CRIPTOGRAFÍA Y CINE: Criptografía en el cine belico

Carlos Domínguez Boiza
Master en Ciberseguridad y Privacidad

Indice

Contexto y justificación

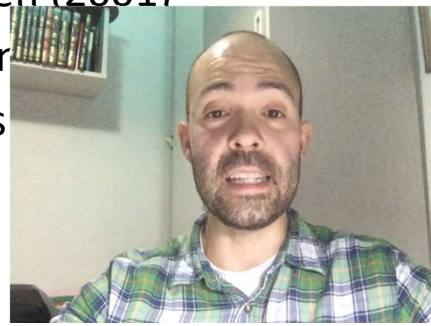
- La criptografía ha sido considerada un arte desde la antigüedad
- Gran papel de los conflictos bélicos en los avances tecnológicos.
- El cine representa la importancia de la criptografía en el devenir de las naciones.

Objetivos del trabajo y enfoque y método seguido

- El principal **objetivo** del trabajo es determinar si los procedimientos criptográficos que estas películas reflejan se ajustan a la realidad o no.
- Visionado de la lista de películas
- Descripción de los procedimientos criptográficos utilizados
- Comparativa con diversos métodos empleados en la realidad

Lista de películas a examinar:

- The Imitation Game (2014)
- Rendezvous (1935)
- Windtalkers (2002)
- La clave está en Rebeca (1985)
- La batalla de Midway (1976)
- La espada de Sharpe (1995)
- El topo (2011)
- All the Queen's Men (2001)
- Desde Rusia con ar
- El puente de los es



The imitation Game (2014)

- Lentitud en las transmisiones hasta la 2ª Guerra Mundial por uso de telegrafía.
- Adopción de transmisión radio lo que llevó a un aumento importante en el número de mensajes intercambiados.
- Necesidad de una mayor protección, se descarta el uso de códigos de sustitución monoalfabética y se obliga el uso de máquinas de rotores que desarrollan un cifrado por sustitución polialfabético inmunes al criptoanálisis por análisis de frecuencias.
- Es un ejemplo claro de que la criptografía puede ca una guerra y por lo tanto del futuro de las naciones

MÁQUINAS DE ROTORES: MÁQUINA ENIGMA

- CIFRADO POR SUSTITUCIÓN POLIALFABÉTICA.
- A MAYOR NÚMERO DE DISCOS MAYOR COMPLEJIDAD DE CIFRADO.

