educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 1

Criptosistemas clásicos

Cifrado de Polybius (150 ac)

- El **cifrado Polybius**, también llamado *cuadrado Polybius*, es un **cifrado de sustitución que utiliza una cuadrícula**.
- La fase de cifrado de Polybius consiste en **sustituir cada letra del texto plano por el par de coordenadas (fila, columna) de la letra en la cuadrícula.**
- Polybius había propuesto transmitir mensajes codificados a distancia de forma visual, por ejemplo mediante antorchas. N en la mano derecha y M en la izquierda para la pareja N, M, por ejemplo.

Ejemplo de sustitución monoalfabética monográmica de alfabeto mixto

- **Cifrar** el texto “DIME CON QUIÉN ANDAS Y TE DIRÉ QUIEN ERES”

  C= 14 24 32 15 13 34 33 41 45 24 15 33 11 33 14 11 43 54 44 15 14 24 42 15 41 45 24 15 33 15 42 15 43

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	NÑ	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Cifrado Playfair (1854)

- El cifrado Playfair fue el **primero en cifrar pares de letras** en la historia criptológica.
- **Wheatstone** inventó el cifrado para el secreto en la telegrafía, pero lleva el nombre de su amigo Lord Playfair, quien promovió su uso.
- La primera descripción registrada del cifrado Playfair fue en un documento firmado por Wheatstone el 26 de marzo de 1854.
- Fue utilizado con fines tácticos por las fuerzas británicas en la Segunda Guerra Bóer y en la Primera Guerra Mundial y para el mismo propósito por los británicos y australianos durante la Segunda Guerra Mundial.
- Un escenario típico para el uso de Playfair era proteger secretos importantes, pero no críticos durante el combate real, por ejemplo, el hecho de que un aluvión de artillería de proyectiles de humo comenzaría en 30 minutos para cubrir el avance de los soldados hacia el siguiente objetivo.

Ejemplo de sustitución monoalfabética digrámica

- **Cifrar** el mensaje:

  M = WITH A LITTLE HELP FROM MY FRIENDS

  Con la clave K = “BEATLES”

- **Solución**:

M = WI TH AL IT TL EH EL PF RO MX MY FR IE ND SX

C = EP BM TB ME LB BI AB RC UP KY RT MY PC KG DV

A	B	C	D	E
F	G	H	IJ	K
L	M	NÑ	O	P
Q	R	S	T	U
V	W	X	Y	Z

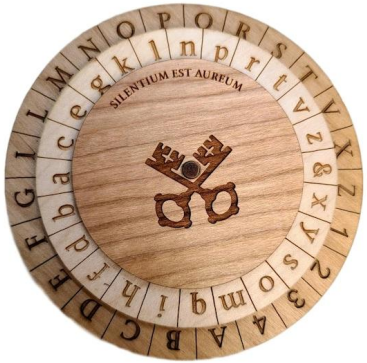
B	E	A	T	L
S	C	D	F	G
H	IJ	K	M	N
O	P	Q	R	U
V	W	X	Y	Z

- Un diagrama está compuesto por 2 caracteres.
- Reglas:
  a. Si M1M2 están en la misma fila/columna C1C2 son los caracteres de la derecha/abajo.
  b. En caso contrario son los caracteres de la diagonal.

Cifrado de Alberti

- **Leon Battista Alberti** desarrolló el método de codificación que lleva su nombre a mediados del siglo XV, entre 1466 y 1470, y lo plasmó en su tratado *De Componendis Cyphris.*
- Su tratado fue escrito para un grupo relativamente cerrado de personas dentro del Vaticano, no para su divulgación general. Tanto es así que no fue publicado hasta 1568.
- Alberti reflexiona en sus estudios sobre la **relación entre vocales y consonantes dentro de un texto,** lo que indica cierta preocupación por estos **aspectos estadísticos de la composición de las palabras.**
- El **disco de Alberti** era un dispositivo compuesto por dos anillos concéntricos, uno fijo en el centro y otro rodeando a ese primero y además móvil, es decir, que puede girar.

- El anillo externo tenía 24 posiciones en las que están grabadas 20 letras latinas, en mayúscula y ordenadas alfabéticamente, y los números del 1 al 4. Las letras que eliminó Alberti de su disco externo no las consideraba esenciales para hacerse comprender.



Comunicar un mensaje

- Para comunicar un mensaje, emisor y receptor debían tener cada uno un disco de Alberti.
- Las letras del anillo interno, que están descolocadas, debían seguir el mismo orden en ambos.
- Al principio del mensaje, el emisor indica dos letras, cada una de un anillo, que deben estar enfrentadas.
- La codificación se hace tomando cada letra del texto en claro, buscándola en el anillo externo y sustituyéndola por aquella que está en el anillo interno en esa misma posición, enfrentada a ella.

Cifrado de Jefferson/Bazeries

- **Thomas Jefferson** ideó el **cifrado de rueda** mientras desempeñaba el cargo de secretario de Estado de George Washington (1790-1793).
- Como se describió (aunque quizás nunca se construyó), el cifrado de la rueda de Jefferson constaba de treinta y seis piezas cilíndricas de madera, cada una de ellas enroscada en un eje de hierro.
- Las letras del alfabeto estaban inscritas en el borde de cada rueda en orden aleatorio. Al girar estas ruedas, las palabras podían mezclarse y cifrarse.
- Aunque parece que Jefferson nunca utilizó el cifrado de rueda y aparentemente abandonó la idea después de 1802, **fue reinventado por Bazeries** de forma independiente a principios del siglo XX.
- Designado como **M-94,** fue utilizado por el ejército de los EEUU y otros servicios militares desde 1922 hasta el inicio de la Segunda Guerra Mundial.

- **El orden de los discos era la clave de cifrado y descifrado.** Una vez que los discos han sido colocados en el eje en el orden correcto, el emisor rota cada disco hasta formar el mensaje deseado en una fila.
- A continuación, el emisor selecciona cualquier otra fila para transmitirse como mensaje cifrado.
- El receptor debe colocar los discos en orden, y rotarlos hasta formar el mensaje recibido en una fila y por último localizar la fila en la que esté el mensaje descifrado.

¡Sigamos trabajando!