

PRÁCTICA 1

**Máquina Enigma**

1. Objetivos

En esta práctica se estudiará un método de criptografía clásico: La Máquina Enigma, usada por los alemanes en la II Guerra Mundial.

2. Objetivos detallados a alcanzar

Objetivo 1:

Entender el funcionamiento de la máquina.

Existe un simulador gráfico muy intuitivo, elaborado en java, disponible en el campus virtual.

Se describirá el proceso de codificación, mediante el uso de los rotores, el reflector y las clavijas de intercambio. Se describirá la clave, consistente en las posiciones de los rotores y los caracteres intercambiados.

La máquina enigma consta de 3 rotores (izquierda, central y derecha), los cuales se ponen en una determinada configuración inicial del alfabeto. Esta configuración inicial es la clave.

Imagen que contiene Forma

Descripción generada automáticamente

Para cifrar solo hacía falta pulsar una letra para que la luz pasara a través de las permutaciones de los rotores, llegase a un reflector, volviese por las permutaciones de los rotores y acabara iluminando la nueva letra codificada.

Dicho reflector es también intercambiable, pero nosotros lo vamos a tener fijo, es decir, siempre será el mismo.

Por lo tanto, cada rotor es una sustitución monoalfabética que va cambiando en cada pulsación:

* El primer cilindro (derecho) avanza una posición en cada pulsación.
* El segundo cilindro (central) avanza una posición por cada vuelta completa del primer cilindro.
* El tercer cilindro (izquierdo) avanza una posición por cada vuelta completa del segundo cilindro.
* El reflector NO gira, está siempre fijo.

Diagrama

Descripción generada automáticamente con confianza media

Además de todo esto, la máquina contaba con una serie de clavijas las cuales se podían conectar para hacer una sustitución inicial. Había una clavija por letra del alfabeto. Al conectar 2 de ellas, por ejemplo, la clavija de la letra “C” y la clavija de la letra “M”, si se tecleaba alguna de estas 2 letras se realizaba una sustitución de la letra “C” por la “M” o de la “M” por la “C” antes de pasar por los rotores, y si la letra codificada tras la vuelta por los rotores era alguna de estas, se volvía a hacer el intercambio. Se pueden unir tantas clavijas como se quiera siempre y cuando no se repitan letras.

Ahora vamos a ver el funcionamiento más en detalle de los rotores. Vamos a suponer que la clave inicial es **CMA** rotores izquierdo, central y derecho respectivamente. Además, los rotores que vamos a utilizar son el I, II y III, para el izquierdo, central y derecho respectivamente. Nuestra letra a codificar va a ser la letra D. Al teclear dicha letra, antes de nada, se incrementan las posiciones, es decir, se incrementa en 1 la posición del rotor derecho, por lo tanto, el rotor que inicialmente estaba en la letra A, pasa a ser una B.

Una vez se han incrementado las posiciones se pasan a hacer las sustituciones. Si no hay intercambio por clavijas la letra seleccionada es el desplazamiento que hay que realizar en el rotor derecho, es decir, si la letra es una D se deberá realizar un desplazamiento de 3 posiciones a partir de la letra que indica el rotor derecho que en este caso es la letra B, por lo que B+3 posiciones se convierte en la letra E. En este punto hay que ver qué letra de la permutación le corresponde a la letra E. Como hemos seleccionado el rotor III para el rotor derecho tenemos que ver qué letra le corresponde a la posición 5 (posición de la letra E en el alfabeto):

**BDFHJLCPRTXVZNYEIWGAKMUSQO**

Para la siguiente sustitución del rotor central el cálculo del desplazamiento se realiza con la diferencia de posiciones entre la nueva letra codificada (en este caso la letra J) y la posición del rotor derecho (en este caso la letra B), por lo que el desplazamiento sería de 10 (posición de la letra J en el alfabeto) – 2 (posición de la letra B en el alfabeto) = 8. A partir de aquí el procedimiento es igual que en el caso anterior, es decir, se suma el desplazamiento a la letra marcada por el rotor central M+8=U y se ve la correspondencia con la permutación del rotor central (rotor II), en este caso corresponde con la letra P.

Este procedimiento se sigue hasta obtener la letra codificada por el reflector. Una vez tenemos dicha letra hay que realizar el mismo camino que hemos hecho, pero en orden inverso hasta llegar al principio que será nuestra letra codificada.

