	94076
17	31819	48704	11557	81078	90567	25006	84804	67611	40964	47620	97947	17795
98	81321	58431	06431	33724	57592	75934	54976	16316	30250	52377	49357	66013
05	44035	05883	28137	67209	29321	98312	65937	89503	74978	00150	87674	24542
38	53252	04722	58423	82158	76830	49301	39180	77289	20120	72090	15782	03640
95	97453	22039	61220	56431	41787	34320	78103	10196	85468	25594	78566	25939
07	84561	70850	41526	18789	60024	54267	10645	09150	62621	65227	16312	93190
52	02843	83208	74802	03172	15640	26854	02163	92218	13056	84914	64117	11285
46	85513	62153	95276	31374	04282	80618	63245	36922	80083	45706	68807	78053
11	90452	41881	52291	99360	70718	61941	88117	12267	73010	10542	88902	40063
04	13767	23648	12023	48762	52050	12805	49350	28294	07034	37760	20865	56021
72	27364	30867	87101	28450	32180	68543	03300	58470	69311	88487	38189	89513
69	09317	52563	19755	76921	24806	45705	27023	09800	22084	59410	76035	04610

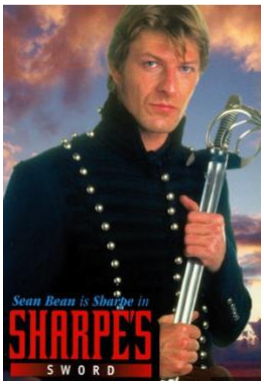
Figura 30. Tabla sumatoria JN25 [27]

La suma se realizaba utilizando el método de suma de Fibonacci o aritmética china, de tal forma que si se sumaban 6+6 el resultado no era 12 sino 2.

Las reseñas criptográficas en la película son pocas, pero se apunta con certeza el cambio de claves en el JN-25, y el poco éxito inicial.

2.6 La espada de Sharpe (1995)

Basada en una novela histórica del autor inglés Bernard Cornwell, forma parte de una serie de TV, ambientada durante las guerras napoleónicas que tuvieron lugar en España a principios del siglo XIX, y que enfrentaron a la alianza anglo-española contra las tropas francesas de Napoleón.



En ella se narra cómo los franceses envían al coronel Leroux a eliminar a un espía al servicio de los ingleses conocido como “El Mirador” y que está suministrando información muy valiosa al ejército inglés, haciéndoles ganar la guerra. El protagonista, Sharpe,

logra capturar a un oficial francés que, aunque en ese momento no lo sabe, es en realidad el coronel Leroux. Este coronel francés tiene en su posesión en el momento de su captura un libro de códigos y una hoja llena de números, que hace pasar por una hoja de facturas, se trata en realidad de un cifrado por libro, o cifrado Ottendorf, en el que el libro usado en este caso es *Cándido* de Voltaire y la hoja llena de números son las posiciones de las letras dentro del libro que el espía, al servicio de Napoleón, le ha enviado; se trata pues de un caso totalmente análogo al caso del apartado 2.4 de "La clave está en Rebeca".

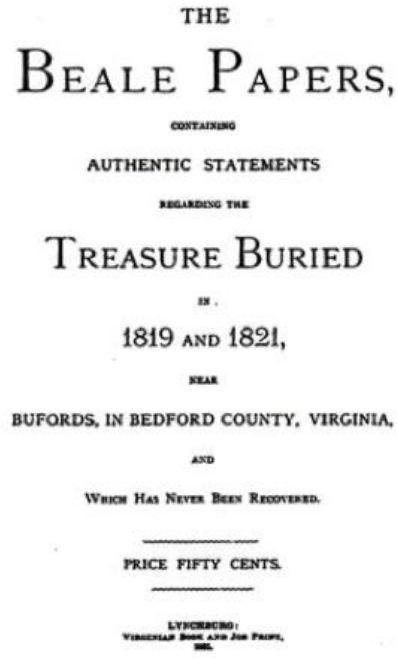
Esto puede verse dentro de la película como se muestra en la siguiente imagen en la que se ve a uno de los protagonistas, Harris, buscar letra por letra en el libro código elegido:

Figura 31. Conteo de letras en "La espada de Sharpe" [31]

De igual forma, en otro momento se puede ver como Harris le explica a otro protagonista, Harper, cómo ha roto el código "You know how the first number is the page, the second number is the line in, the third is the line down and the fourth is the letter in the word" aunque también añade "The clever bugger kept changing the combination" es decir, tanto el espía como el coronel Leroux cambiaban regularmente esta disposición de números, cambiaban continuamente la clave, para que el número de página no fuera siempre en el mismo orden, dificultando así el criptoanálisis. Por lo que parece claro que, de los dos tipos de codificación por libro, o cifrado Ottendorf, que se vieron en el apartado 2.4 se está usando un esquema de codificación letra por letra.

Este cifrado, como ya se ha dejado entrever es de uso muy común en un ambiente bélico ya que logra no llamar la atención, al ser libros de lectura general como Cándido o Rebeca no provocan ningún tipo de sospecha de que se puedan estar usando para mandar mensajes al enemigo, al contrario que lo haría un libro de códigos que provocaría el arresto inmediato de su poseedor.

Quizás entre los más famosos criptogramas relacionados con un cifrado por libro, se encuentren los llamados papeles de Beale [32], cuya historia se remonta a principios del siglo XIX. La historia cuenta que Thomas J. Beale confió a Robert Morriss una caja para que se la guardara en su ausencia, caja que según Beale contenían "papeles de valor y de importancia". Morriss aguardó la llegada de Beale, pero ésta nunca se produjo, finalmente, 23 años más tarde y pensando en que Beale había muerto, Morriss se decidió a abrir la caja en la que encontró una nota escrita en texto claro por Beale y tres hojas encriptadas, llenas de números. En la nota en claro, Beale explicaba su historia en la que él y 28 compañeros más, habían encontrado una mina de oro y proseguía que durante 18 meses habían explotado esta mina, y con el temor a morir sin que este tesoro pasara a sus descendientes habían decidido poner por escrito la localización de este tesoro que habían vuelto a enterrar, a quienes eran sus parientes a los que traspasar dicho tesoro y en qué consistía éste concretamente. Morriss dedicó el resto de su vida a tratar de desencriptar estas hojas si ningún éxito, sintiendo pronta su muerte decidió traspasar el secreto a un amigo que publicó la historia con los tres documentos encriptados, él mismo consiguió descifrar uno de estos papeles, concretamente el que consistía en describir el tesoro enterrado. En la siguiente imagen se puede ver la portada del libro donde publicó estas cifras de Beale:


THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

LYNCHBURG:

Figura 32. Portada de "The Beale Papers"

Este hoja, como las otras dos, contenía 800 números empezaba con la secuencia *115,73,24,807,37,…*Este hombre asumió que los números se referían a las palabras o letras de un libro, es decir, asumió que se encontraba frente a un cifrado por libro con un

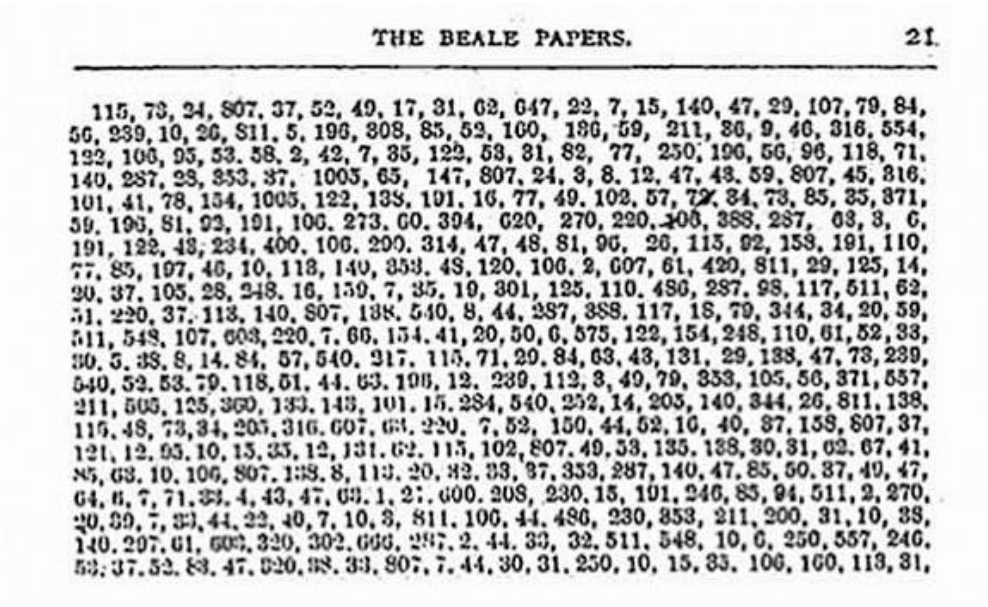
esquema de codificación letra por letra, tal y como se explicó en el apartado 2.4. Para ello utilizó como libro la Declaración de Independencia, que empieza de esta forma:

When(1), in(2) the(3) course(4) of(5) human events it becomes necessary(10) for one people to dissolve the political bands which have(20) connected them with another, and to assume among the powers(30) of the earth, the separate and equal station to which(40) the laws of nature and of nature's God entitle them(50), a decent respect to the opinions of mankind requires that(60) they should declare the causes which impel them to the(70) separation. We hold these truths to be self-evident, and that(80) all men are created equal, that they are endowed by(90) their Creator with certain inalienable rights, that among these are(100) life, liberty and the pursuit of happiness; That to secure(110) these rights, governments are instituted among men…

Por lo que siguiendo con la numeración establecida en la hoja se descifra el siguiente texto:

"I have deposited in the county of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following articles: … The deposit consists of two thousand nine hundred and twenty one pounds of gold and five thousand one hundred pounds of silver; also jewels, obtained in St. Louis in exchange for silver to save transportation … The above is securely packed in iron pots, with iron covers. The vault is roughly lined with stone, and the vessels rest on solid stone, and are covered with others …"

Ahora mismo el valor de tal tesoro rondaría entre los 40 y 50 millones de dólares. Se intentó descifrar también las dos hojas restantes usando la misma la *Declaración de Independencia* pero no hubo éxito. A continuación se muestra la cifra Beale que logró descifrarse y que describía en qué consistía el tesoro.



