El arte de la Criptografía

INDICACIONES

Hola.
Resolvamos juntos: El cifrado de código Ottendorf, lo realizaremos sobre dos páginas de un libro.
El emisor envía grupos de 3 números.
-El primero corresponde al número de página.
-El segundo al número de renglón.
-El tercero al número de letra.
Los signos de puntuación ocupan un lugar y cuentan como si fuese una letra, al final de cada palabra siempre irá un punto.
Descubramos al o los autores del delito juntos...

ORÍGENES

La aparición de los sistemas de cifrado para ocultar información -o mejor dicho protegerla de otros- tienen aproximadamente unos cuatro mil años de antigüedad. La palabra criptografía proviene del griego ***Krypto, oculto y Graphos, escribir***. Se dice que una comunicación está cifrada cuando solamente la persona que envía el mensaje (emisor) y la que lo recibe (receptor) son los únicos que poseen la capacidad de descifrarlo. Cualquier persona que intercepte este mensaje vería solamente un texto o un montón de letras sin sentido.

Ejemplos de cifradas están presentes en todas las civilizaciones antiguas e incluso en la mitología.

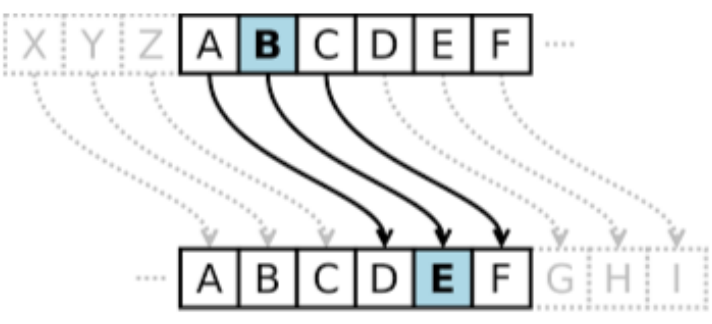
En la Biblia, en el libro de Jeremías, se nombra el ***Atbash*** un sistema de sustitución de letras que se utiliza para cifrar mensajes (aprox, 600 AC).

En la antigua Grecia, en el libro de la Ilíada de Homero, aparece la referencia al cifrado de mensajes. Belerofonte, el héroe mitológico debía entregar un mensaje al Rey Preto de Tirinto, enviada por el Rey Lobates de Licia, en esta carta el portador no conocía el contenido de esta, ya que el mensaje que escondía era la muerte para su portador.

Los espartanos utilizaban el sistema de ***transposición***. Consistía en enrollar un pergamino alrededor de una estaca de madera -llamada escitala- que servía para ordenar las letras. Aquí tanto emisor como receptor debían tener en su poder la misma escitala para leer correctamente el mensaje. Como para hacer gráfico, esta estaca se podría decir que es el antepasado del criptex, que aparece en la Novela de Dan Brown en el Código Da Vinci. El protagonista Profesor Robert Langdon, interpretado por el actor Tom Hanks, debe resolver una serie de mensajes encriptados por poder abrir el criptex y encontrar la tumba con los restos de María Magdalena.

Escitala Espartana

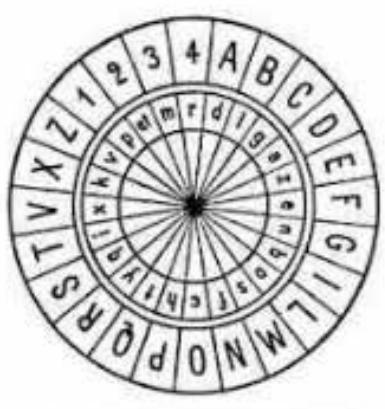
En la antigua Roma aparece el denominado Cifrado Cesar, en donde su uso e invención se le atribuyen al político y militar Cayo Julio César. Este tipo de cifrado se basa en el desplazamiento de letras, cada letra del mensaje se sustituye por las letras que la precede o antecede en el alfabeto. El historiador Romano Suetonio, César utilizaba el desplazamiento de 3 letras y el primer emperador de Roma Augusto (sobrino nieto de Julio Cesar) utilizaba el desplazamiento de 1 letra.



Cifrado de Cesar

Así llegamos a la edad media, donde se dio la gran revolución de la ***criptografía***. Su origen se lo debemos al árabe Al-Kindi, el que sentaría las bases para romper este tipo de cifrados. Por medio del análisis de patrones en donde se ponía atención a la repetición y frecuencia de letras o palabras. Los árabes Ibn al-Durayhin y Ahmad al-Qalqashandi perfeccionaron los análisis de las frecuencias y desarrollaron códigos más complejos.

