INFORME ENIGMA

Alumnos: Luis Lazo, Gabino (71028058X)

Sánchez San Blas, Héctor (70901148Z)

Asignatura: Teoría de códigos y teoría de la información

Índice

No se encontraron entradas de tabla de contenido.

# Introducción

En este documento se pretender explicar el funcionamiento y los componentes de la máquina enigma que se ha llevado a cabo para la asignatura de Teoría de Códigos y Teoría de la Información del grado en Ingeniería Informática de la Universidad de Salamanca. Ha de tenerse en cuenta que el programa realizado supone una simulación de la máquina Enigma utilizada por los alemanes en la Segunda Guerra Mundial pero con algunos cambios propios aunque la base sigue siendo la misma. Tomando como ejemplo los datos recopilados de la Enigma militar M3 aunque algo más limitada, en el presente documento se van a explicar cómo se han llevado a cabo los distintos elementos que componen la máquina y su funcionamiento.

# Plugboard

Este mecanismo se compone de un panel con distintas entradas que están unidas entre sí a través de cables, de esta forma lo que se logra es que, cuando un impulso llega por una de esas entrada, se transmite por su conexión para generar una salida distinta.

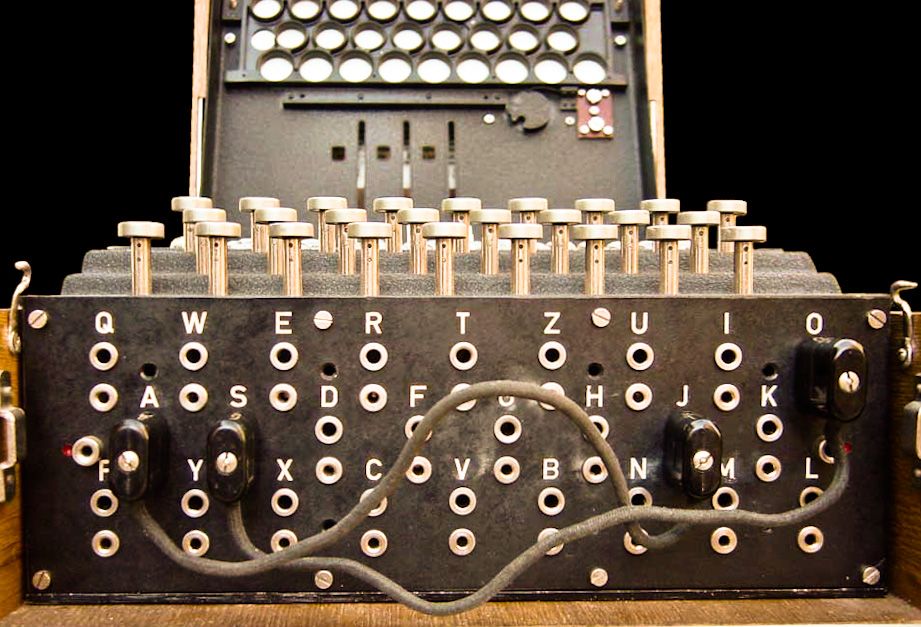


Imagen tomada de la página Pinterest para el plugboard

De esta forma lo que tenemos son pares de palabras para los cuales una determinada entrada de una letra se transformará en la salida según la correspondencia de estas parejas. Un ejemplo de la correspondencia utilizada para el plugboard es la siguiente:



Imagen tomada de la página https://www.cryptool.org/en/cto-ciphers/enigma

Teniendo en cuenta este ejemplo, si en el plugboard se tuviese como entrada la letra ‘A’ obtendríamos como salida la letra ‘D’. En la implementación llevada a cabo, se deja al usuario escoger dichas correspondencias.