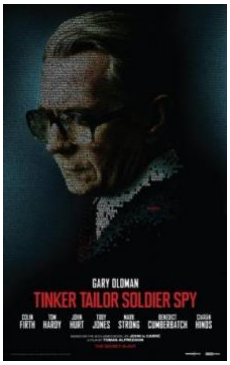
THE BEALE PAPERS. 21.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84,
56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554,
122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71,
140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316,
101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371,
59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6,
191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110,
77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14,
20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62,
51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59,
511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33,
30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239,
540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557,
211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138,
115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37,
121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47,
64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270,
20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38,
140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246,
53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31,

Figura 33. Segunda cifra de Beale

Muchos criptógrafos actuales consideran que esta historia se trata de un bulo y que los papeles de Beale restantes no tienen un texto un texto en claro posible.

2.7. El Topo (2011)



Esta película, ambientada en plena Guerra Fría, se basa en el libro del antiguo espía británico y famoso novelista John Le Carré (seudónimo de David John Moore Cornwell). En ella se narra la búsqueda de un topo infiltrado en la cúpula de los servicios secretos británicos, por parte del protagonista, George Smiley, que también será el protagonista de otras muchas novelas de John Le Carré.

Las películas y novelas basadas en la Guerra Fría son también una fuente importante de sistemas y procedimientos criptográficos, ya que durante este periodo los dos bloques en conflicto invirtieron importantes recursos en ocultar su información al otro bloque.

En la trama de esta película se pude observar el envío y recepción de información mediante el uso de máquinas de cifrado automáticas, alimentadas por corriente eléctrica, como se puede ver en la siguiente imagen a la izquierda:

Figura 34. Máquina cifradora en "El Topo" [33]

Un ejemplo de mensaje que se recibe se puede ver a continuación, compuesto de números en grupos de cinco en cinco, que hay que recordar, es el número de signos que se cuentan como una palabra en el envio de un mensaje por telégrafo y que, por tradición se

transmitirán los criptogramas en grupos de cinco en cinco. Esto se puede ver en la siguiente imagen:

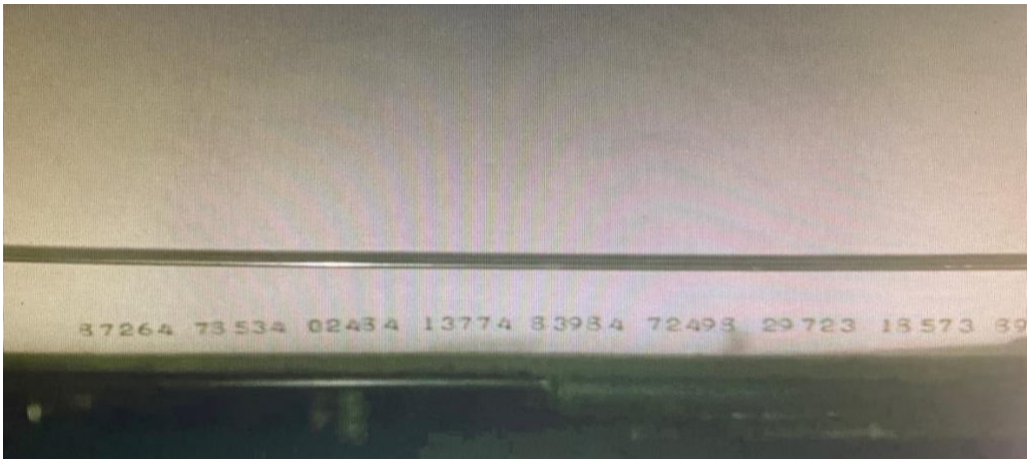


Figura 35. Recepción de información cifrada en "El Topo" [33]

Como ya se ha comentado, los procedimientos que reproducen estos criptógrafos mecánicos están basados en la sustitución polialfabética, debido a su dureza y facilidad de realización mecánica, tal y como se vio en el apartado 2.1 con la máquina Enigma. Los diseños que tienen estas máquinas son múltiples y variados pero todas tienen unas partes obligadas, que son las siguientes [17]:

- Dispositivos para la **introducción de claves**. Se tiene que determinar la posición inicial del mecanismo de cifrado y la ley de movimiento que afecta a las partes móviles, lo que al fin y al cabo constituye el verdadero dispositivo de cifra.

- Dispositivo para la **entrada del texto en claro**, normalmente en forma de teclado, pero también los hay en forma de lector de cinta y dial.

- Dispositivo de **cifrado**, compuesto de piezas móviles, normalmente rotores eléctricos que provocan el desplazamiento variable del alfabeto de sustitución respecto del alfabeto en claro en función de la posición que ocupan en cada momento.

- Dispositivo de **salida del cripto**, ya sea en forma de impresora, perforadora de cinta, ventana con luces etc. Como se puede ver en la anterior Figura 35 el dispositivo de salida es en forma de impresora, para la máquina Enigma era en forma de ventanas, cuando cada una de las ventanas con las letras se iluminaban.

Como es de suponer, la mayor parte de estas máquinas basan su mecanismo de cifrado en un conjunto de ruedas o rotores, montados en un eje común, cada uno de los cuales girará

de forma independiente según una ley de movimiento, tal y como se vio en el apartado 2.1.

Está claro que la 2ª Guerra Mundial conllevó el uso y proliferación del uso de máquinas cifradoras, entre ellas se encontraban la SIGABA y la SIGCUM de origen americano, mientras que del lado alemán se pueden ver la famosa Enigma y la Lorenz SZ40, ésta última mucho más sofisticada que la anterior e invencible a las bombas de Turing, por lo que se llegó a utilizar para cifrar las comunicaciones de Hitler con sus mariscales [2]. Esto supuso un importante aumento de mensajes cifrados contra los que se tuvo que hacer frente con la invención y desarrollo de máquinas automáticas, como la máquina programable Colossus que ayudó a descifrar el código producido por la Lorenz SX40/42.

A continuación se puede ver una imagen de la máquina cifradora conocida como SIGABA, desarrollada por los Estados unidos poco antes de la guerra [36]:

Figura 36. Máquina cifradora SIGABA

Como ya hemos comentado el código producido por la Lorenz SZ40 pudo burlar en un principio el criptoanálisis de los aliados y de las bombas de Turing. Para lograr romper la cifra producida por esta máquina se tuvo que implementar el considerado primer ordenador del mundo, conocido como Colossus, diseñado por el ingeniero británico Tommy Flowers, En la siguiente imagen puede observarse una máquina Lorenz SZ40 sin las cubiertas:

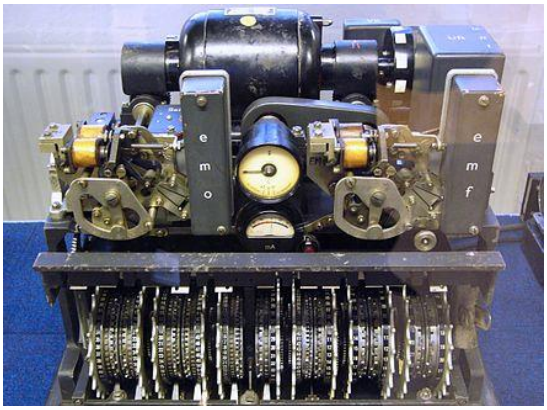


Figura 37. Máquina cifradora Lorenz SZ42. Museo de Bletchley Park

A partir de este hecho, se diseñaron y crearon otras máquinas electromecánicas, tales como la TSEC/KL-7, Fialka M-127 y la Hagelin CX-52, que han permanecido en uso hasta la década de 1980, década en que la digitalización de las comunicaciones irrumpió y provocó el cambio de paradigma de lo analógico a lo digital, acelerando la desaparición de estas máquinas [34]. La Hagelin CX-52, desarrollada por la empresa suiza Crypto AG en 1.952, fue una máquina de tipo mecánico, es decir, no necesitaba alimentación eléctrica, aumentó sobremanera la seguridad de las comunicaciones frente a sus predecesoras, debido a su gran profundidad criptográfica [35], que hace que cuando se eligen de forma adecuada las claves externas, a elegir por el operador, proporciona una fortaleza criptográfica comparable incluso a las conseguidas actualmente. Debido a esto, esta máquina fue comprada por más de 60 países. A continuación se puede ver una imagen de esta máquina:

Figura 38. Máquina cifradora Hagelin CX-52 [35]

No obstante, es opinión de muchos expertos, el dispositivo de encriptamiento más seguro y completo, fue la máquina SECM (Electrical Cipher Machine) Mark II, más conocida como SIGABA. Esta máquina fue desarrollada por Estados Unidos y más concretamente por William Friedman, antes de la guerra pero fue usada durante ésta y hasta la década de 1950 entrada ya la Guerra Fría, su información ha estado clasificada hasta el año 1996, casi cuatro décadas de que fuera retirada de su uso.

