Informe de Laboratorio - Máquina Enigma

Victor Ponce Pinedo
Universidad Nacional de Ingeniería,
Facultad de Ciencias,
e-mail: victor.ponce.p@uni.pe

Edson Nicks Lázaro Camasca
Universidad Nacional de Ingeniería,
Facultad de Ciencias,
e-mail: elazaroc@uni.pe

Edwin Edy Condori Cornejo
Universidad Nacional de Ingeniería,
Facultad de Ciencias,
e-mail: edwin.condori@uni.pe

Angela Serrano Sánchez
Universidad Nacional de Ingeniería,
Facultad de Ciencias,
e-mail: aserranos@uni.pe

Curso:

CC003 Tópicos Especiales de Ciencia de la Computación 3
Laboratorio Máquina Enigma

Abstract

Desde la aparición de internet la criptografía ha tenido grandes avances, debido a la cantidad inmensa de tráfico y a que los usuarios deben sentirse seguros de que su información sea confidencial, para ello se implementaron diversos métodos criptográficos dentro de la red. Sin embargo, la criptografía se ha desarrollado durante siglos y a jugado un papel muy importante durante los conflictos, y una de las épocas que cobró gran importancia fue la segunda guerra mundial, donde los alemanes usaban la máquina enigma para encriptar sus mensajes de los lugares a los que se iba atacar.

En este trabajo, se ha desarrollado una demo de la máquina enigma implementada en el lenguaje python con el paradigma orientado a objetos (POO), usando estructuras básicas como listas para modelar los rotores y conexiones de la máquina enigma, para la interfaz gráfica se usó la librería nativa de python llamada tkinter. Además, se implementó una mayor complejidad de encriptación, agregando más de 3 rotores y la posibilidad de poder establecer el orden de estas.

Keywords: Maquina Enigma, Demo, Python, POO, Tkinter.

Índice general

1 Introducción

La máquina enigma es una de las máquinas de cifrado más conocidas hechas por el hombre. Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso. La historia de Enigma empieza alrededor de 1915, con la invención de la máquina de cifrado basada en rotores. En el presente informe implementamos una maquina enigma haciendo uso de la programación.

2 Fundamento Teórico

2.1 Historia

2.1.1 Inicios

La historia de Enigma empieza alrededor de 1915, con la invención de la máquina de cifrado basada en rotores. Como es usual en la historia la máquina a rotores fue inventada más o menos simultáneamente en diferentes partes del mundo. Fue patentada en 1918 por la empresa alemana Scherbius & Ritter, cofundada por Arthur Scherbius, quien había comprado la patente de un inventor neerlandés, y después de varios años de mejoras, la primera máquina se puso a la venta en 1923 para un uso comercial. En 1926, la Armada alemana la adoptó para uso militar.

2.1.2 Guerra civil española

Durante la Guerra Civil española, el bando sublevado dispuso de al menos veinte máquinas Enigma que le permitieron al general Franco mantener una comunicación secreta y permanente con sus generales. Las diez primeras fueron vendidas por los nazis al bando sublevado en noviembre de 1936 cuando el avance franquista se detuvo a las puertas de Madrid. Sin embargo, no se trataba del modelo más avanzado (era el D de la gama comercial) ya que a los alemanes les preocupaba que alguna de ellas pudiera caer en manos de los soviéticos, que apoyaban a los republicanos, o de los servicios secretos británicos desplegados en España. El encargado del adiestramiento de los militares que iban a utilizarla fue el comandante Antonio Sarmiento —miembro del Estado Mayor y jefe de la Oficina de Escuchas y Descifrado del Cuartel General del Generalísimo—, quien en un informe redactado en Salamanca en noviembre de 1936 afirmaba: ≪Para dar una idea del grado de seguridad que se consigue con estas máquinas basta decir que el número de combinaciones posibles de acordar se eleva a la fabulosa cifra de 1.252.962.387.456≫. A principios de 1937 se compraron diez máquinas más del mismo modelo. Actualmente una de las máquinas forma parte de la colección estable del Museo Histórico Militar de Sevilla. La máquina data de diciembre de 1938, cuando recaló en Sevilla, asignada al Ejército del Sur. Posteriormente, en julio de 1939, pasó al Estado Mayor de la Segunda Región Militar en Sevilla.