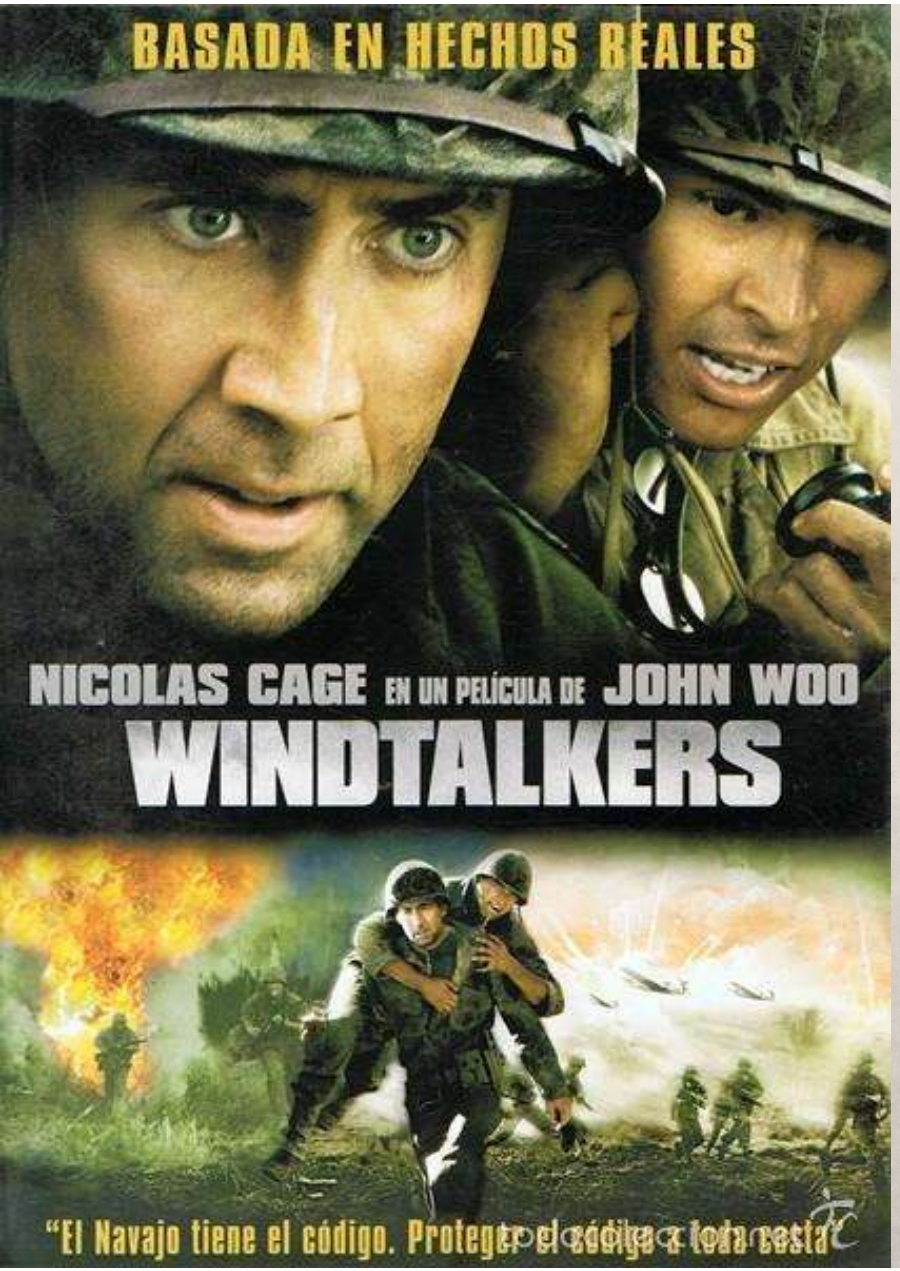
Descifrando Enigma

- Bomba: construcción de máquina electromecánica que usaba la fuerza bruta

- Método de la criba, intuir que unas palabras formarían parte del texto en claro para romper el cifrado.

Rendezvous(1935)

- Uso de criptografía durante la 1ª Guerra Mundial, criptografía de “lápiz y papel”.
- Datos transmitidos por telegrafía, uso de libros de códigos para descodificar el mensaje recibido.
- Uso de tinta invisible como método esteganográfico.
- Criptoanálisis por análisis de frecuencias usados para quebrar códigos de sustitución monoalfabéticas.
- Utilización de discos de Alberti para el análisis de frecuencias.
- El uso de los procedimientos criptográficos y c representados en la película son fiel reflejo de vida real en aquellos momentos.



Windtalkers (2002)

- Uso de código basado en el lenguaje navajo para codificar las comunicaciones del ejército americano durante la contienda.
- Este lenguaje no tiene conexión con ninguna lengua europea o asiática lo que dificulta la decodificación.
- Se creó un alfabeto concreto, viéndose de gran utilizad ya que el alfabeto navajo simplificaba mucho las frases.
- Problema en que muchos términos modernos no existían en este lenguaje por lo que tuvo que crearse un nuevo léxico.
- La película muestra momentos en el que se explica este código a los operadores encargados de las transmisiones.
- Se trata de uno de los pocos códigos que jamás fue enemigo.

La clave está en Rebeca (1985)