SIGABA contaba con un total de 15 rotores, que se pueden dividir entre:

- 5 rotores de control
- 5 rotores de indexación
- 5 rotores de cifrado

Como se ha dicho, se consideraba un dispositivo tan altamente seguro, que fue utilizado para comunicaciones de tipo estratégico, como las comunicaciones efectuadas entre

Churchill y Roosevelt [37], se llegaron a construir más de 10.000 unidades. Se puede decir que funcionaba como la máquina Enigma pero de una forma mucho más inteligente y compleja ya que contenía un total de 15 rotores, en vez de los 3 o 4 rotores que tenía como máximo Enigma; al contrario que ésta, SIGABA no disponía de disco reflector ni tampoco disponía del clavijero frontal, como contrapartida y debido a esta complejidad, SIGABA nunca se utilizó en el campo de batalla.
Dicha complejidad se basaba en el hecho de que el movimiento de sus rotores no se asemejaba a los de otros dispositivos de cifrado. En éstos el movimiento de los rotores se asemejaba a un odómetro, con el primer rotor moviéndose una posición cada vez que se introducía una letra, el siguiente rotor se moviéndose cuando el anterior había completado una vuelta completa y así sucesivamente como se vio en el apartado 2.1. En la máquina SIGABA, el movimiento de los rotores de cifrado, dependía del movimiento de otros dos bancos de rotores, conocidos en su conjunto como *stepping maze*.

Tanto los rotores de cifrado como los de control contaba con 26 pines, representando a las 26 letras del alfabeto, mientras que los rotores de indexación contaban únicamente con 10 pines de entrada. Como se ha recalcado, los rotores de control e indexación controlan el movimiento de los rotores de cifrado. Tanto estos rotores de cifrado como los rotores de control podían ser colocados en una orientación normal o de forma inversa, cambiando así el número de posibles claves. En la siguiente imagen se tiene un esquema del funcionamiento de los rotores en la máquina SIGABA:

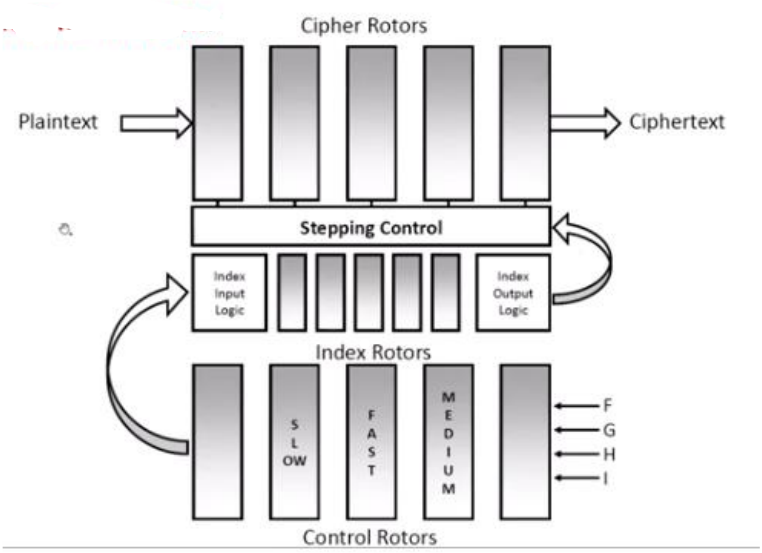


Figura 39. Esquema de funcionamiento de SIGABA [38]

Como se puede ver en la anterior figura, los rotores de control, cada uno de 26 letras, se componían de un rotor de movimiento lento, otro de movimiento rápido, otro de movimiento medio y dos rotores fijos. Los rotores con movimiento giraban de una forma irregular, al contrario que la máquina Enigma, que giraban de forma totalmente regular, dificultando así la ruptura del código, se hace notar también que las entradas de las letras

F,G,H,I siempre tienen corriente y, según se ve, la salida de estos rotores de control eran la entrada a los rotores de indexación.
Se puede ver de forma más clara el funcionamiento de los rotores de control en la siguiente figura, donde se aclaran los contactos de cada uno de los rotores, su entrada y su salida antes de entrar a los rotores de indexación:

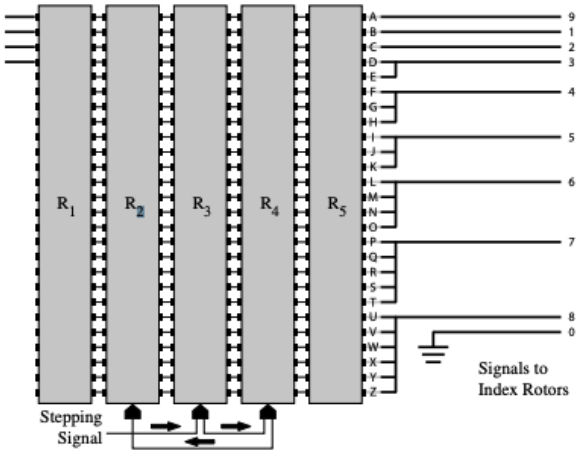


Figura 40. Rotores de control de SIGABA [38]

Como se puede ver en la anterior figura, hay cuatro señales que entrantes al rotor R1 que, como se puede ver en la Figura 40, son las entradas correspondiente a los pines F,G,H,I, estas señales son codificadas por los rotores y son la entrada a los rotores de indexación como se muestra en la figura. Durante la encriptación, tanto R1 como R5 son rotores estacionarios, el R3 rota una posición por cada letra de entrada a la máquina, R4 rota una vez cada 26 letras introducidas, es decir cuando el R1 haya completado una vuelta completa y el rotor R2 rota una vez cada 676 (o 26^2) letras, cuando el rotor R4 haya dado una vuelta completa. Las 26 salidas del banco de rotores de control se muestran en la anterior figura como entradas a los rotores de indexación, estas salidas se adecuarán a las diez entradas posibles al banco de rotores de indexación, por ejemplo, una señal de salida D ó E resultarán una señal de entrada 3 al siguiente banco de rotores, que sólo cuentan con diez pines de entrada y salida.

Estos rotores de indexación constituyen la segunda parte del llamado *stepping maze* y reciben como entrada la salida de los rotores de control, como se mostró en la Figura 41. Como se puede ver cuentan con diez conexiones tanto de entrada como de salida, la salida de estos rotores irán directamente al banco de rotores de cifrado que serán los encargados del cifrado propiamente dicho. En la siguiente figura se puede ver un esquema de estos rotores de indexación:

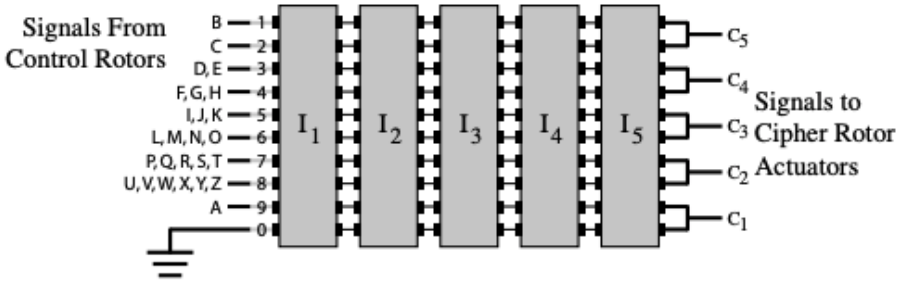


Figura 41. Rotores de indexación de SIGABA [38]

En la anterior figura se muestra la entrada a los rotores de indexación proveniente de los rotores de control y su salida, que serán la entrada a los rotores de cifrado. Estas señales c_1,c_2,c_3,c_4 y c_5 provocarán que uno de los rotores de cifrado se mueva o se quede en estado estacionario según presente corriente o no, es decir, harán de actuadores tal y como se puede ver en la anterior figura.
En la siguiente figura se puede observar el esquema de funcionamiento de los rotores de cifrado en un dispositivo SIGABA y la entrada de los pines c_1,c_2,c_3,c_4 y c_5 a este banco de rotores de cifrado:

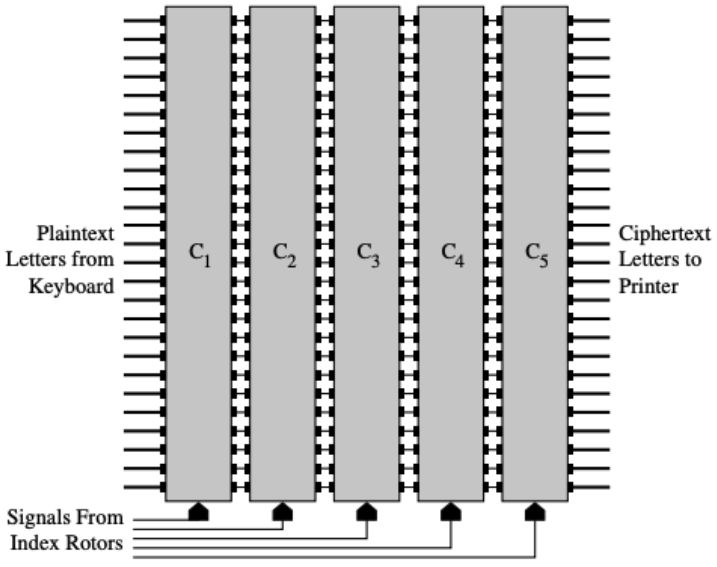


Figura 42. Rotores de cifrado SIGABA [38]

Como también se puede observar en la figura, aparte de la entrada proveniente de los rotores de indexación, que indicarán cuál de los rotores de cifrado se moverá.