# Rotores

La máquina Enigma implementada utilizada tres rotores para encriptar y su funcionamiento es similar al de los de la máquina utilizada. En la realidad, teniendo en cuenta el modelo M3 de Enigma, existen 8 tipos de rotores aunque en la implementación llevada a cabo solo se disponen de 3 (en futuros cambios con disponibilidad de tiempo se podrían añadir más tipos y más rotores a utilizar). Cada rotor posee un anillo interno que hace contacto con otro anillo que genera la salida y, por tanto, la cambia respecto a la entrada. La salida de un rotor está conectada con la entrada del siguiente elemento. El funcionamiento interno del rotor es el siguiente:

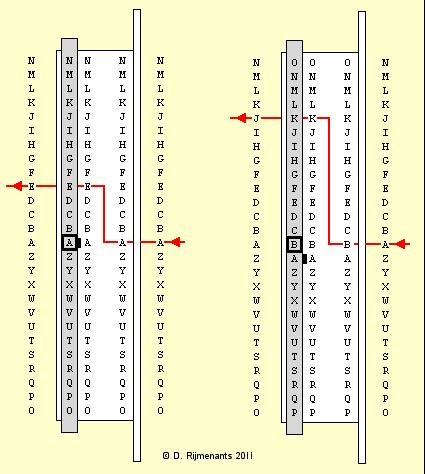


Imagen tomada de la página http://users.telenet.be/d.rijmenants/en/enigmatech.htm#wiringdiagram

En la implementación llevada a cabo, dos arrays de salidas se han tenido en cuenta de modo que se simule el funcionamiento de los anillos internos del rotor. Las correspondencias de cada tipo de rotor es la siguiente:



Imagen correspondencias tipos del primer anillo de la página https://www.codesandciphers.org.uk/enigma/rotorspec.htm

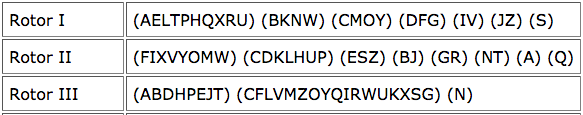


Imagen correspondencia tipos segundo anillo de la página https://www.codesandciphers.org.uk/enigma/rotorspec.htm

Como se puede observar en la imagen, para una entrada ‘A’ en el rotor de tipo I obtenemos una salida ‘E’ del primer anillo que al pasar por el segundo se transforma en una ‘P’. Esta implementación tiene alguna variación respecto al original en cuanto a las correspondencias del segundo anillo.

Cabe destacar que, cuando una letra es encriptada, el rotor rota una posición de forma que las correspondencias entre letras cambian.

# Reflector

El reflector tiene un comportamiento muy similar al del plugboard. Este elemento coge una señal de entrada transformándola otra distinta de salida realizando el proceso contrario al recorrido hasta ahora. Estas correspondencias se llevan a cabo de la misma forma que sucede con el plugboard. Ha de tenerse en cuenta que existen varios tipos de reflectores, sin embargo, en la implementación solo uno fijo se ha incluido de forma que no puede cambiarse el tipo (en futuros cambios con más disponibilidad de tiempo sería posible añadir los otros tipos y permitir el cambio entre ellos). La correspondencia utilizada dentro de la implementación para llevar a cabo este reflector (que se corresponde con el tipo) es el siguiente:



Imagen sacada de correspondencias reflector tipo B de la página https://www.codesandciphers.org.uk/enigma/rotorspec.htm

Como se puede observar, si introducimos la letra ‘A’ la salida obtenida sería la letra ‘Y’.

# Funcionamiento

El funcionamiento completo de la máquina Enigma, la cual se ha implementado, es la siguiente:

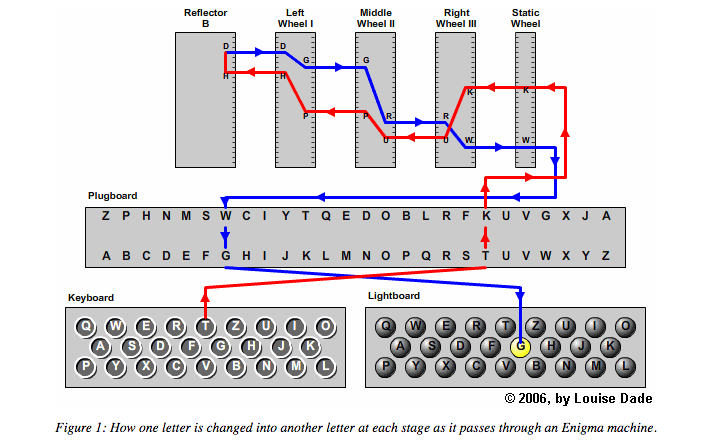


Imagen del funcionamiento completo de la página http://enigma.louisedade.co.uk/howitworks.html