En la época del Renacimiento, los Estados Pontificios, harían una uso intensivo de los mensajes criptográficos. Una figura relevante para esta disciplina fue León Battista Alberti un arquitecto, humanista, matemático, criptógrafo, filósofo, lingüista y músico, que se desempeñó como secretario personal de los Papas Eugenio IV, Nicolas V y Pío II, trabajó en el llamado cifrado ***polialfabético*** y sentaría las bases para la fabricación de sistemas automáticos de cifrados más modernos. Este sistema ideado por Alberti utilizaba un mecanismo de codificación mecánico (basado en discos) conocido como el ***cifrado de Alberti***, al día de hoy continúa siendo un misterio ya que no pudo ser descifrado.



Leon Battista Alberti's cipher disk

Tal vez el mas famoso de todos gracias a el 7° arte, fue la ***maquina enigma*** utilizada por la Alemania Nazi. La enigma fue una máquina de rotores, diseñada para cifrar y descifrar mensajes, patentada en 1918 por la empresa alemana Scherbius y Ritter. Este sistema en su interior poseía rotores con letras al estilo Criptex, estos discos rotatorios poseían un funcionamiento eléctrico. Este juego de rotores -también llamados ruedas o tambores- son discos rotatorios con una formación de contactos eléctricos en cada lado, el cableado entre los contactos realizaba una sustitución de letras, reemplazándolas de una manera compleja, después de encriptar cada letra. Los rotores avanzaban posiciones, cambiando la sustitución. Parece un trabalenguas pero así funcionaba. Una máquina de rotores produce un complejo cifrado de sustitución polialfabética (como la que utilizaba Alberti), que cambia con cada tecla pulsada. Aquí tanto emisor como receptor tenían que tener una máquina y el correspondiente cifrado. Este sistema fue un gran dolor de cabeza para las fuerzas aliadas durante la guerra, hasta que lograron dar con una de ellas a bordo de un U-boat o submarino alemán. Aquí es donde aparece la figura de Alan Turing, conocido como el padre de la computación.

Un día después de la declaración de Guerra de Gran Bretaña, en septiembre de 1939, Alan Turing fue convocado a Bletchley Park, lugar donde funcionaba la Escuela Gubernamental de Código y Cifrado. Cerca de nueve mil personas trabajaban para interpretar comunicaciones enemigas. El equipo liderado por Turing, a través de ecuaciones y cálculos, encontró pautas para determinar el funcionamiento de la misma, sin embargo no podían descifrarlos, entonces el genio pensó que para luchar con una máquina enigma hacía falta otra máquina.

Pudo poner en práctica sus ideas creando la ***máquina Bombe***. Esta buscaba la configuración de los rotores de la máquina alemana, implementando una secuencia de deducciones lógicas para cada combinación posible. Gracias a las mejoras aportadas por Gordon Welchman el 14 de marzo de 1940, la máquina estaba lista.

Máquina Bombe

Se construyeron alrededor de 200 máquinas, los trabajos dirigidos por Turing según historiadores acortaron la guerra unos dos años y salvaron la vida de más de catorce millones de personas.

RESPUESTAS

50-1-16 : L
50-2-13: A
50-6-31: .
50-6-27: H
50-7-8: I
50-10-25: S
50-11-30: T
50-12-4: O
50-13-12: R
50-12-18: I
50-14-12: A
50-12-9: .
50-15-31: T
50-16-1: E
50-16-22: R
50-16-28: M
50-18-16: I
50-19-3: N
50-22-20: A
50-17-21: .
50-22-19: C
50-24-7: O
50-25-3: N
50-23-8: .
56-1-15: D
56-1-19: O
56-1-32: S
56-3-19: .
56-3-12: P
56-3-24: E
56-4-14: C
56-4-16: A
56-5-9: D
56-5-38: O
56- 6-10: R
56-7-24: E
56- 8-14: S
56- 5-22: .
56-11-13: Q
56-11-14: U
56-11-16: E
56- 3-19: .
56-12-16: N
56-13-3: O
56- 3-19: .
56- 13-7: A
56-13-17: T
56-14-13: R
56-14-23: A
56-16-3: P
56- 16-13: A
56-17-11: R
56-17-21: A
56-18-15: N
56-17-17: .