Se puede usar el software Cryptool 2, con el módulo de SIGABA, para encriptar y desencriptar texto como se muestra a continuación en la siguiente figura:

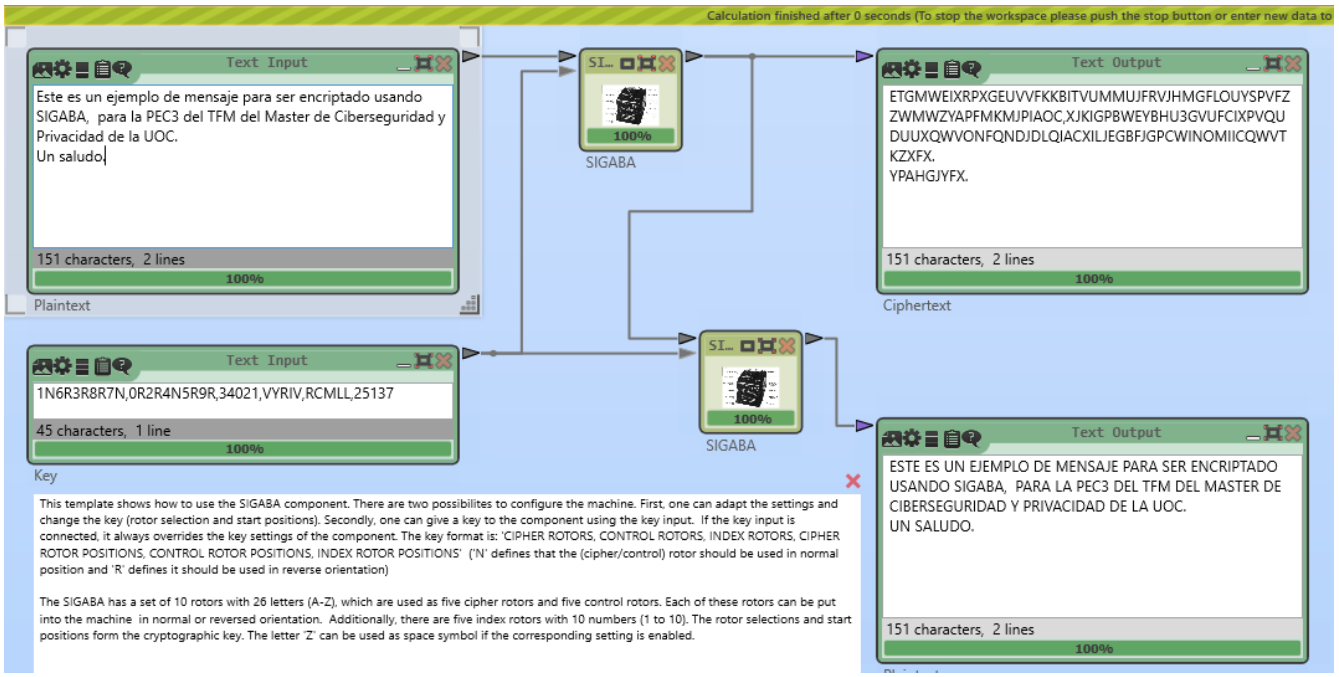


Figura 43. Resultado de encriptación/desencriptación usando SIGABA en Cryptool 2 [37]

En la caja, denominada *Key* de la anterior figura, se puede observar la clave utilizada en este ejemplo para la máquina SIGABA. La clave, según se utiliza en el anterior ejemplo es “CIPHER ROTORS, CONTROL ROTORS, INDEX ROTORS, CIPHER ROTOR POSITIONS, CONTROL ROTOR POSITIONS, INDEX ROTOR POSITIONS. Como se puede observar en la imagen, hay 5 rotores para cada banco de rotores y en cada uno se especifica la posición que deben adoptar, ‘N’ para posición normal y ‘R’ en posición reversa:

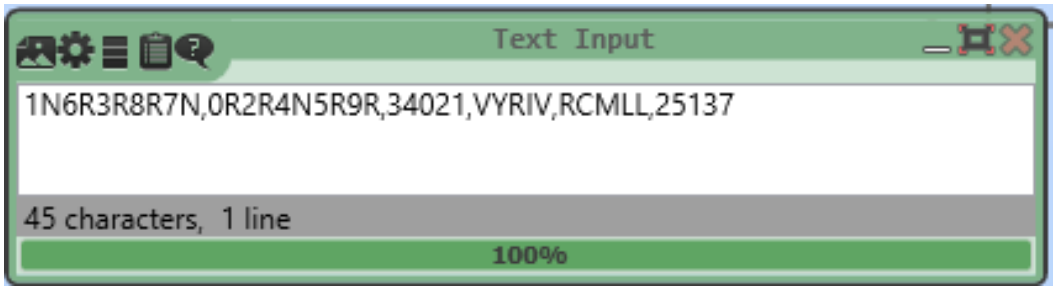
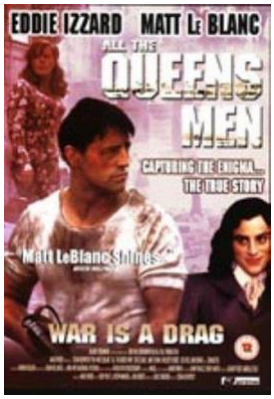


Figura 44. Detalle de claves en SIGABA

2.8 All the Queen's Men (2001)



Esta película narra la historia de un grupo compuesto por un militar americano y varios militares ingleses que durante la 2ª Guerra Mundial tratan de infiltrarse en la fábrica de la máquina Enigma en Berlín, con el objetivo de hacerse con una de estas máquinas.

Se trata de una fábrica en la que solo trabajaban mujeres, por lo tuvieron que infiltrarse vestidos de mujer, con lo que llega a ser una película más cómica que bélica.

Los aportes criptográficos en la película son escasos, sin embargo podemos encontrar varios apuntes de este tipo, cuando la película se centra en la fábrica donde se fabricaban las máquinas Enigma. En particular se pueden observar varios fotogramas que muestran los rotores usados en las máquinas Enigma, como se puede ver en la siguiente imagen.

Figura 45. Detalle de los rotores de una máquina Enigma en All the Queen's men [39]

También se muestra en un momento como los tres rotores de una máquina Enigma son insertados dentro de ella:

Figura 46. Inserción de rotores dentro de una máquina Enigma [39]

Aunque los apuntes criptográficos sean muy escasos, se puede afirmar que los detalles de fabricación de estas máquinas Enigma parecen correctas.

2.9. Desde Rusia con Amor (1963)

Este clásico del cine narra cómo una agente del departamento de criptografía de la embajada rusa en Estambul, se pone en contacto con los servicios secretos británicos para proponer su deserción junto con la máquina codificadora Lektor, dispositivo muy deseado tanto por los servicios secretos americanos como por los ingleses ya que su estudio podría suponer revelar todas las comunicaciones rusas por parte del bloque occidental, siempre y cuando se ponga en contacto con ella el agente secreto James Bond. Esta maniobra es una estratagema por parte de la organización Spectre, ya que de esta forma se harán con la máquina cifradora rusa y se vengaría de la muerte del Dr. No por parte de James Bond.

En la siguiente imagen se puede ver una imagen del dispositivo conocido como Lektor en la película:

Figura 47. Máquina Lektor en "Desde Rusia con amor [40]"

Durante el transcurso de la película esta agente rusa describe la máquina Lektor a James Bond, ya que en una ocasión fue testigo de su reparación, describe que ésta tenía 24 teclas para signos y 16 teclas para cambios de clave, la cinta perforada se introduce en una ranura y el mensaje sale en un rollo de papel, continúa describiendo el mecanismo por dentro comentando que "tenía muchos discos perforados, creo que de cobre, discos de cobre ligeros", por lo que confirma que esta máquina, al igual que la Enigma y la SIGABA usaban del sistema de rotores para su funcionamiento. También se confirma que la interfaz de salida hace uso de un rollo de papel, como se ha comentado en el apartado 2.7, la interfaz de salida de estos dispositivos podrían consistir en una impresora, una perforadora de cinta, como es este caso, o una ventana de luces, como en el caso de Enigma.

Ya se ha comentado la importancia que llegaron a tener los dispositivos cifradores durante la 2ª Guerra Mundial, como ejemplos se tiene la conocida y comentada máquina Enigma por parte de Alemania, la SIGABA por parte de Estados Unidos que también fue utilizada durante parte de la Guerra Fría, pero no se ha comentado ningún dispositivo por parte de la Unión Soviética. La máquina cifradora que destacó desde 1947 hasta 1991 por parte de la URSS, es la denominada Fialka M-125. Este es un dispositivo basado en la máquina Enigma alemana y como tal, se trataba de un dispositivo basado en rotores, usando sustitución polialfabética, pero al contrario que la Enigma, que contaba con 3 o 4 rotores, la máquina rusa llegó a contar con hasta 10 rotores con 30 contactos cada uno [41]. A continuación se puede ver una imagen de este dispositivo:

Figura 48. Fialka M-125 [42] con el detalle de los rotores

Esta máquina pronto se convirtió en el dispositivo criptográfico más utilizado por todos los países afines a la URSS, incluido Cuba. Al igual que la máquina Enigma, se trataba de una máquina electromecánica que con cada introducción de texto en claro provocaba el giro de sus rotores para cambiar el alfabeto de sustitución. Esta máquina se mantuvo en activo hasta principios de 1990 y desapareció junto con la desintegración de la URSS [42] que se encargó de destruir todas las máquinas que pudo, una vez que se fue retirando de todos los países bajo su órbita. A la anterior versión M-125, que se observa en la anterior figura y que estuvo operativa desde 1947 hasta mediada la década de 1960, le sucedió la versión M-123-3M que introducía variantes según el país de uso y que se mantuvo en activo hasta los primeros años de la década de los 90.

Las similitudes con la máquina Enigma hizo que se la bautizara con el sobrenombre de la *Enigma rusa*, aunque también presentaba grandes diferencias respecto a ésta, entre ellas se pueden encontrar las siguientes:

1. Uso de diez rotores en vez de los 3 o 4 que la Enigma podía presentar.
2. Mayor frecuencia de giro de sus rotores.
3. Los rotores adyacentes siempre se mueven en sentido opuesto.
4. Desde 1.978 la conexión entre las ruedas podía ser efectuada en campo.
5. Una letra podía ser codificada por ella misma, algo imposible en la Enigma debido a la presencia de los rotores denominados reflectores.
6. La Fialka M-123 no disponía de un clavijero como tenía la Enigma, para lograr la conexión entre dos letras se hacía uso de tarjetas perforadas.

