Criptografía

Profesor: Melvin Fernández Ch.

Video 2

fidélitas

Virtual

fidélitas Virtual

Historia y Evolución de la Criptografía

Módulo: 1

Historia de la criptografía

LA ESCITALA (SIGLO V a. c)

El primer caso de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta, por parte de los lacedemonios. El cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar el mensaje en un rodillo llamado escitala, de longitud y grosor prefijados.

Historia de la criptografía

fidélitas Virtual

- Con el paso del tiempo aparecen otras técnicas de cifra basadas en la sustitución de caracteres.
- Usaban jeroglíficos para adornar las tumbas egipcias donde contaban la historia del difunto.
- Los métodos de encriptación evolucionaron para ocultar información.
- Un método hebreo llamado ATBASH mapeaba las letras.

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

DUERMO FELIZ = WFVINL UVORA

Historia de la criptografía

fidélitas Virtual

- Julio César (100 AC – 44 AC) – definió el cifrado mono alfabético por Desplazamiento.

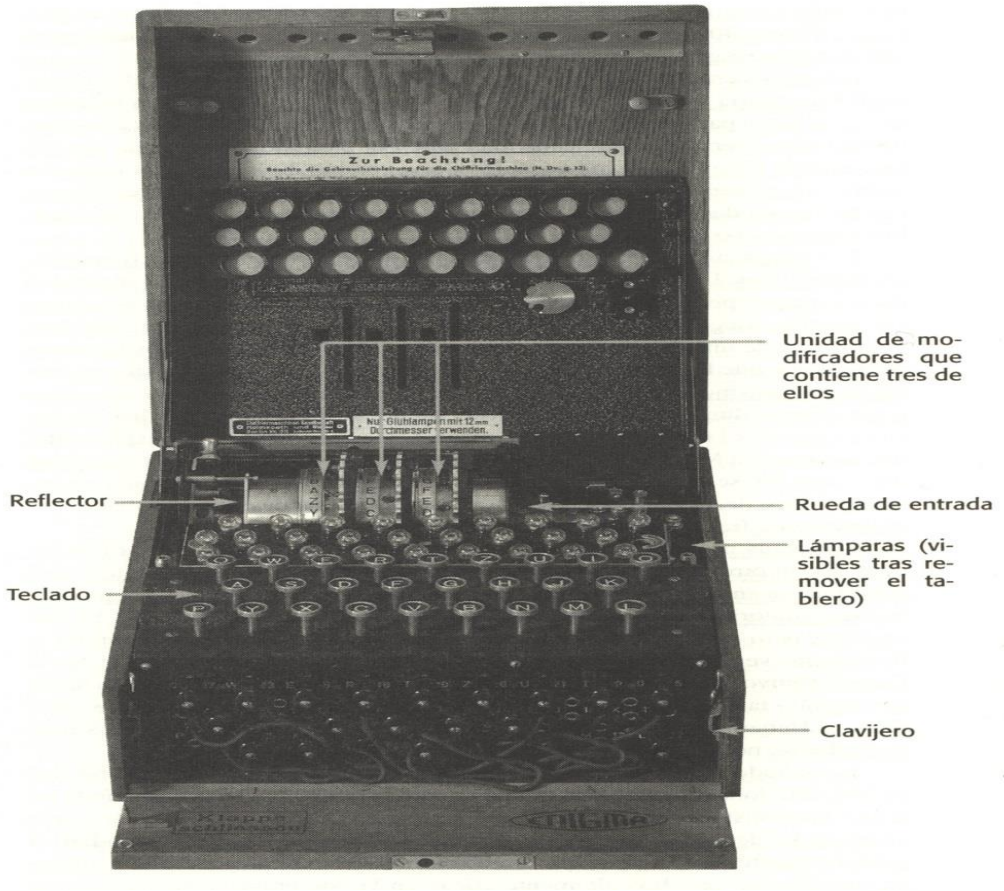
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

  - ROT13 se diseñó en 1980 con desplazamiento de 13 espacios. Se utilizó para esconder material que pudiera resultar ofensivo.

- Los algoritmos actuales más populares y seguros son:
  - ✓ 3DES – RSA – BlowFish – SHA1 – MD5

Historia de la criptografía

ENIGMA



- Creada en 1923.
- Utilizada en la II Guerra Mundial por el ejército alemán.
- Utiliza mecanismo de rotores.
- Permite codificar/decodificar el mensaje a encriptar.

Gracias

fidélitas Virtual