En la siguiente imagen tenemos el resultado del ejemplo:

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Ejercicio 1

Objetivo 2: Elaborar un simulador, en Python, que admita una codificación en forma de clave. Se utilizarán los rotores y reflector descritos en:

http://en.wikipedia.org/wiki/Enigma\_rotor\_details

En concreto se usarán los rotores y reflector B :

|  |  |
| --- | --- |
| Rotor/INPUT | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| I | EKMFLGDQVZNTOWYHXUSPAIBRCJ |
| II | AJDKSIRUXBLHWTMCQGZNPYFVOE |
| III | BDFHJLCPRTXVZNYEIWGAKMUSQO |
| IV | ESOVPZJAYQUIRHXLNFTGKDCMWB |
| V | VZBRGITYUPSDNHLXAWMJQOFECK |
| Ref. B | YRUHQSLDPXNGOKMIEBFZCWVJAT |

El programa debe aceptar el uso de tres de los cinco rotores, en las posiciones izquierda, central y derecha. También debe aceptar el uso del reflector B, opcionalmente se podrá cambiar a otro reflector.

El avance de los rotores se hace mediante medios mecánicos de engranajes. Para forzar el paso del rotor situado a la izquierda, cada rotor dispone de una muesca. A los efectos de simulación es irrelevante este detalle, pero introduce un comportamiento peculiar que lo hace algo diferente de lo esperado en un mecanismo de engranaje. Por la disposición de los rotores, cada muesca le hace corresponde con una cierta posición mostrada en la ventanilla, que es lo que nos importa, en la tabla vemos las posiciones de las muescas, y su correspondencia con la letra mostrada como clave:

|  |  |  |  |
| --- | --- | --- | --- |
| **Rotor** | **Pos. Muesca.** | **Letra clave** | **Salto izda.** |
| I | Y | Q | Q -> R |
| II | M | E | E -> F |
| III | D | V | V -> W |
| IV | R | J | J -> K |
| V | H | Z | Z -> A |

**Importante. Doble paso de Enigma**

El salto del rotor a la izquierda se produce en el paso de la letra clave a su siguiente. Los criptoanalistas ingleses utilizaban la frase mnemónica “Royal Flags Wave Kings Above” para memorizarlas.

Y una cuestión IMPORTANTE, el avance del rotor central, sea del tipo que sea, por su disposición mecánica, hay un momento en que se produce un doble paso: Cuando hace avanzar al rotor del extremo izquierdo.

Además, si en la clave inicial figura en el rotor central la letra clave, también se producirá un cambio en la primera pulsación, aun cuando aparentemente no corresponde.

Ejercicio 2

Objetivo 3: Ataque en fuerza bruta contra la máquina Enigma.

Se trata de emular las tareas de Alan Turing y el equipo de Bletchley Park durante la II Guerra Mundial y su bomba criptográfica.

El objetivo es tratar de descubrir la clave utilizada en un mensaje mediante un ataque de fuerza bruta. Para ello se dispone de un diccionario de 18 palabras, de las que una de ellas aparece en el mensaje. La clave consiste en la disposición inicial de los tres rotores. En este caso, y por simplificar, asumimos que el rotor I está a la izquierda, el II en el centro, y el III a la derecha, siendo éste el que avanza con cada pulsación, y sabiendo que puede haber un único intercambio por clavija (podría no haberlo). Es decir, la clave está en la forma XXXYY, siendo las X las posiciones de los rotores, e YY las clavijas intercambiadas.

El mensaje a descifrar es:

KHRVSLTCYDFAFTEBVSCTMMRFVDMSIIRRTRZFBAOMWHJQDTOTARWWYIPWEZLUKBAVMYLOSGRIDOWMEGBBVULAUDXOCXGBEZPJQXEEVTYMMIHEEZPDUORIJLHKNOXSRQCONNXIWWOIROXQIMKZMJIRMYCSJLIUSDMMEGNSPKUSJALYLMWIDXFXVFSWZQUZQSWMVFVHOXVPVIXLUZVREKBZIIPHCOSBKBA

Y el diccionario:

1. ambiguo

2. obvio

3. trivial

4. estupendo

5. politecnica

6. lechuga

7. lugar

8. pacifico

9. primera

10. señora

11. bancal

12. mancha

13. celula

14. albacete

15. suaves

16. mancha

17. fiesta

18. patata

El ataque por fuerza bruta en esta forma puede dar lugar a falsos positivos (si la palabra del diccionario no tiene caracteres intercambiados). Por lo que conviene listarlos todos y dejar a interpretación humana las salidas.

El algoritmo debe ser: Para todas las posibles claves, cifrar de nuevo el mensaje, y buscar en el mismo la aparición de alguna palabra del diccionario.