Estas tarjetas perforadas se introducían a la izquierda de la máquina y comparado con el uso de un clavijero, como en la Enigma, su principal ventaja respecto al clavijero de la Enigma radica en que es mucho menos propenso a errores e incrementa el número de permutaciones posibles lo que la hace mucho más potente desde el punto de vista criptográfico. Todas las tarjetas eran fabricadas en la Unión Soviética y distribuidas a todos sus países satélites, normalmente todas las tarjetas eran eliminadas una vez se usaban por lo que, que se sepa, sólo ha sobrevivido una hasta nuestros días y se muestra en la siguiente imagen:

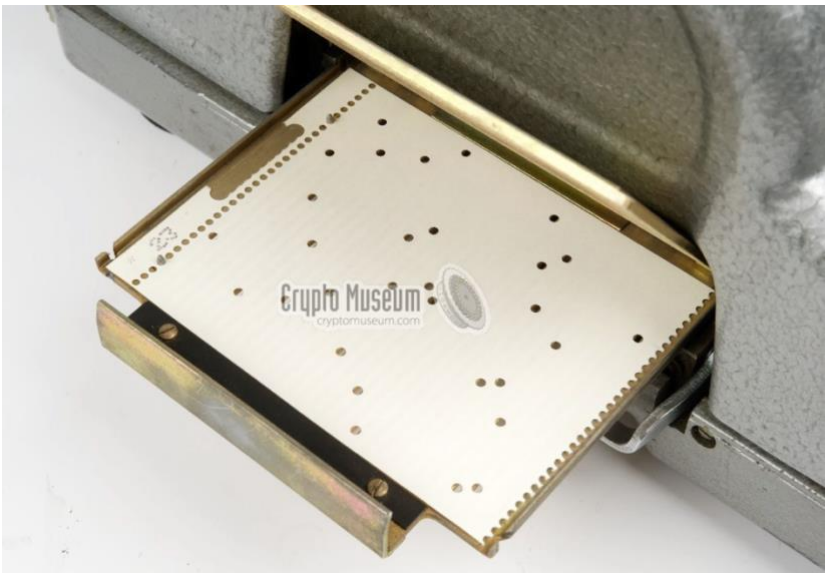


Figura 49. Tarjeta perforada para la Fialka M-125 [42]

En la misma película la agente rusa le comenta a James Bond que "la tarjeta perforada se introduce en una ranura y el mensaje sale en un rollo de papel" por lo que parece probable que se esté describiendo el uso de esta máquina.

Cuando la agente rusa comenta que el mensaje sale en un rollo de papel, está describiendo una de las posibles interfaces de salida que se conocen en este tipo de máquinas, algo que fue ya descrito en el apartado 2.7, cuando se comentó que el mensaje de salida podía salir en un rollo de papel, este es el caso para la Fialka M-123, según se puede ver en la siguiente imagen:

Figura 50. Cinta de papel anexada a una máquina Fialka [43]

Una imagen de los rotores usados por la Fialka M-125, que son diez en su totalidad se puede ver en la siguiente imagen:

Figura 51. Rotores en Fialka M-125 [43]

Como se puede ver en la anterior figura, el número de rotores era de diez para esta máquina, muchos más que los 3 o 4 que llegó a tener Enigma pero aun así, cinco rotores menos que la americana SIGABA.

Los rotores podían ser de dos tipos: fijos y ajustables. En un principio esta máquina fue distribuida con un conjunto de diez rotores fijos, con 30 contactos cada uno a cada lado, a partir de 1978 se reemplazaron por los rotores del tipo denominados como PROTON-2, que eran un conjunto de rotores ajustables. Un esquema de este tipo de rotores puede verse en la siguiente figura de frente, de lado y por la parte de atrás [43]:

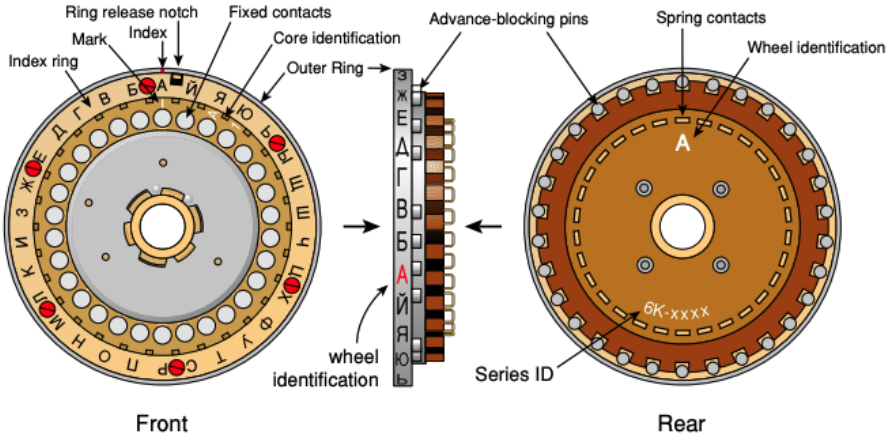


Figura 52. Esquema de rotor ajustable para Fialka M-125 [43]

Cada uno de los rotores distribuidos tenían una serie de conexiones distintas según la serie a la que pertenecían, en el caso de la anterior imagen se puede ver que el rotor pertenece

a la serie 6K, dependiendo de la serie, las conexiones de los contactos en la parte delantera con los contactos en la parte trasera serán distintos.
A continuación se puede observar un ejemplo de encriptación usando esta máquina a través del software Cryptool 2, para lo que se puede utilizar la siguiente configuración de la máquina en este software:

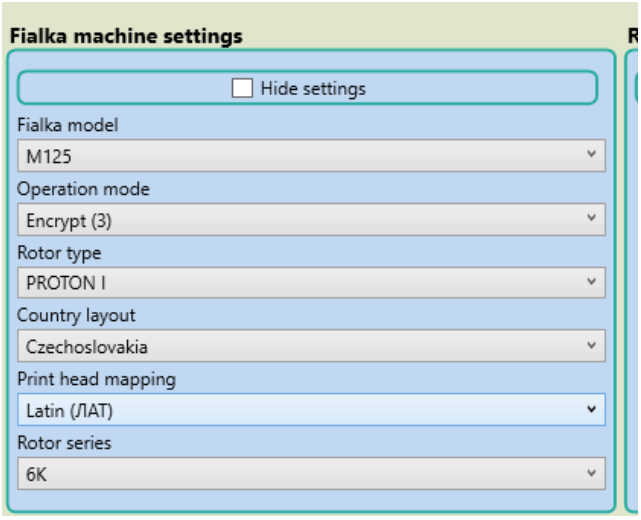


Figura 53. Configuración Fialka M125 Cryptool2

Como se puede ver en la anterior figura se ha configurado los rotores al tipo PROTON1, es decir, rotores fijos antes de 1978, se hace uso de la configuración usada en Checoslovaquia, y el teclado en caracteres latinos y los rotores son de la serie 6K

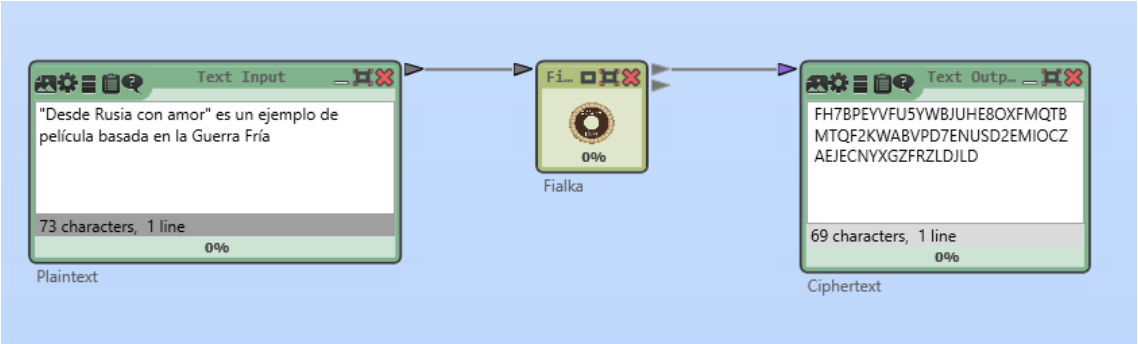


Figura 54. Ejemplo de encriptación en Fialka M125

2.10 El puente de los espías (2015)

Esta película, se basa en hechos reales que tuvieron lugar en 1957, en plena Guerra Fría. En ella se narra la captura de un espía soviético en Nueva York, Rudolf Abel, quien es acusado de enviar mensajes cifrados a la URSS. Interrogado por el FBI se niega a cooperar con los agentes y ser agente doble por lo que es recluido en prisión a la espera de juicio, para lo que se le asigna un abogado de oficio, James Donovan, quien se encargará de dar un juicio justo a Rudolf Abel. A pesar del ambiente de crispación y paranoia que su defensa provoca en la población, provocando incluso ataques a su propia familia, logra conmutar la pena del espía de una segura pena de muerte a prisión durante 30 años. Poco tiempo después un espía americano, Francis Gary Powers, es derribado cuando surcaba el espacio aéreo soviético en un U2, durante una misión de reconocimiento, este espía es condenado por la URSS 10 años de prisión. El abogado James Donovan, gracias al talento demostrado en la defensa de Rudolf Abel, es reclutado por la CIA para lograr este intercambio de prisioneros entre Abel y Powers y al mismo tiempo James Donovan logró que también se liberase al estudiante americano Frederic Pryor, arrestado en Berlín oriental bajo la acusación falsa de espionaje.