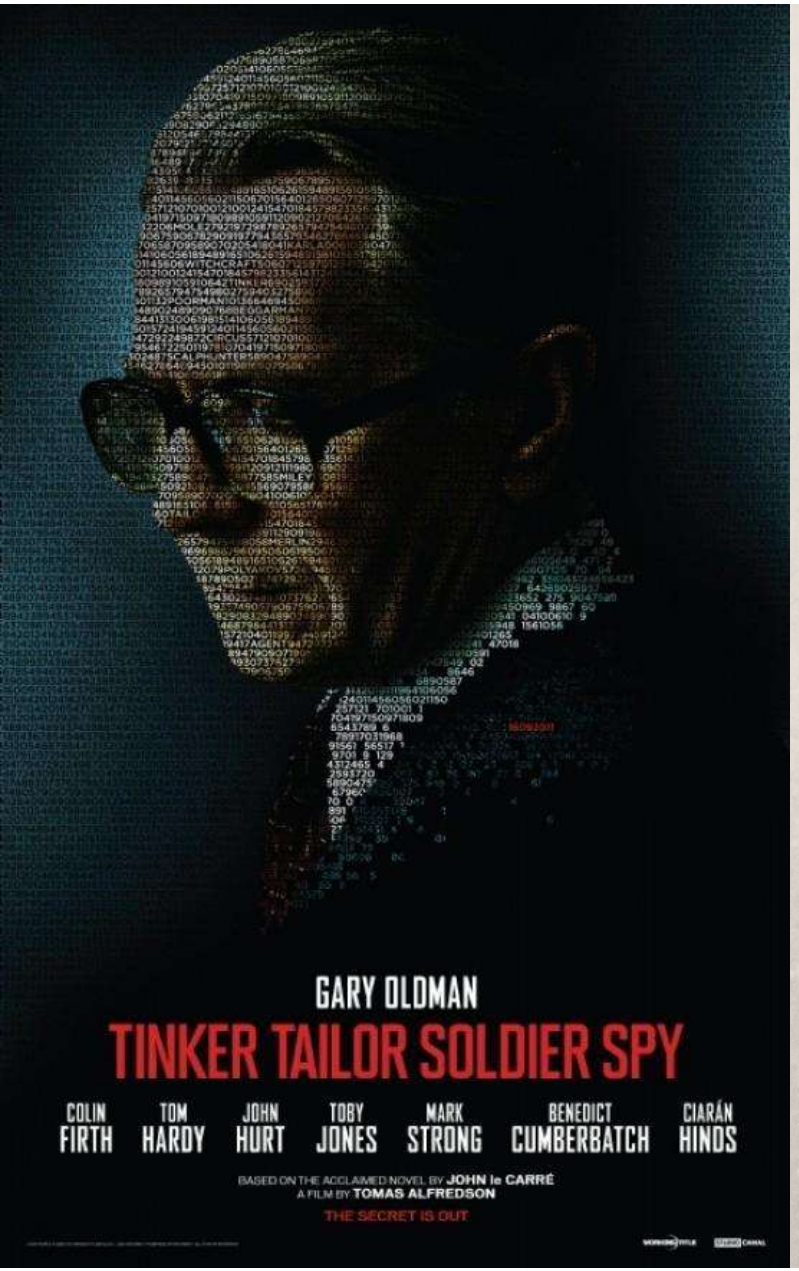
- Uso de codificación por libro o cifrado Ottendorf, el libro utilizado en la película y que da nombre a la misma es Rebeca.
- Codificación letra por letra o por palabra completa.
- Necesidad de que tanto emisor como receptor sean poseedores del mismo libro y de la misma edición del mismo.
- Muy usado por espías dentro de territorio enemigo debido a su baja detectabilidad.

La batalla de Midway (1976)

- Código naval JN-25 usado por los japoneses pudo ser descifrado.
- Utilización de un diccionario de 33.333 letras, palabras y frases asignadas a un número de cinco dígitos.
- Para las palabras no incluidas dentro del diccionario se empleaba el silabario kana japonés.
- John Tiltman junto con Alan Turing idearon un método para romper este código.
- Otro ejemplo claro de que la criptografía puede ca
de las naciones