2.1.3 Segunda guerra mundial

Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso. Sin embargo, gracias a las investigaciones llevadas a cabo por los servicios de inteligencia polacos, quienes instruyeron a su vez a los servicios franceses e ingleses en el sistema de cifrado, fue finalmente descubierto y la lectura de la información que contenían los mensajes supuestamente protegidos es considerada como una de las causas de haber podido concluir la Segunda Guerra Mundial al menos dos años antes de lo que habría acontecido sin su descifrado. A pesar de tener algunas debilidades criptográficas, el descifrado también se facilitó por fallos de procedimientos y uso por parte de los operadores alemanes, como el no desarrollar modificaciones continuas en el cifrado, además de la captura, por parte de los Aliados de tablas de descifrado y las propias máquinas.

2.1.4 Post guerra

El hecho de que el cifrado de Enigma había sido roto durante la guerra permaneció en secreto hasta finales de los años '60. Las importantes contribuciones al esfuerzo de la guerra de muchas grandes personas no fueron hechas públicas, y no pudieron compartir su parte de la gloria, pese a que su participación fue probablemente

una de las razones principales por las que los Aliados ganaran la guerra tan rápidamente como lo hicieron. Finalmente, la historia salió a la luz.

Tras el fin de la guerra, los británicos y estadounidenses vendieron las máquinas Enigma sobrantes a muchos países alrededor del mundo, que se mantuvieron en la creencia de la seguridad de ésta. Su información no era tan segura como ellos pensaban, lo que, por supuesto, fue la razón de que británicos y norteamericanos pusieran a su disposición las máquinas.

En 1967, David Kahn publicó su libro The Codebreakers, que describe la captura de la máquina Enigma Naval del U-505 en 1945. Comentó que en aquel momento ya se podían leer los mensajes, necesitando para ello máquinas que llenaban varios edificios. Hacia 1970 los nuevos cifrados basados en ordenadores se comenzaron a hacer populares a la vez que el mundo migraba a comunicaciones computarizadas, y la utilidad de Enigma (y de las máquinas de cifrado rotatorio en general) rápidamente decrecía. En ese momento se decidió descubrir el pastel y comenzaron a aparecer informes oficiales sobre las operaciones de Bletchley Park en 1974.

En febrero de 2006, y gracias a un programa de traducción de este tipo de mensajes denominado "Proyecto-M4", se logró descifrar uno de los últimos mensajes que quedaban por descifrar aún tras la rendición alemana.

Con la ayuda de ordenadores particulares, se ha podido descifrar el contenido, enviado por un sumergible desde el Atlántico, y cuya traducción decía así: "Señal de radio 1132/19. Contenido: Forzados a sumergirnos durante ataque, cargas de profundidad. Última localización enemiga: 8:30h, cuadrícula AJ 9863, 220 grados, 8 millas náuticas. [Estoy] siguiendo [al enemigo]. [El barómetro] cae 14 milibares. NNO 4, visibilidad 10."

2.2 Componentes de la máquina Enigma

Una máquina Enigma consistía de cinco componentes principales:

1. Una placa de conectores que contenía de cero a treinta cables con doble conector.
2. Tres rotores ordenados de izquierda a derecha los cuales conectaban 26 puntos de contacto de entrada a 26 puntos de contacto de salida posicionados en caras alternas de un disco.
3. Ruedas dentadas alrededor de los rotores los cuales permitían al operador especificar una posición inicial para los rotores.
4. Un anillo móvil en cada uno de los rotores los cuales controlaban el comportamiento rotacional del rotor inmediatamente a la izquierda por medio de una hendidura.
5. Un reflector para reflejar las entradas y salidas de nuevo en la misma cara de puntos de contacto.

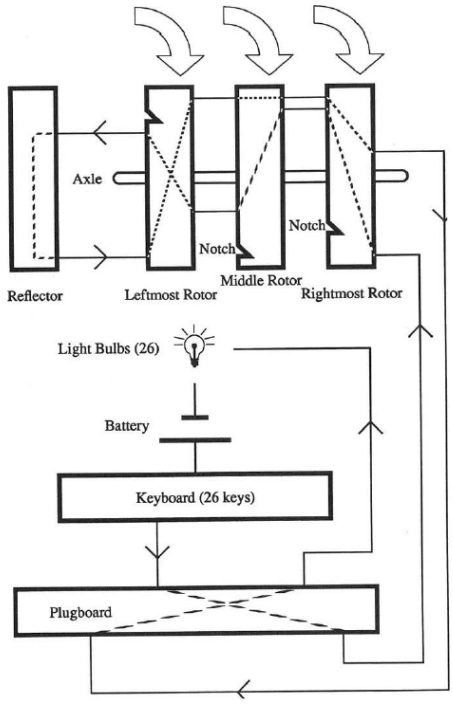

Figure 1: Esquema de la máquina Enigma

Equipo necesario adicional incluía un sistema mecánico para forzar el movimiento de los rotores, un teclado de 26 letras, 26 bombillas para las letras de la salida de la máquina y una batería para alimentar las bombillas.