Los apuntes criptográficos en la película empiezan cuando el espía soviético abre una moneda para extraer de su interior un mensaje criptografiado como se puede ver en la siguiente imagen:

Figura 55. Ocultación de mensaje dentro de moneda hueca [44]

En la película se adivina un poco el contenido de este mensaje y cómo está formado por grupos de 5 números, por lo que claramente se trata de un mensaje criptografiado, a la vez que se oculta dentro de un objeto de tipo común para que pase desapercibido. Una imagen del mensaje criptografiado puede adivinarse en la siguiente imagen sacada de la película [44]:

Figura 56. Código oculto dentro de moneda en El puente de los espías [44]

Este mismo proceder de ocultar la información dentro de objetos de uso común ha sido ampliamente usada desde tiempos inmemoriales, son lo que se vienen en llamarse dispositivos de ocultación [45] que, como su propio nombre indica, se utilizan para ocultar cosas con el propósito final de mantener el secreto o la seguridad, se pueden usar objetos domésticos de uso común como un libro, una lata de refresco, una vela o incluso, una moneda como es el caso de la película, con la idea de que no se podría esperar que un objeto tan discreto contenga nada de valor. En concreto los libros son posiblemente los dispositivos de ocultación más comunes en uso, ya que se fabrican fácilmente y pueden albergar objetos grandes, en la siguiente imagen se puede observar una radio escondida dentro de un libro, en concreto para ocultarla de los ocupantes alemanes durante la 2ª Guerra Mundial:

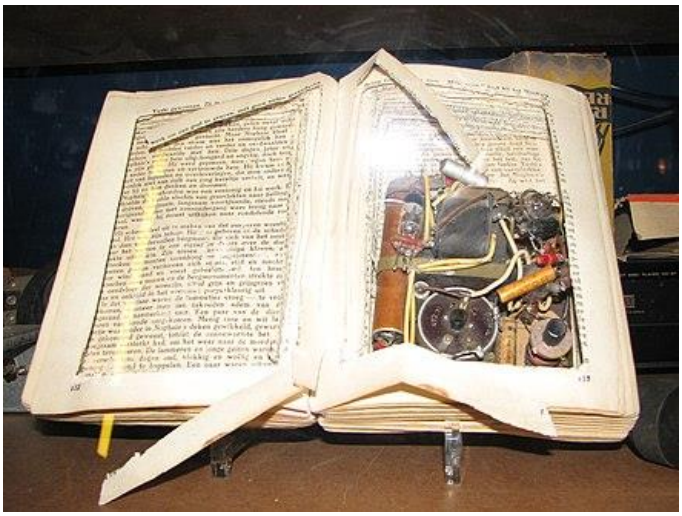


Figura 57. Ocultación de radio en dispositivo de ocultación. [45]

Este mismo caso puede ser visto en otras películas que han formado parte de este trabajo, como es el caso de Rendezvous, que se discutió en el apartado 2.2, como se puede ver en la siguiente imagen sacada de la película:

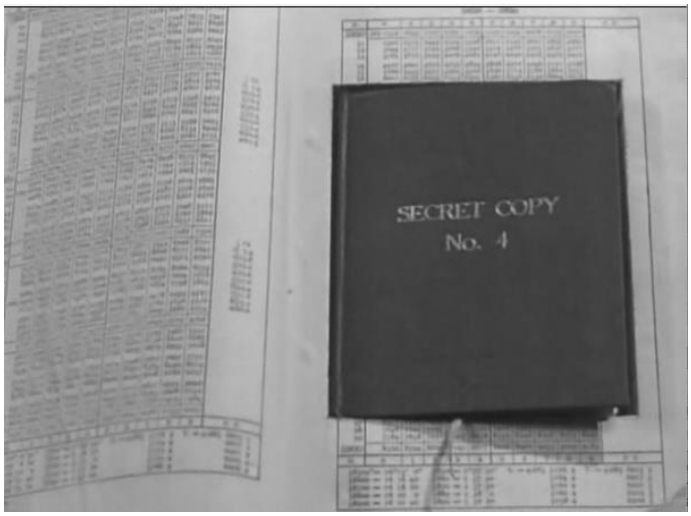


Figura 58 Ocultación de libro de códigos en otro libro en Rendezvous

Durante la Guerra Fría los espías debían de ser dotados de sistemas de cifra fiables y resistentes y a ser posible de tamaño reducido, por lo que las máquinas cifradoras que se han visto en apartados anteriores, como la Fialka M125, quedaban pronto descartados, por lo que se tuvo que volver a sistemas de lápiz y papel que imperaban antes de la 2ª Guerra Mundial.

Esto se puede ver en uno de los casos que llevó el FBI durante estos primeros años de la Guerra Fría, el llamado *Hollow Nickel Case*, fue un caso de investigación que nació a partir del descubrimiento de una moneda de cinco céntimos hueca, por parte de un chico que vendía periódicos, dentro de esta moneda se encontraba un mensaje cifrado que contenía hasta 207 conjuntos de cinco cifras, a continuación se muestra una imagen de la moneda hueca:

Figura 59. Moneda de cinco céntimos hueca [46]

En la siguiente imagen se muestra el mensaje encontrado dentro de esta moneda:

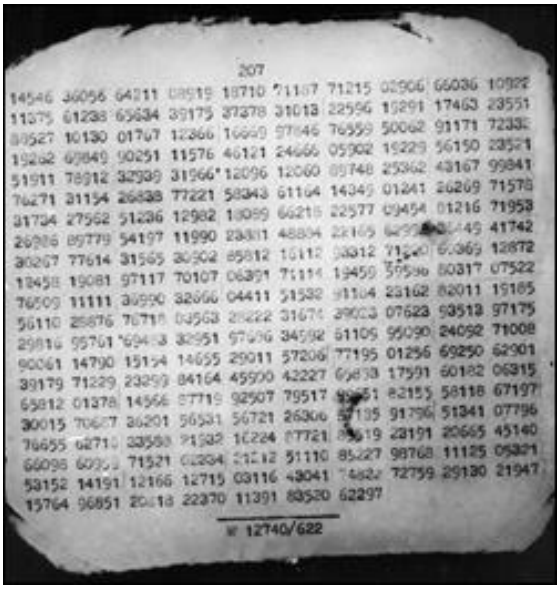


Figura 60. Mensaje cifrado encontrado en el caso de la moneda hueca [46]

El anterior mensaje no pudo ser descifrado puesto que no se conocía la clave, los criptoanalistas del FBI trataron durante cuatro años de romper el cifrado sin éxito alguno. No fue hasta la deserción del agente del KGB Reino Häyhänen, cuando fue posible descifrar el anterior mensaje, que resultó ser un mensaje personal del KGB dándole la bienvenida a los Estados Unidos y dándole instrucciones para su correcto asentamiento y evitar ser descubierto. La deserción de Häyhänen conllevó romper este cifrado y el arresto de varios agentes soviéticos en los Estados Unidos.

Este sistema de cifrado tomó el nombre de cifrado VIC y fue usado por todos los espías soviéticos durante toda la Guerra Fría, toma su nombre del apodo que tomó Reino Häyhänen durante su estancia en los Estados Unidos, espiando para la URSS, VICTOR. Su rendición y deserción a los americanos provocó la caída de su compañero Rudolf Abel al mismo tiempo que también provocó la ruptura de este cifrado.

Este cifrado es considerado como la más compleja modificación de los cifrados de la familia de los Nihilistas rusos [47] y es considerado como uno de los cifrados más fuertes que se pueden ser usados de forma manual sin el uso de ordenadores.

La cifra de los Nihilistas Rusos consistía en una variante de la tabla de Polibio que opera con una contraseña [2], a la que se añade otra segunda clave cuyo cifrado se obtiene por la misma tabla. Como se sabe, la construcción de una tabla de Polibio es un procedimiento para escribir las letras como pares de números, por ejemplo si se crea la siguiente tabla de Polibio con la contraseña PECTRES quedaría la siguiente tabla:

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

Tabla 6. Tabla de Polibio para la cifra de los Nihilistas Rusos [2]

En la anterior tabla, primeramente se rellena con la contraseña elegida PECTRES, sin repetir letras, y se rellena la tabla con la restantes letras del alfabeto. Seguidamente se escoge otra contraseña, por ejemplo MASTERUOC, que cifraremos a partir de la anterior tabla, por lo que se obtendría : 42 22 21 14 12 15 51 44 13.

A continuación se creará una nueva tabla, en la que en la primera fila se pondrá el mensaje en claro, debajo el mismo mensaje pero ya cifrado, y en la tercera fila la contraseña cifrada repitiéndola hasta el final de la fila si fuera el caso, por lo que si queremos enviar AGENTE DESCUBIERTO se construirá la siguiente tabla:

A	G	E	N	T	E	D	E	S	C	U	B	I	E	R	T	O
22	31	12	43	14	12	24	12	21	13	51	23	33	12	15	14	44
42	22	21	14	12	15	51	44	13	42	22	21	14	12	15	51	44
64	53	33	57	26	27	75	56	34	55	73	44	47	24	30	65	88

Tabla 7. Construcción de cifrado de Nihilistas Rusos

El cifrado final es consecuencia de la suma de la 2ª y 3ª línea por lo que el mensaje cifrado será: **64533 35726 27755 63455 73444 72430 6588**, para descifrar el mensaje al receptor tan sólo le bastaría realizar la operación inversa, es decir, restar el cifrado de la clave para

obtener el primer mensaje codificado que podrá decodificar con la tabla de Polibio creada que también conocerá.

Como se ha dicho, el cifrado VIC es una evolución del anterior cifrado descrito, pero mucho más evolucionado, éste usa también de una tabla que cambiará el texto en claro en números, como en el caso anterior, pero para el cifrado VIC esta tabla recibe el nombre de tablero demediado que, a diferencia de la tabla de Polibio utilizada en la cifra de los Nihilistas rusos que cifraba con un par de dígitos cada letra, no cifra cara carácter con el mismo número de dígitos, lo que hará mucho más difícil el criptoanálisis.

A modo de explicación, un tablero demediado o, también encontrado en la literatura como tablero de ajedrez a horcajadas, es una forma de obtener una sustitución del texto claro del mensaje en dígitos, de forma similar a un tablero de Polibio, pero obteniendo al mismo tiempo un fraccionamiento y una relativa compresión de los datos. El tablero que se empleaba para la cifra VIC era similar a este [47]:

	0	1	2	3	4	5	6	7	8	9
	E	T		A	O	N		R	I	S
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	/	U	V	W	X	Y	Z	.

