****

**CIENCIAS DE LA COMPUTACIÓN**

**ÁLGEBRA ABSTRACTA**

**ALGORITMOS DE CRIPTOGRAFIA TRADICIONALES**

**ALUMNO:**

**ROLANDO ALBERTO CATERIANO DELGADILLO**

**III SEMESTRE**

**ABRIL 2020**



**FIRMA**

¨LOS ALUMNOS DECLARAN HABER REALIZADO EL PRESENTE TRABAJO DE ACUERDO A LAS NORMAS DE LA UNIVERSIDAD CATÓLICA SAN PABLO¨.

**Algoritmos de Criptografía Tradicionales**

**Introducción**

A lo largo de la historia de la humanidad se ha tenido la necesidad de codificar mensajes para ocultar cierta información, ya sean por motivos religiosos, políticos o por diversión, esto ha originado que se busquen maneras de ocultar esta información siguiendo algún algoritmo para que pueda ser descifrado solo por el destinatario.

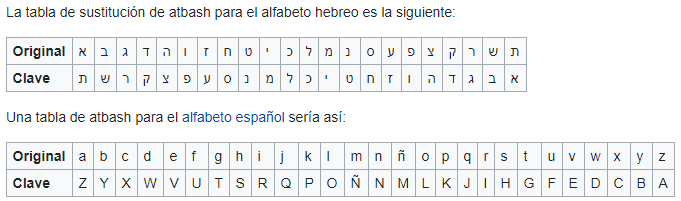
Para asegurarse que el destinatario sea el único que pueda descifrar el mensaje es que se empezaron a usar fórmulas matemáticas y nuevas técnicas de encriptación para que, si por algún motivo, una persona ajena interceptaba el mensaje no le fuera fácil conocer el contenido del mismo.

Con los avances de la tecnología los algoritmos de encriptación han ido evolucionando, esto se debe que al vivir en un mundo digitalizado debemos mantener mucha información oculta y segura, como cuentas de banco, datos personales, etc. Ya que ninguno de estos algoritmos llega a ser 100% irrompible es que se estudian nuevas formas para mejorarlos, ya que, como dijimos antes, todos se pueden romper, pero la idea es que sea muy muy difícil poder hacer eso.

**Algoritmos Tradicionales**

**Atbash**

Es un tipo de cifrado por sustitución utilizado por los hebreos, consiste en reemplazar la primera letra del alfabeto por la última, la segunda por la penúltima, la tercera por la tras antepenúltima y así sucesivamente.



El criptoanálisis de este algoritmo es bastante sencillo ya que no cuenta con una gran complejidad.

**Libreta de un solo uso**

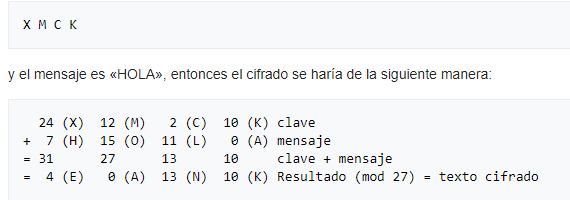
Es un tipo de algoritmo de cifrado por el que el mensaje se combina con una clave aleatoria igual de larga que el mensaje, y que solo se utiliza una vez, fue inventada en 1917 por Gilbert Vernam.

Este algoritmo es mono alfabético y funciona de manera similar al algoritmo de Vigenere, ya que a la posición de cada letra del mensaje se le tiene que sumar la posición que le corresponda en la clave, la diferencia con Vigenere, además del mono alfabeto es que en Vigenere se repite la clave hasta completar el mensaje, en este caso cada palabra del mensaje tiene una clave de igual tamaño de la palabra que le corresponde, es acá dond radica la complejidad del criptoanálisis de este algoritmo,

Este algoritmo tiene pocas desventajas como que las libretas de un solo uso deben ser realmente aleatorias, la generación e intercambio de las libretas de un solo uso tiene que ser segura, y la libreta tiene que ser al menos tan larga como el mensaje.

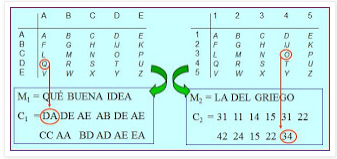
En esta imagen se puede ver un ejemplo de las claves.





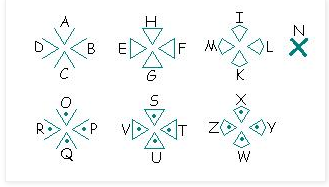
**Polybios**

Es el cifrado por sustitución de caracteres más antiguo que se conoce, se usa una matriz en la que se escribe todo el alfabeto, en los índices se pueden usar letras o números para la codificación, se usa un sistema de coordenadas para sustituir cada letra del mensaje original.



**El cifrado Pigpen**

El Temple era una orden de monjes fundada en el siglo XII., cuya misión principal era asegurar la seguridad de los peregrinos en Tierra Santa. Rápidamente, los templarios se desentendieron de este objetivo, y se enriquecieron considerablemente hasta el punto de llegar a ser tesoreros del rey y del Papa. Para codificar las letras de crédito que ellos intercambiaban, ellos remplazaban cada letra por un símbolo.



**Enigma**

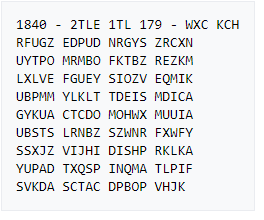
Es una máquina de 3 rotores que permitía usarla tanto para cifrar como para descifrar mensajes, esta máquina fue utilizada por los alemanes en la segunda guerra mundial para codificar sus mensajes.