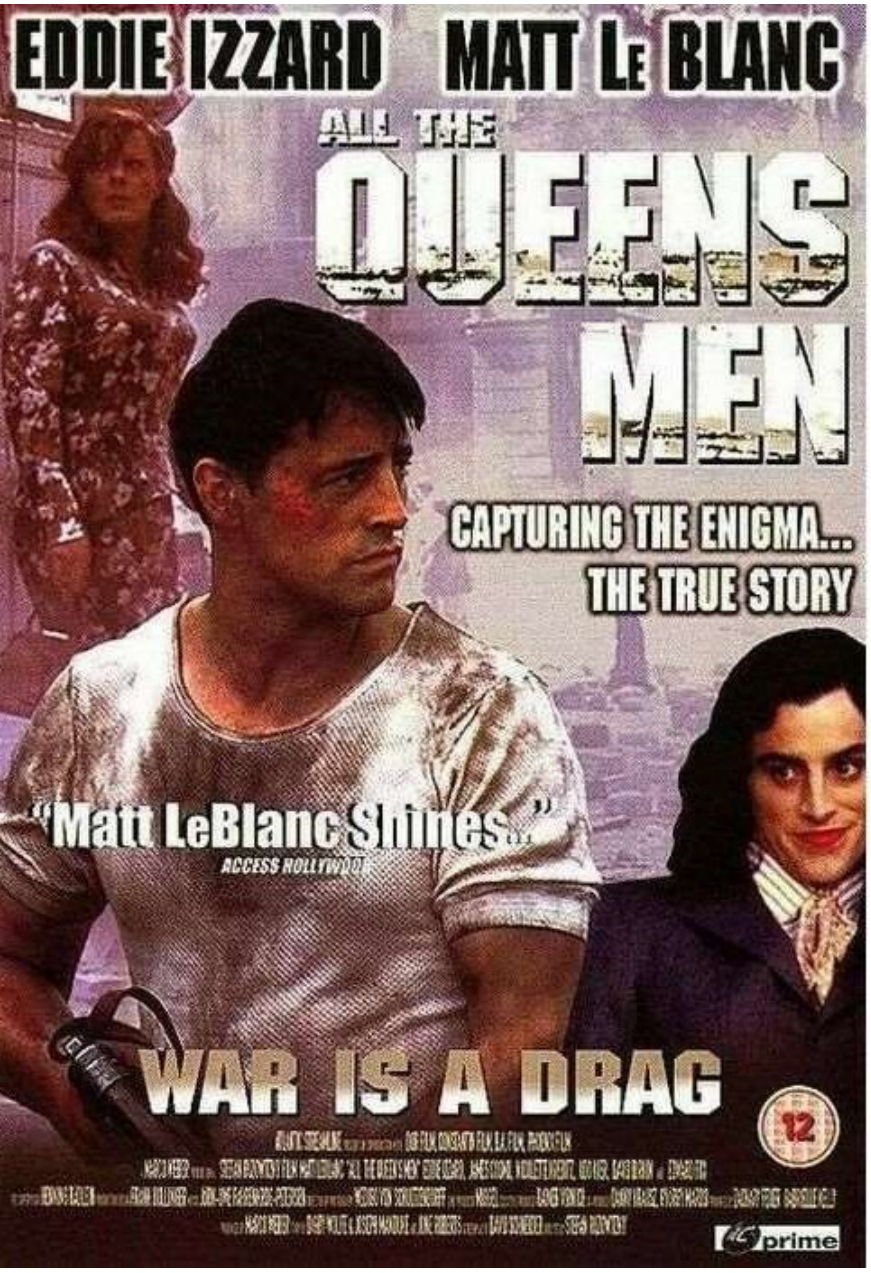
La espada de Sharpe (1995)

- Codificación por libro o cifrado Ottendorf
- Esquema de codificación letra por letra.
- Otro ejemplo más de que este cifrado es uno de los más usados por espías dentro de territorio enemigo.



El Topo (2011)

- Se representa el uso de maquinas cifradoras alimentadas por corriente eléctrica.
- Cifrado por sustitución polialfabética.
- Uso de rotores en todas las máquinas cifradoras utilizadas.
- SIGABA: maquina cifradora con 15 rotores.