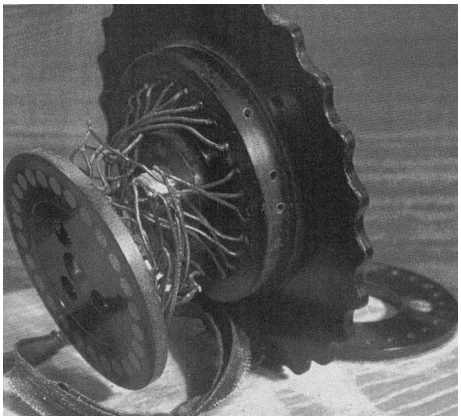

Figure 2: Uno de los rotores de la máquina Enigma

El primer componente variable era la placa de conectores, que contenía 26 de estos en el panel frontal de Enigma. Un cable de doble conexión podía unir dos conexiones que correspondían a dos pares de letras.

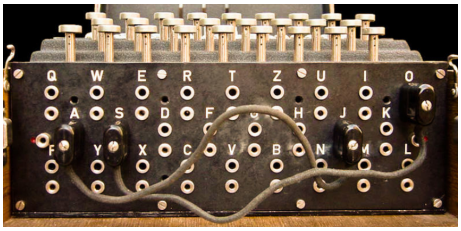

Figure 3: Vista frontal de la máquina

Los criptógrafos de enigma tenían la posibilidad de elegir cuantos cables diferentes podrían ser insertados

(de 0 a 13) y que letras deberían ser conectadas

2.3 Matemáticas detrás de la máquina Enigma

Habían tres elementos los cuales deben ser considerados cuando se calcula el número de conexiones posibles: el número de cables usados, qué conjunto de orificios de conexión fueron seleccionadas para recibir los cables y las interconexiones dentro del conjunto de orificios para recibir los cables. Habían 26 orificios, cada cable consume 2 orificios (uno para cada extremo del cable). Habiendo usado p cables ($0 \leq p \leq 13$) insertados en la placa de orificios de conexion (plugboard), hay por lo tanto $\binom{26}{2p}$ combinaciones diferentes de orificios que podrían haber sido seleccionados. Habiendo calculado el número de grupos diferentes. Después de insertar el primer extremo del primer cable, el otro extremo tendría 2p-1 orificios libres, en caso del segundo habría 2p-3. De esto la cantidad de formas de conectar sería $(2n-1)!!$. Este patrón sigue para el cable número p para el cual solo habría un orificio disponible, pues cada cable consume 2 de ellos, por lo tanto el número de conexiones diferentes que podría haber sido hecha por un operador de enigma está dado por la combinación de estos dos resultados:

$$\binom{26}{2p} x (2p-1)!! = \frac{26!}{(26-2p)!xp!x2^p}$$

Usando la ecuación anterior el número de combinaciones para todos los posibles valores de p se muestran en la siguiente tabla:

p	combinaciones	p	combinaciones
0	1	7	1,305,093,289,500
1	325	8	10,767,019,638,375
2	44,850	9	53,835,098,191,875
3	3,453,450	10	150,738,274,937,250
4	164,038,875	11	205,552,193,096,250
5	5,019,589,575	12	102,776,096,548,125
6	100,391,791,500	13	7,905,853,580,625

Table 1: Número de combinaciones para todos los valores de p

Una característica interesante de la máquina es que el máximo número de combinaciones no ocurre para 13 cables conectados como se esperaría, sino cuando los operadores usan 11 de ellos. Por lo tanto el número total de combinaciones está dado por la siguiente formula:

$$\sum_{p=0}^{13} \frac{26!}{(26-2p)!xp!x2^p} = 532,985,208,200,576$$

2.4 Método de cifrado

Los alemanes establecieron un sistema que mezcló dos ideas.

Al principio de cada mes, se daba a los operadores de la Enigma un nuevo libro que contenía las configuraciones iniciales para la máquina. Por ejemplo, en un día particular las configuraciones podrían ser poner el rotor n.º 1 en la hendidura 7, el n.º 2 en la 4 y el n.º 3 en la 6. Están entonces rotados, para que la hendidura 1 esté en la letra X, la hendidura 2 en la letra J y la hendidura 3 en la A. Como los rotores podían permutarse en la máquina, con tres rotores en tres hendiduras se obtienen otras 3 x 2 x 1 = 6 combinaciones para considerar, para dar un total de 105.456 posibles alfabetos.