Tabla 8. Tablero demediado para cifrado VIC [47]

Como se ve la primera fila está formada por dígitos simples, de igual forma que la Tabla 6 que mostraba una tabla de Polibio. La segunda fila será rellanada con las letras más comunes del idioma inglés, dejando dos huecos y como se ve no tiene ningún número asignado a su izquierda. Las dos filas restantes que sí que tienen números asignados correspondientes a las columnas en las que se han dejado huecos en blanco, se emplean para rellenar con las siguientes letras. Esta cifra se operaba en inglés con sólo 26 letras, por lo que se completaban los dos huecos restantes con los signos convenidos entre emisor y receptor, en este caso un ‘/’ y un ‘.’ .

Para convertir un texto empleando el anterior tablero se sustituirá cada letra por su coordenada en el anterior tablero, tal y como se hizo ya con la cifra de los Nihilistas rusos, quedaría entonces la siguiente tabla, con el mismo texto en claro a transmitir AGENTE DESCUBIERTO:

A	G	E	N	T	E	D	E	S	C	U	B	I	E	R	T	O
3	24	0	5	1	0	22	0	9	21	63	20	8	0	7	1	4

Tabla 9. Codificado de texto en claro mediante tablero demediado

Como se ve, gracias a la inserción de una fila con las letras más comunes en una determinada lengua se logra una mayor compresión de la información a enviar.

A continuación, se sumaría la secuencia anterior la secuencia pseudoaleatoria generada a través de elegir una fecha en particular, o un número propio de cada agente, digamos que se elige la fecha de nacimiento del agente, 20179:

	3	2	4	0	5	1	0	2	2	0	9	2	1	6	3	2	0	8	0	7	1	4
+	2	0	1	7	9	2	0	1	7	9	2	0	1	7	9	2	0	1	7	9	2	0
=	5	2	5	7	4	3	0	3	9	9	1	2	2	3	2	4	0	9	7	6	3	4

Tabla 10. Suma de texto codificado con secuencia pseudoaleatoria

Y la cifra que se mandaría al receptor sería 52574 30399 12232 40976 34.

En algunas ocasiones es una buena idea cambiar estos dígitos de nuevo a letras, usando la misma tabla que se usó durante el proceso de encriptación, con lo que quedaría de la siguiente forma:

5	25	7	4	3	0	3	9	9	1	22	3	24	0	9	7	63	4
N	H	R	O	A	E	A	S	S	T	D	A	G	E	S	R	U	O

Tabla 11. Cambio a caracteres en cifrado VIC usando el mismo tablero demediado

Este cifrado está bien diseñado y proporciona muy buena seguridad, hace que el criptoanálisis lleve mucho tiempo, al hacer uso de las frecuencias de las letras en cada

idioma. Se encuentran muchas modificaciones de este cifrado, los cambios pueden ser efectuados en el tablero demediado, cambiando el orden de las letras, algunas celdas pueden ser dejadas vacías, lo que hará el criptoanálisis mucho más complicado. El cifrado recibido puede ser modificado a su vez usando a su vez algoritmos de transposición, lo que hará incluso mucho más potente el cifrado.

Se concluye que los pocos datos que aparecen en la película al respecto de esta cifra parecen correctos.

3. Conclusiones finales

Si bien en la lista de películas que se han usado en el apartado 1.8, las hay que realizan un análisis mucho más certero de los procedimientos criptográficos que en otras, se resume a continuación cada una de ellas:

1. En “Descifrando Enigma”[15] , la explicación del procedimiento usado para romper el cifrado de la máquina Enigma está muy bien desarrollado al explicar cómo el uso de palabras repetidas o predecibles ayudaron a que las Bombas construidas entre polacos e ingleses pudieran romper el cifrado de la máquina Enigma.

2. Se puede afirmar que “Rendezvous” [16] es la película donde mejor se explican los procedimientos criptográficos usados, convirtiendo a la criptografía como personaje principal de la película y la propia trama en personaje secundario. Sobre todo explicando el cifrado de sustitución y su criptoanálisis mediante el uso del análisis de frecuencias de las letras en un determinado idioma y con la ayuda de discos de Alberti para lograrlo.

3. Si bien la explicación del código navajo que se hace en “Windtalkers” [21] es escasa, en ningún momento se comete ningún error, como ya se apuntó en el apartado 2.3. La otra película donde aparece el uso de un código usado durante la 2ª Guerra Mundial puede verse en “Midway” [28], aunque en este caso el código JN-25, utilizado por los japoneses, es nombrado mucho más por encima dentro de la película y sin ningún tipo de explicación, al contrario que ocurre en “Windtalkers”.

4. Tanto en “La clave está en Rebeca” [22] como en “La espada de Sharpe” [31] se refleja el uso de un cifrado por libro o código Ottendorf, sistema muy utilizado en situaciones bélicas por espías dentro de territorio enemigo, debido principalmente a su baja detectabilidad. Se tiene que destacar que la metodología en sí está mucho mejor explicada en “La espada de Sharpe”, ya que en “La clave está en Rebeca”, únicamente se ve contar palabras al espía alemán y hacer uso del libro usado para la codificación, sin ningún tipo de explicación adicional de este código.

5. En la película de “El Topo” [33] se muestra por primera vez el uso de una máquina cifradora, aunque la película no explica en ningún momento ningún detalle sobre la máquina en sí. Este tipo de dispositivos nacidos a partir de la 2ª Guerra mundial fueron muy usados durante toda la Guerra Fría y en fechas posteriores. Como se ha mencionado basaban su cifrado en un cifrado por sustitución polialfabética, mediante el uso de discos rotadores, como la máquina Enigma.

6. Se ha incluido en el trabajo la película “All the Queen’s Men” [39], que aunque su trama tiene lugar durante la 2ª Guerra Mundial y tiene como objetivo la captura de una máquina Enigma, llega a ser una película más cómica que bélica. Los únicos apuntes a reseñar en la película son cuando se muestra la fábrica de la máquina Enigma, y cuando enseña la instalación de los discos rotadores dentro de una de estas máquinas.

7. En “Desde Rusia con Amor” [40] la criptógrafa rusa describe a James Bond, la máquina Lektor, máquina cifradora usada por los soviéticos, pareciendo que describe una verdadera máquina usada por el bloque comunista durante la Guerra Fría, la Fialka M-125. Este apartado es usado para describir esta máquina cifradora usada por la URSS, conocida como la Enigma rusa.

8. En “El puente de los espías” se muestra muy por encima como espías soviéticos se pasaban mensajes dentro de territorio americano, escondidos incluso dentro de monedas de curso legal como representa la película, en ésta también se puede ver un fragmento del mensaje escondido dentro de ella. En el apartado se explica un poco más acerca del caso *Hollow Nickel Case*, que llevó a descubrir estos mensajes, aunque no pudieran ser descifrados hasta la deserción del principal espía soviético dentro de territorio americano, Reino Häyhänen, y que llevó a la caída de Rudolf Abel, y del descifrado del conocido cifrado VIC, usado por todos los espías soviéticos en territorio americano.

Como puede verse, todas las películas analizadas en mayor o menor grado, hacen un uso correcto de los procedimientos criptográficos que describen, por lo que se puede responder al objetivo buscado en este Trabajo Fin de Máster destacando que en todas ellas se ha hecho un buen trabajo de documentación y se ajustan a sistemas que fueron o son usados en la vida real.

3.1 Trabajo Futuro

Se pueden realizar varias líneas de estudio a partir del presente trabajo. Como se puede ver todos los sistemas criptográficos descritos, basan su funcionamiento en la criptografía considerada como clásica, por lo que un nuevo desarrollo podría basarse en películas que usan de sistemas criptográficos más actuales, como criptografía de clave simétrica, asimétrica, certificados digitales, uso del blockchain con aplicación en el uso de monedas virtuales etc.

4. Glosario

Para una mayor claridad de conceptos, se expone a continuación un glosario de términos usados a lo largo del trabajo [51]:

- **Cifrado o cifra:** Transformación de una información (texto claro) en otra ininteligible (texto cifrado) según un procedimiento y usando una clave determinados que pretende que sólo quien conozca dicho procedimiento y clave puede acceder al texto claro.

- **Clave:** Cada uno de los factores de un procedimiento de cifrado que permiten cambiar el resultado de la aplicación del mismo sin modificar su naturaleza. Esto es, sin cambiar ninguna de las operaciones que deben realizarse para cifrar.

- **Código:** Sistema en el que grupos arbitrarios de cifras, letras o símbolos representan a unidades de texto claro de longitud fija o variable. Puede ser público, que no aporta seguridad en la comunicación como el código Morse, o secreto que sí aporta seguridad, como el código navajo. El código secreto constituye en sí un método de cifra.

- **Codificar:** Convertir un texto claro en su equivalente (también claro) utilizando un código público.

- **Criptograma:** Fragmento de mensaje cifrado, y cuyo significado es ininteligible hasta que es descifrado.

- **Criptoanálisis:** Pasos y operaciones orientadas a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado y/o la clave.

- **Criptología:** Ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Comprende la cifra y el criptoanálisis.

- **Criptografía:** Rama de la cifra que trata de la información escrita.

- **Descifrar:** Transformar un texto cifrado en el claro equivalente, conociendo el procedimiento y la clave de descifrado.

- **Decodificar:** Convertir una información en su equivalente claro utilizando un código público.

- **Descriptar:** Resultado positivo de la acción de criptoanálisis.

- **Esteganografía:** Procedimientos encaminados a ocultar la existencia de un mensaje, como en el caso del uso de tintas invisibles.

- **Libro de claves:** Documento que recoge las claves que serán utilizadas por la red de cifra durante un tiempo determinado.

- **Procedimiento de cifrado:** Cada uno de los métodos específicos de cifrado dentro de un determinado método. Se puede entender como el conjunto de las manipulaciones a que se somete un texto claro para cifrarlo.

- **Red de cifra:** Asociación de elementos físicos y humanos con un criptosistema y con las normas de funcionamiento, considerados como un conjunto único que interviene en un proceso de cifrado.