Tal y como se puede observar, cuando introducimos una letra a través del teclado, la señal viaja a través del plugboard transformando dicha entrada en otra distinta, esta señal de salida del plugboard viaja hasta la entrada del primero rotor pasando por cada uno de los rotores disponibles generando cada uno salidas distintas hasta llegar al reflector. En el reflector se introduce la letra generada por la salida del último rotor y se transforma en otra distinta según las correspondencias mostradas antes, la salida del reflector va a realizar el viaje contrario que el realizado por la letra original pasando desde la salida cada rotor hacia la entrada (que internamente cambiará dicha letra). Por tanto, la letra del reflector pasará desde el último rotor pasando por cada uno de los rotores en orden inverso hasta pasar por el primer rotor. La letra obtenida a través de estos cambios en los rotores se introducirá en el plugboard que cambiará de nuevo la letra obteniendo la salida final que proporciona Enigma.

El código correspondiente a la encriptación directa es el siguiente:

//TODO código encriptación

El código correspondiente a la encriptación inversa es el siguiente:

//TODO código inverso

Una vez se ha encriptado una letra, el primer rotor rota una posición. Cuando uno de los rotores llega a su límite en rotaciones, la siguiente vez envía una señal parea que rote una posición el rotor inmediato a él. Es entonces cuando el primer rotor vuelve a iniciar sus rotaciones. Este proceso se repite en todos los rotores del sistema. El código correspondiente a esta parte es el siguiente:

//TODO código rotar

De esta forma, logramos que cambiar las posibilidades obtenidas de forma que el número de posibilidades que obtenemos con los tres rotores es de 26 x 26 x 26= 17576 posibilidades de caminos que puede tomar una letra. Además, como el tipo de los rotores puede cambiar de orden, por ejemplo tipo I, tipo II y tipo III, pero en otro caso podría ser tipo II, tipo I y tipo III, entonces, tenemos distintas posibilidades según la colocación de los rotores, en nuestro caso, como poseemos tres tipos de rotores, nuestras posibilidades de colocación son 3 x 2 x 1 = 6 posibilidades de colocación. Si estas las tenemos en cuenta con lo anteriormente calculado obtenemos que finalmente las posibilidades de caminos que puede tomar una letra son 17576 x 6 = 105456 posibilidades.

A lo anterior se puede añadir los intercambios realizados en el plugboard y en el reflector, teniendo en cuenta las distintas posibilidades. Puesto que nuestro reflector es fijo no lo tendremos en cuenta, pero investigando un poco, los matemáticos resolvieron el número de posibles maneras de conectar el plugboard obteniendo 150,738,274,937,250. Si añadimos a las posibilidades anteriores las del plugboard obtenemos que los caminos posibles ahora son de 15,896,255,521,782,636,000 posibilidades.

Finalemente, decir que la aplicación correspondiente a la encriptación en Enigma es biyectiva, es decir, si se conocen las posiciones y colocaciones iniciales de los elementos de un determinado mensaje encriptado, al introducir dicho mensaje obtenemos el mensaje desencriptado. Este es el motivo por los cual los nazis tenían cuidado de que, al transportar la clave de encriptación (que se corresponde con lo mencionado anteriormente) tenían un mecanismo que destruyese el contenido de dicha clave si era conseguido por los enemigos debido a que la clave de encriptación es a su vez la clave de desencriptación.

Cabe destacar que la implementación llevada a cabo es una representación del sistema descrito a lo largo de este documento de forma que su interfaz se presupone sencilla de utilizar.

# Referencias

<http://enigma.louisedade.co.uk/howitworks.html>

<http://users.telenet.be/d.rijmenants/en/enigmatech.htm#wiringdiagram>

<https://hackaday.com/2017/08/22/the-enigma-enigma-how-the-enigma-machine-worked/>

<https://www.codesandciphers.org.uk/enigma/rotorspec.htm>

<https://www.cryptool.org/en/cto-ciphers/enigma>

<https://www.cryptomuseum.com/crypto/enigma/m3/index.htm>

<https://plus.maths.org/content/exploring-enigma>

<https://learncryptography.com/history/the-enigma-machine>