A estas alturas, el operador seleccionaría algunas otras configuraciones para los rotores, esta vez definiendo sólo las posiciones o "giros" de los rotores. Un operador en particular podría seleccionar ABC, y éstos se convierten en la configuración del 'mensaje para esa sesión de cifrado'. Entonces teclearon la configuración del mensaje en la máquina que aún estaba con la configuración inicial. Los alemanes, creyendo que le otorgaban más seguridad al proceso, lo tecleaban dos veces, pero esto se desveló como una de las brechas de seguridad con la que "romper" el secreto de Enigma. Los resultados serían codificados para que la secuencia ABC tecleada dos veces pudiera convertirse en XHTLOA. El operador entonces gira los rotores a la configuración del mensaje, ABC. Entonces se teclea el resto del mensaje y lo envía por la radio.

En el extremo receptor, el funcionamiento se invierte. El operador pone la máquina en la configuración inicial e introduce las primeras seis letras del mensaje. Al hacer esto él verá ABCABC en la máquina. Entonces gira los rotores a ABC e introduce el resto del mensaje cifrado, descifrándolo.

Este sistema era excelente porque el criptoánalis se basa en algún tipo de análisis de frecuencias. Aunque se enviaran muchos mensajes cualquier día con seis letras a partir de la configuración inicial, se asumía que esas letras eran al azar. Mientras que un ataque en el propio cifrado era posible, en cada mensaje se usó un cifrado diferente, lo que hizo que el análisis de frecuencia fuera inútil en la práctica.

La Enigma fue muy segura. Tanto que los alemanes confiaron mucho en ella. El tráfico cifrado con Enigma incluyó de todo, desde mensajes de alto nivel sobre las tácticas y planes, a trivialidades como informes del tiempo e incluso las felicitaciones de cumpleaños.

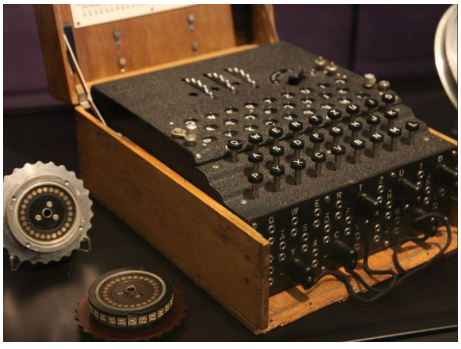

Figure 4: Vista superior de la máquina

3 Results and Discussion

3.1 Implementación de la máquina enigma

Para simular el funcionamiento de la máquina Enigma utilizamos tres clases, la clase Rotor, la clase Plugboard y la clase Máquina:

1. La clase Rotor: esta clase será utilizada para representar el cableado interno de los rotores y del reflector.
   (a) ATRIBUTOS: la clase rotor cuenta con dos atributos: una cadena con los 26 caracteres del alfabeto desordenados y que representará el cableado interno de los rotores. Por ejemplo, veamos la siguiente ilustración de un rotor:

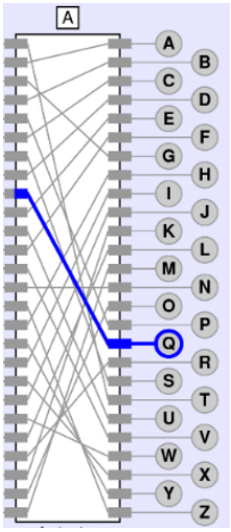

Figure 5: Representación de un rotor

Aquí vemos que la letra A de la parte derecha se conecta a la izquierda con la B, la B de la derecha con la D de la izquierda, la C de la derecha con la F de la izquierda y así sucesivamente. Por ello la cadena que nos ayudaría a representar este rotor sería: "BDFHJLCPRTXVZNYEIWGAKMUSQO".

El reflector se puede modelar del mismo modo, por ejemplo, para la siguiente imagen:

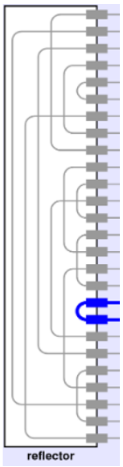

Figure 6: Representación del reflector de la máquina

Este reflector puede modelarse así: "IXUHFEZDAOMTKQJWNSRLCYPBVG". La letra A con la I, la B con la X, la C con la U y así sucesivamente. El segundo atributo es un entero que

medirá el número de veces que ese rotor ha girado. Ese método se llamará cuando los botones sean presionados.