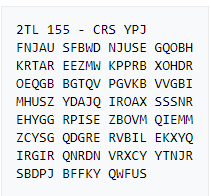


El uso de rotores múltiples en Enigma brindó un modo simple de determinar qué alfabeto de sustitución usar para un mensaje en particular (en el proceso de cifrado) y para un texto cifrado (en el de descifrado). A este respecto fue similar al cifrado polialfabético. Sin embargo, a diferencia de la mayoría de las variantes del sistema polialfabético, Enigma no tenía una longitud de clave obvia, debido a que los rotores generaban una nueva sustitución alfabética en cada pulsación, y toda la secuencia de alfabetos de sustitución podía cambiarse haciendo girar uno o más rotores, cambiando el orden de los rotores, etc., antes de comenzar una nueva codificación. En el sentido más simple, Enigma tuvo un repertorio de 26 x 26 x 26 = 17.576 alfabetos de sustitución para cualquier combinación y orden de rotores dada. Mientras el mensaje original no fuera de más de 17.576 pulsaciones, no habría un uso repetido de un alfabeto de sustitución.

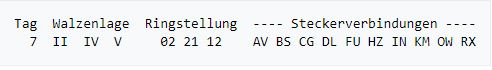
Al principio de cada mes, se daba a los operadores de la Enigma un nuevo libro que contenía las configuraciones iniciales para la máquina. Por ejemplo, en un día particular las configuraciones podrían ser poner el rotor n.º 1 en la hendidura 7, el n.º 2 en la 4 y el n.º 3 en la 6. Están entonces rotados, 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.

El siguiente es un mensaje auténtico enviado el 7 de julio de 1941 por la División SS-Totenkopf sobre la campaña contra Rusia, en la Operación Barbarroja. El mensaje (enviado en dos partes) fue descifrado por Geoff Sullivan y Frode Weierud, dos miembros del Crypto Simulation Group (CSG).



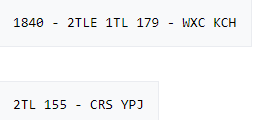


El mensaje fue cifrado para el modelo de tres rotores con el reflector B (habrá que usar el mismo modelo para descifrarlo, o uno compatible). Para descifrar el mensaje, primero hay que configurar la máquina con la información diaria especificada en los libros de códigos alemanes para ese mes. Para el 7 de julio de 1941 era:

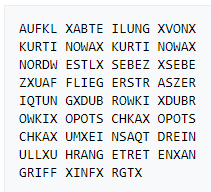


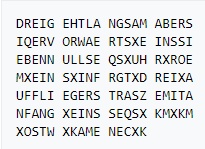
El operador de la máquina debía colocar esa configuración antes de enviar o recibir el primer mensaje del día. Cogería los rotores (Walzenlage) 2, 4 y 5 (en ese orden), y movería el anillo de cada rotor a las posiciones 2, 21 y 12 respectivamente, como se indica en Ringstellung (a veces la configuración se puede ver en las letras correspondientes a la posición del anillo; en este caso serían B U L), y los insertaría en la máquina. También debía colocar los cables conectores uniendo en la parte baja de la máquina las posiciones que se indican en Steckerverbindungen, uniendo A con V, B con S, C con G, etc. Esta configuración se mantendrá en todos los mensajes del día, y con ella ya se pueden empezar a descifrar mensajes.

El mensaje original se envió en dos partes (ya que el tamaño máximo por cada mensaje era de 250 letras). Cada mensaje tiene una cabecera, que se enviaba sin cifrar (y es la única parte del mensaje que podía tener números); en este caso:

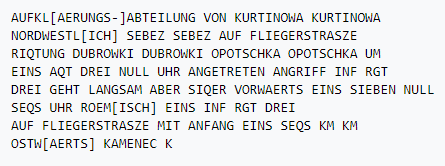


En la cabecera se indicaba la hora a la que se mandaba el mensaje (en este caso 1840 representa las 18:40), cuántas partes componían el mensaje (seguido de TLE, de Teile) y qué parte era (seguido de TL, de Teil) si había más de una, el tamaño del texto cifrado y dos grupos de tres letras (que eran diferentes y aleatorios en cada mensaje). El primer grupo era la configuración inicial y el segundo la clave cifrada del mensaje. El operador moverá los tres rotores a la letra indicada por el primer grupo (W X C), y tecleará el otro grupo, la clave cifrada (K C H), que le dará al operador la clave sin cifrar, en este caso B L A). A continuación pondrá los tres rotores en las posiciones B L A. y tecleará el resto del mensaje cifrado, teniendo en cuenta que las cinco primeras letras corresponden al Kenngruppe, que indicará quiénes pueden leer el mensaje (en este caso se puede ignorar)





Uniendo los mensajes, y usando las X como espacios (algunos espacios faltan en el mensaje original), y algunas abreviaturas (entre corchetes) queda:



Los nombres propios se ponían dos veces seguidas (por ejemplo, KURTINOWA), y algunas combinaciones de letras se sustituían, por ejemplo, CH por Q (en SIQER, que es sicher), y los números debían escribirse con letras. El texto traducido sería:

**Unidad de reconocimiento de Kurtinowa, noroeste de Sebez en el corredor de vuelo en dirección a Dobrowki, Opotschka. Empezó a moverse a las 18:30. Ataque. Regimiento de infantería 3 avanza despacio pero seguro. Hora 17:06, I Regimiento de infantería 3 en el corredor de vuelo comenzando a 16 km hacia el este de Kamenec.**

**Referencias**

<https://es.wikipedia.org/wiki/Atbash>

<https://es.wikipedia.org/wiki/Libreta_de_un_solo_uso#Historia>

<http://manuelluna08.blogspot.com/2012/10/criptografia-y-los-diferentes-tipos-de_6.html>

<https://es.wikipedia.org/wiki/Enigma_(m%C3%A1quina)>