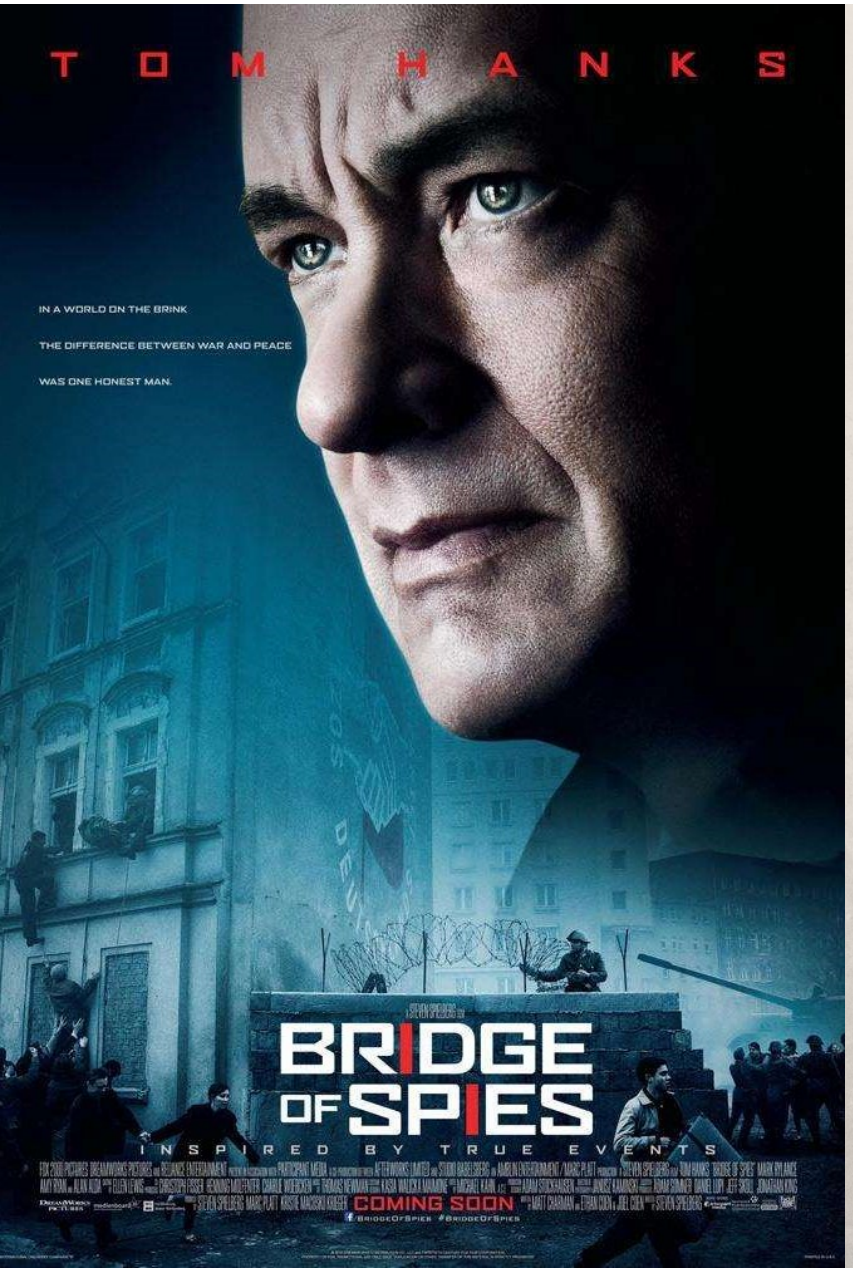
All the Queen's Men(2001)

- Película de tipo más cómica que bélica.

- Se representa la forma de la instalar los rotores dentro de una máquina Enigma.

Desde Rusia con amor (1963)

- El objetivo es hacer con una máquina cifradora rusa conocida como Lektor, máquina cifradora soviética.
- Según descripciones de la agente soviética se trata de una máquina con muchos discos perforados.
- Se presenta en el trabajo la máquina cifradora Fialka M-125 utilizada por todo el bloque soviético durante la Guerra Fria, que presenta unas características similares a la película.



El puente de los espias (2015)

- Red de espías soviéticos en los EE.UU, caso de *Hollow Niquel Case*, mensaje cifrado dentro de moneda hueca.
- Dispositivos de ocultación, en los que ocultar objetos importantes.
- El cifrado utilizado por todos los espias soviéticos es el denominado código VIC.
- Se considera la más compleja modificación de los cifrados de la familia de los Nihilistas rusos.

CONCLUSIONES

Como puede verse, todas las películas analizadas realizan un buen trabajo de documentación , por lo que se puede afirmar que todos los procedimientos criptográficos que representan se ajustan a sistemas que fueron o son usados en la vida real.

Lineas de trabajo futuras:

Seria interesante realizar un estudio desde la perspectiva de la criptografía moderna.


The End