(b) INSTANCIACIÓN: Para instanciar un rotor se necesitan dos variables: el carácter inicial del rotor y la cadena de 26 caracteres en desorden (NOTA: para el reflector, dicha cadena no puede tener un carácter en su verdadera posición del alfabeto, por ejemplo, la A no puede ir al inicio o la I no puede ir en la novena posición). Dependiendo del carácter inicial, el cableado interno del rotor se modificará, ya que en la máquina real el rotor se mueve para poder definir las condiciones iniciales.

```
def __init__(self, char_init='A', dest_go=""):

    self.count = 0
    self.dest_go = dest_go

    if(char_init != 'A'):
        ind_init = ascii_uppercase.find(char_init)
        self.dest_go = self.dest_go[ind_init:] + self.dest_go[:ind_init]

    if(len(dest_go) == 0):
        self.dest_go = self.set_random_string()
```

Figure 7: Condiciones iniciales

(c) MÉTODOS: esta clase cuenta con tres métodos:

- move: modifica el cablead cuando el rotor se mueve una posición. Se llamará en la clase MÁQUINA cuando se presiona una tecla.
- push: procesa una letra que ingresa en el flujo de ida de la encriptación al presionar una tecla.
- anti_push: procesa una letra que ingresa en el flujo de vuelta de la encriptación tras pasar por el reflector.

2. La clase Plugboard:

(a) ATRIBUTOS: esta clase solo tiene como atributo un diccionario que le permite modelar el cableado en el panel frontal de una máquina enigma real.

(b) INSTANCIACIÓN: para instanciar esta clase solo es necesario pasarle al constructor un diccionario que simule el cableado del panel frontal.

```
cables = {
'A' : 'C',
'B' : 'F',
'G' : 'H',
'L' : 'N',
'K' : 'R',
'Q' : 'E'
}


plugboard = Plugboard(cables)
```

Figure 8: Conexiones de los cables

(c) Métodos: procesar_caracter(char): este método solo recibe un argumento de tipo CHAR que viene a ser el carácter que el Plugboard va a procesar.

```
def procesar_caracter(self, char):
    char_procesado = ''

    cableado_claves = list(self.cableado.keys())
    cableado_valores = list(self.cableado.values())

    if char in cableado_claves:
        char_procesado = self.cableado[char]
    elif char in cableado_valores:
        char_procesado = cableado_claves[cableado_valores.index(char)]
    else:
        char_procesado = char

    return char_procesado
```

Figure 9: Procesamiento del caracter en el plugboard

3. La clase Máquina: esta clase es la piedra angular de la aplicación e integra a las dos clases previamente mencionadas.

(a) ATRIBUTOS:

i. **list_of_rotors:** este atributo es un arreglo que almacenará objetos de la clase Rotor representando a todos los rotores de la máquina. La máquina solo podrá tener hasta 5 rotores.

ii. **Plugboard:** este atributo es un objeto de la clase Plugboard.

iii. **Reflector:** este atributo representará al reflector mediante un objeto de la clase rotor.

iv. **INSTANCIACIÓN:** en el constructor se tienen cadenas predefinidas con los cableados de los rotores y del reflector. Además, el constructor tiene como argumentos una lista con los rotores que se desean utilizar, una lista con las posiciones iniciales de cada uno de los rotores y un diccionario para el plugboard. La instanciación se realiza así:

```
rotors_numbers = [2,1,3,5,4]
init_chars = ['C','F','G','B','M']
cables = {
'A' : 'C',
'B' : 'F',
'G' : 'H'
}

mq = Maquina(rotors_numbers, init_chars, cables)
```

Figure 10: Orden de los rotores, posiciones iniciales y cableado del plugboard

4 Conclusiones

Se logró desarrollar con éxito la implementación de la máquina enigma en el lenguaje python, se pudo agregar una mayor complejidad a la máquina agregando más rotores a la máquina (ya que no se tiene la limitación física del diseño de la máquina) y la posibilidad de establecer el orden, sin embargo, esta complejidad agrega hace que el usuario que desea descifrar el mensaje necesita conocer más parámetros iniciales de la máquina. Durante el desarrollo se estableció un mayor enfoque en comprender el funcionamiento de la máquina y cómo modelar esta a un lenguaje de programación, es por ello que se usó librerías básicas para la interfaz gráfica, sin embargo, la interfaz es muy intuitiva y sencilla.

La implementación también proporciona la limitación de que usuario que desea desencriptar el mensaje tiene que volver a ejecutar el programa y establecer los parámetros de la máquina que ha encriptado el mensaje.

References

[1] A. Ray Miller. The cryptographic mathematics of enigma, cryptologia, 1995.

[2] Crypto museum. History of the enigma. `https://www.cryptomuseum.com/crypto/enigma/hist.htm`, 2020 (accessed: jule 28, 2020).