- **Sistema de cifrado**: Principio general adoptado para cifrar. Puede ser por sustitución, por transposición o mixto.

- **Sustitución:** Sistema de cifrado que consiste en reemplazar los caracteres del texto claro por una representación distinta de la original. Puede ser simple, de representación única, cuando a cada carácter del texto claro le corresponde sólo un posible carácter del texto cifrado y viceversa, o de representación múltiple si le pueden corresponder varios pero a cada uno del texto cifrado sólo una del claro o polialfabética, si a cada carácter del texto cifrado le pueden corresponder varios del texto claro y viceversa.

- **Texto cifrado o cripto:** Texto resultante de aplicar un procedimiento de cifrado a un texto claro.

- **Transposición o permutación:** Sistema de cifrado que consiste en alterar el orden de los caracteres del texto claro.

5. Bibliografía

[1] Susana Mataix, “Las mujeres y la ciencia. Mujeres en la Criptografía”, 100cias@uned. Facultad de Ciencias., pp 1-2. Nº 3 (2010).

[2] Carlos Taranilla, “Criptografía. Los lenguajes secretos a lo largo de la historia”. Ed: Guadalmazán (2021).

[3] J.G. Carmona “Tratado de criptografía con aplicación especial al Ejército”. Ministerio de Defensa (2011)

[4] sarnek Marcin. (2014). "Cryptographer-Magician" and other modes of presence of cryptography in contemporary American cinema. W: W. Kalaga, M. Mazurek, M. Sarnek (red.)"Camouflage : secrecy and exposure in literary and cultural studies" (S. 166-179). Katowice : Wydawnictwo.

[5] Ramesh et al (2019) “The Portrayal of Great Mathematicians in Movies: A review” International Journal of Recent Technology and Engineering (IJRTE) Volume 7 Issue -5C pp 182-185

[6] Hernández Encinas, Luis (2016) *“¿Qué sabemos de la criptografía?”* Madrid. CSIC

[7] Musgrave, Erica (2016) *“Breaking the Enigma Code”* Mathematics Senior Seminar. Saint Mary’s College of California. Recuperado a partir de: http://math.stmarys-ca.edu/wp-content/uploads/2017/07/Erica-Musgrave.pdf>

[8] Singh, Simon (1999) *“Los códigos secretos”* Editorial: Debate

[9] “Ruptura del cifrado Enigma de cuatro rotores” (2006) [en línea] [Consultado el 1 de noviembre de 2022]< https://unaaldia.hispasec.com/2006/03/ruptura-del-cifrado-enigma-de-cuatro-rotores.html>

[10] “La Máquina Enigma” (2020) [en línea] [Consultado el 2 de noviembre de 2022] <https://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm>

[11] “158,962,555,217,826,360,000 (Enigma Machine) – Numberphile [enlinea] [<https://www.youtube.com/watch?v=G2_Q9FoD-oQ> [Consultado el 1 de noviembre de 2022]

[12] “Luz Desencriptada” (2018) [en línea] [Consultado el 5 de noviembre de 2022] < https://elanartista.com.ar/2018/06/29/cuerpo-alan-mathison-turing-padre-la-informatica/>

[13] “Bombe” [en línea] [Consultado el 5 de noviembre de 2022] https://en.wikipedia.org/wiki/Bombeb

[14] Ateneo 304. Alan Turing y el descifrado de mensajes de Enigma en la II Guerra Mundial [en línea] [Consultado el 5 de noviembre de 2022] https://www.youtube.com/watch?v=LzcL7p1GlkU

[15]Tyldum, Morten "Descifrando Enigma" [Film] United Kingdom (2014)

[16] Howard, William "Rendezvous" [Film] USA, (1935)

[17] "Criptología Clásica". Centro Criptológico Nacional (2022)

[18] "Criptografía-Tintas Simpáticas" (2022) [en línea] [Consultado el 5 de noviembre de 2022]< https://prezi.com/q6xt3buvvhhq/criptografia-tintas-simpaticas/?frame=f4806a866da7c88bb65cd3e16615baf1f57fb81f>

[19] "CIA Desclassifies Documents from World War I"(2011) [en linea] [Consultado el 6 de noviembre de 2022]< https://fas.org/blogs/secrecy/2011/04/cia_wwi/>

[20] Macrakis,K & Sweeder Ryan. D (2012.) "Invisible Ink Revealed: Concept, Contex and Chemical Principles of Cold War Writing" Journal of Chemical Education.

[21] Woo, John "Windtalkers" [Film] USA (2002)

[22] Hemmints, David "The Key to Rebecca" [Film] USA (1985)

[23] The Book Cipher Explained- Encription & Decryption Using a Book [en linea] [Consultado el 7 de noviembre de 2022]< https://www.youtube.com/watch?v=JyTDwbzhcx0>

[24] "Create your own Codebook Cipher as Used in The Zimmermann Telegram" (2020) [en linea] [Consultado el 7 de noviembre de 2022] https://www.youtube.com/watch?v=2AyXPSZU4uY

[25] Morales-Luna, G (2016) "Sobre el Telegrama Zimmerman" [White paper] Centro de Investigación y Estudios Avanzados del IPN. Departamento de Computación. http://delta.cs.cinvestav.mx/~gmorales/16Zimm/zimm.pdf

[26] "Como detector un ciberataque" (2022) [en línea] [Consultado el 18 de noviembre de 2022]< https://encyclopedia.kaspersky.es/knowledge/how-to-detect-a-hacker-attack/>

[27] "Código Naval Japonés JN-25" (2020) [en línea] [Consultado el 18 de noviembre de 2022] <https://www.exordio.com/1939-1945/militaris/espionaje/jn-25.html>

[28] Smight , Jack "Midway" [Film] USA (1976)

[29] Ahmed, M et al (2016) “A survey or a network anomaly detection techniques” Journal of Network and Computer Applications, Volume 60 , pp 19-31 https://www.sciencedirect.com/science/article/pii/S1084804515002891

[30] “Códigos navales japoneses” (2019) [en linea] [Consultado el 19 de noviembre de 2022] < https://hmong.es/wiki/JN-25>

[31] Clegg,Tom, “Sharpe’s Sword” [TV Show] United Kingdom (1995)

[32] “The Beale Treasure Ciphers” (1999) [en linea] [Consultado el 22 de noviembre de 2022] https://simonsingh.net/media/articles/maths-and-science/the-beale-treasure-ciphers/

[33] Alfredson, T “Tinker Tailor Soldier Spy” [Film] UK (2011)

[34] “Cipher Machines and Cryptology” (2022) [en linea] [Consultado el 26 de noviembre de 2022] https://www.ciphermachinesandcryptology.com/

[35] “Hagelin C-52 and CX-52 Cipher Machines” (2022) [en linea] https://www.ciphermachinesandcryptology.com/en/c52tech.htm

[36] “SIGABA (ECM)” (2010) [en linea] [Consultado del 27 de noviembre de 2022]< https://www.lasegundaguerra.com/viewtopic.php?t=13988>

[37] “La máquina de cifrado SIGABA de EE.UU: un dispositivo de cifrado increíble” (2021) [en línea] [Consultado el 27 de noviembre de 2022]< https://www.youtube.com/watch?v=ITOmFP1oG0c>

[38] Lee, Michael (2003) “Cryptanalysis of the SIGABA” University of California. Santa Barbara https://ucsb.curby.net/broadcast/thesis/thesis.pdf

[39] Ruzowitzky,S “All the Queen’s Men” [Film] Alemania (2001)

[40] Young, T “From Russia With Love” [Film] UK (1963)

[41] “Cryptojourney” (2017) [en linea] [Consultado el 6 de diciembre de 2022] https://github.com/EdOverflow/cryptojourney-content/blob/master/cryptojourney.md

[42] “Fialka M-125, USSR rotor-based cipher machine” (2008) [en linea] [Consultado el 6 de diciembre de 2022] https://www.cryptomuseum.com/crypto/fialka/

[43] Reavons P & Simons M “Fialka M-123. Detailed description of the Russian Fialka cipher machines” (2005) < https://www.cryptomuseum.com/pub/files/Fialka_200.pdf>

[44] Spielberg, S “Bridge of Spies” [Film] USA (2015)

[45] “Dispositivos de ocultación” (2020) [en línea][Consultado el 7 de diciembre de 2022]< https://hmong.es/wiki/Trap_(car)>

[46] “Hollow Nickel Case” (2022) [en línea] [Consultado el 7 de diciembre de 2022]< https://en.wikipedia.org/wiki/Hollow_Nickel_Case>

[47] “VIC Cipher. Polyalphabetic Substitution Cipher” (2022)< http://www.crypto-it.net/eng/simple/vic.html#:~:text=The%20VIC%20cipher%20uses%20a,sending%20to%20the%20second%20party).>

[48] “Criptografía Histórica- La cifra Vic” [en línea] (2005) [Consultado el 7 diciembre de 2022]< https://www.ugr.es/~aquiran/cripto/enigma/boletin_enigma_38.htm#3>

[49] “Cifrado VIC” [en línea](2010) [Consultado el 7 de diciembre de 2022]< https://hmong.es/wiki/VIC_cipher>

[50] “Cifra VIC” [en línea] (2020) [Consultado el 7 de diciembre de 2022]< https://es.wikipedia.org/wiki/Cifra_VIC#El_tablero_demediado>

[51] “Glosario de términos de Criptología” (3ª Edición) Centro Superior de Información de la Defensa. Ministerio de Defensa.

[52] “Descifrando Enigma (2014-Morten Tyldum)” [Consultado el 5 de noviembre de 2022] <“https://www.youtube.com/watch?v=JS4k00Jj4z0>

6. Anexos

Se debe mencionar que junto a la memoria y presentación del presente trabajo se entregarán lo programas implementados en el programa gratuito Cryptool2 que se han mostrado en el presente trabajo.