educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 1

Criptosistemas clásicos

Antecedentes históricos

- **4500 a. C.**: jeroglíficos egipcios.
- **1500 a. C.**: Mesopotamia, escritura cuneiforme.
- **500 a. C.**: cifrados hebreos Atbash y Albam.

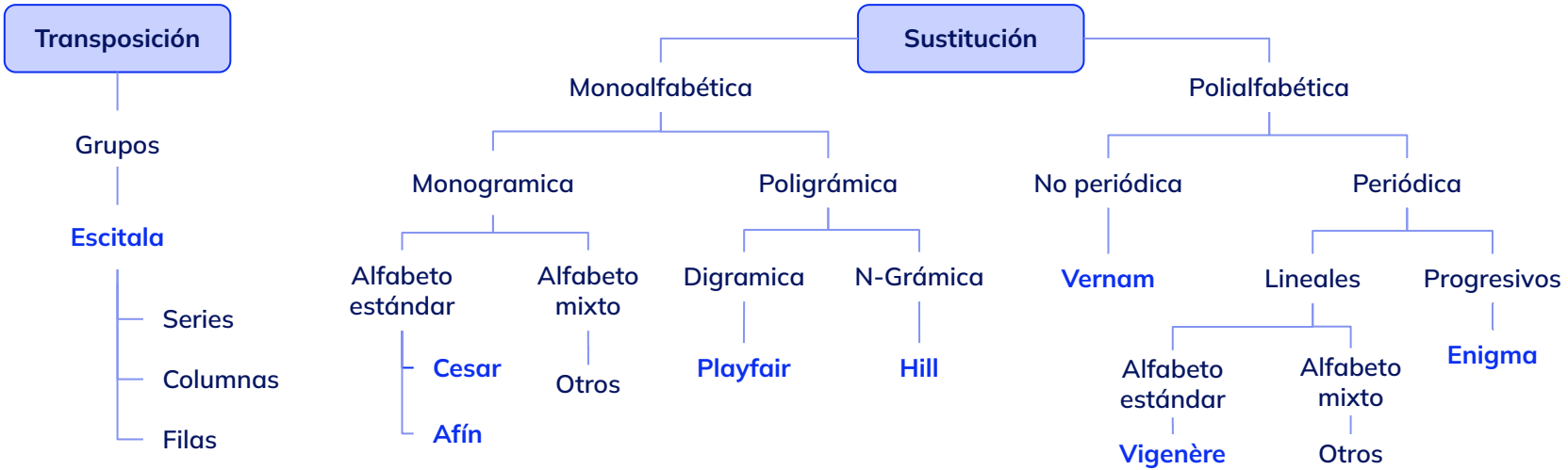
Atbash

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

Atbam

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

Clasificación de criptosistemas clásicos



Escítala

Se considera el **primer aparato criptográfico de uso militar** de la historia. Se remonta al siglo V a. C. y lo utilizaron los lacedemonios durante las guerras del Peloponeso, entre Esparta y Atenas, para enviar mensajes de manera segura.

Plutarco, el historiador y filósofo griego nacido en el siglo I, menciona en su obra Vidas paralelas cómo usaban los espartanos la escítala.

Ejemplo

- **Descifrar** el siguiente secreto:

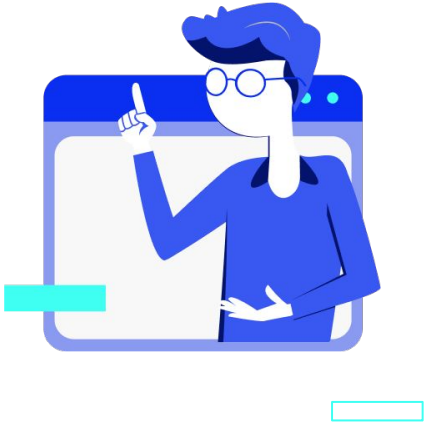
ABESASINCCCIIOTFNARLLAAA

- **Solución**: 8 vueltas de 3 letras cada una.

Criptograma: ABE SAS INC CCI IOT FNA RLL AAA

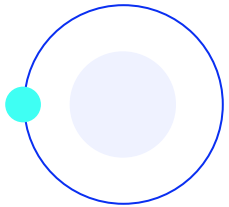
A S I C I F R A
B A N C O N L A
E S C I T A L A

Mensaje: ASÍ CIFRABAN CON LA ESCITALA



Trasposición por series

Los mensajes se ordenan como una serie o cadena de submensajes.



Ejemplo

Sean las series:

S1: 1, 2, 3 , 5, 7, 11, 13, 17, 19, 23 (números primos).

S2: 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26 (números pares).

S3 :9, 15, 21, 25, 27 (números impares).

- **Cifrar** el mensaje:

  ERRAR ES HUMANO PERDONAR DIVINO

- **Solución**:

  ERRRSAODNI AEHMNPROADVN UERIO

Transposición por columnas

Ejemplo

- **Cifrar** el mensaje con 6 columnas:

  M= NUNCA ES TARDE CUANDO LA DICHA ES BUENA

- **Solución**:

  NSCLA NUTUA EANAA DSXCR NIBXA DDCUX EEOHE X

N	U	N	C	A	E
S	T	A	R	D	E
C	U	A	N	D	O
L	A	D	I	C	H
A	E	S	B	U	E
N	A	X	X	X	X

Trasposición por filas

Ejemplo

- **Cifrar** el mensaje:

  C= MAPDDITOOERURNX de clave 3

- **Solución**:

  M=MIRA TU POR DONDE

M	A	P	D	D
I	T	O	O	E
R	U	R	N	X

Cifrado César

Le debemos a **Suetonio,** el historiador que vivió a caballo entre el siglo I y II y autor de *Vida de los doce Césares*, el conocimiento del **cifrado de Julio César,** ya que fue él quien nos dejó escrito cómo enviaba cartas a Cicerón y a otros romanos, utilizando un método sencillo pero efectivo.

Lo que hacía César era **sustituir cada letra por la que estaba en el abecedario tres posiciones hacia adelante.**

En la actualidad se ha denominado ***cifrado o código César*** a cualquier método o sistema que funcione de esta forma, sea cual sea el **desplazamiento a lo largo del alfabeto,** tres posiciones, como al inicio, o cualquier otra cifra.

Octavio Augusto, hijo adoptivo de Julio César, utilizaba este mismo método, si bien reducía el desplazamiento a una sola posición.

Ejemplo de una sustitución monoalfabética monográmica de alfabeto estándar.

- **Descifrar** lo siguiente:

M= FHVDU HÑHOS HUDGR UKDVL GRDVH VLPDG R

- **Solución**:

M= FHVDU HÑHOS HUDGR UKDVL GRDVH VLPDG

C= CESAR EL EMPERADOR HA SIDO ASESINADO

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	16	18	19	20	21	22	23	24	25	26	27
M	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Transformación afín

Utiliza aritmética modular. Sus ecuaciones generales son:

C = a * M + b (mod n)

M = a $^{-1}$ (C-b) (mod n)

Ejemplo

- Use la transformación afín C = 5 * M + 8 (mod 27) para **cifrar** el mensaje:

M = DABALE ARROZ A LA ZORRA EL ABAD

- **Solución**:

Ej: tomamos la primera letra del mensaje (D). Su índice o posición es. Si calculamos:

C = 5 * 3 + 8 = 23.

Si dividimos por 27 da 0 con resto 23, que es el índice de la letra W, luego, se cifra la letra D con la W.

C = WINIJ BIQQC DIJID CQQIB JINIW

¡Sigamos trabajando!