educación IT
CODE YOUR FUTURE

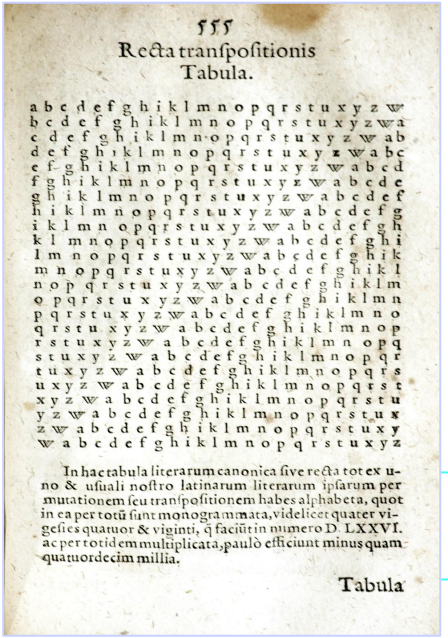
Criptografía y Blockchain

Módulo 1

Criptosistemas clásicos avanzados

Cifrado de Vigenère (1586)

- Es el **cifrador polialfabético** más conocido y utiliza el **mismo método que el cifrado César.**
- El **desplazamiento de caracteres** viene indicado por el valor numérico asociado a cada uno de los caracteres de una clave que se escribe cíclicamente bajo el mensaje.
- Suele utilizarse junto con la **tabula recta de Tritemio.**
- Supuso un gran avance que volvió obsoleto el criptoanálisis de aquella época.



ſſſ

Recta tranſpoſitionis Tabula.

a b c d e f g h i k l m n o p q r s t u x y z w
b c d e f g h i k l m n o p q r s t u x y z w a
c d e f g h i k l m n o p q r s t u x y z w a b
d e f g h i k l m n o p q r s t u x y z w a b c
e f g h i k l m n o p q r s t u x y z w a b c d
f g h i k l m n o p q r s t u x y z w a b c d e
g h i k l m n o p q r s t u x y z w a b c d e f
h i k l m n o p q r s t u x y z w a b c d e f g
i k l m n o p q r s t u x y z w a b c d e f g h
k l m n o p q r s t u x y z w a b c d e f g h i
l m n o p q r s t u x y z w a b c d e f g h i k
m n o p q r s t u x y z w a b c d e f g h i k l
n o p q r s t u x y z w a b c d e f g h i k l m
o p q r s t u x y z w a b c d e f g h i k l m n
p q r s t u x y z w a b c d e f g h i k l m n o
q r s t u x y z w a b c d e f g h i k l m n o p
r s t u x y z w a b c d e f g h i k l m n o p q
s t u x y z w a b c d e f g h i k l m n o p q r
t u x y z w a b c d e f g h i k l m n o p q r s
u x y z w a b c d e f g h i k l m n o p q r s t
x y z w a b c d e f g h i k l m n o p q r s t u
y z w a b c d e f g h i k l m n o p q r s t u x
z w a b c d e f g h i k l m n o p q r s t u x y
w a b c d e f g h i k l m n o p q r s t u x y z

In hac tabula literarum canonica ſive recta tot ex uno & uſuali noſtro latinarum literarum ipſarum permutationem ſeu tranſpoſitionem habes alphabeta, quot in ea per totũ ſunt monogrammata, videlicet quater vigeſies quatuor & viginti, q̃ faciũt in numero D. LXXVI. ac per totidem multiplicata, paulò efficiunt minus quam quatuordecim millia.

Tabula

Ejemplo

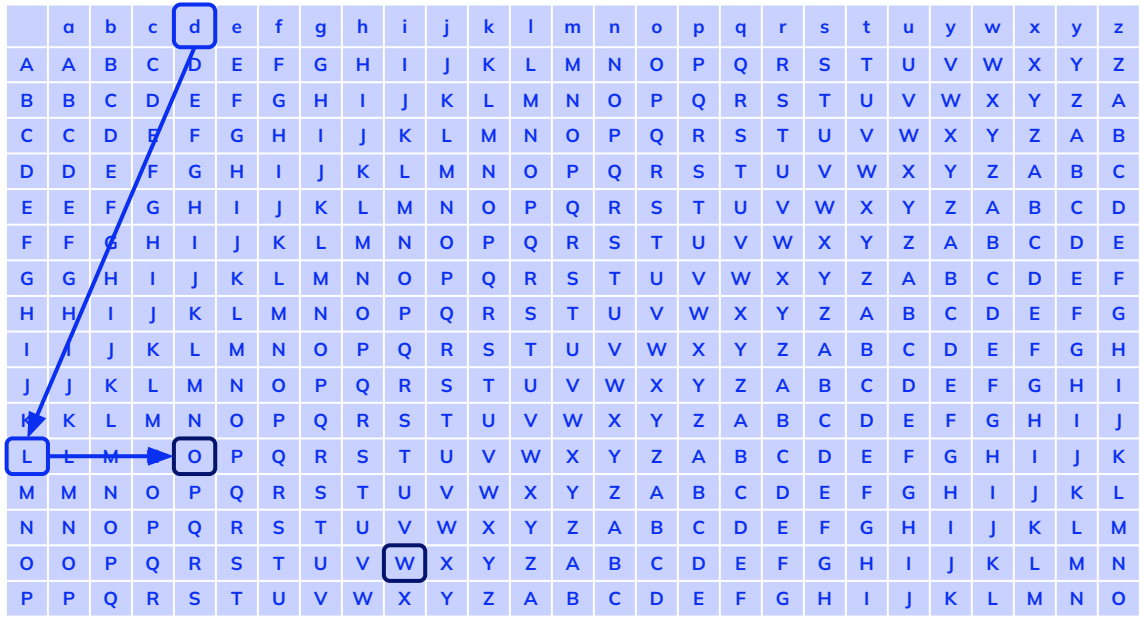
Cifrar:

DIEU PROTEGE LA FRANCE con K = LOUIS

Se toma la primera letra del texto claro (d) junto a la primera letra de la clave (L), luego se extrae la primera letra del criptograma buscando la intersección en la tabula recta.

Repitiendo el procedimiento se obtiene el **mensaje cifrado**:

OWYCHCCNMYPZUNJLBWM

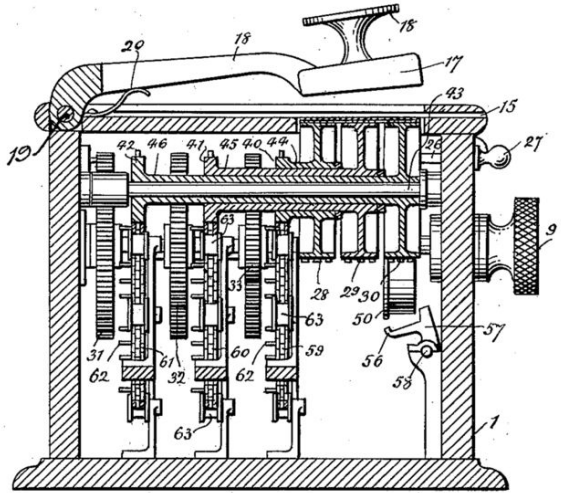


	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	y	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	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
N	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
O	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	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

d	i	e	u	p	F	o	t	e	g	e	l	a	f	r	a	n	c	e
L	O	U	I	S	L	O	U	I	S	L	O	U	I	S	L	O	U	I

Cifrado de Hill (1929)

- En 1929 el matemático **Lester Hill** publica en Nueva York un artículo donde propone el **cifrado mediante el uso del álgebra, en particular las matrices.**
- No era fácil de implementar y no pudo competir con la máquina Enigma de los alemanes.
- Bajo ciertas condiciones presenta una alta seguridad y puede implementarse en computadoras actuales.



Cifrado Vernam (1917)

- **Gilbert Vernam** diseñó un sistema criptográfico para comunicaciones telegráficas seguras basado en los 32 códigos Baudot de los teletipos de AT&T, compañía para la cual trabajaba.
- Propuso el uso de una clave continua para cifrar el mensaje carácter por carácter.
- Junto a **Joseph Mauborgne** (capitán de la US *Army Signal Corps*) idearon la **libreta de un solo uso *(one time pad)*** para dificultar el criptoanálisis.
- Vernam patentó estas ideas, conocidas como el *cifrado Vernam,* en 1919, y utilizó lo que se conoce habitualmente en el mundo de la computación como operación XOR o, dicho de otro modo, un OR exclusivo *(exclusive OR),* aunque él no usó entonces esta terminología.
- El sistema diseñado por Vernam funcionaba sin problemas y este tenía a su alcance la capacidad para construir los dispositivos de envío y recepción que implementaran su idea. Es más, la facilidad de uso del sistema era una de sus ventajas.

- **Claude Shannon** demostró en la década del ‘40 que el sistema tenía la **propiedad del secreto perfecto.**
- En aquel documento en el que trataba del sistema de cifrado perfecto es donde Shannon utilizó por primera vez una expresión por la que ha pasado a la historia de la ciencia: **Teoría de la Información.**

El cifrado de Vernam es el **único algoritmo criptográfico conocido irrompible** si se dan una serie de condiciones:

1. Libretas de un solo uso perfectamente aleatorias.
2. Generación e intercambio de libretas de modo seguro.
3. La libreta tiene que ser igual o más larga que el mensaje.
4. Debe asegurarse la destrucción segura de la libreta tras su utilización

Ejemplo

Cifrar el mensaje:

M = BYTES con la clave K = VERNAM

Solución:

B + V = 11001 + 11110 = 00111 = U

Y + E = 10101 + 00001 = 10100 = H

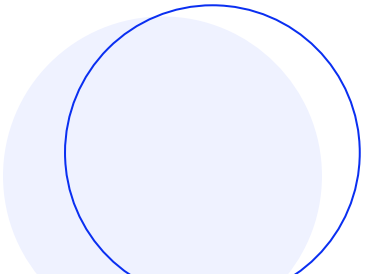
T + R = 10000 + 01010 = 11010 = G

E + N = 00001 + 01100 = 01101 = F

S + A = 00101 + 00011 = 00110 = I

C = UHGFI

- El problema que persiste con este cifrado es la transmisión segura de la clave.
- Habrá que esperar hasta 1977 cuando se presenta el esquema de cifrado de asimétrico o de clave pública para solucionar el problema del intercambio de la clave.

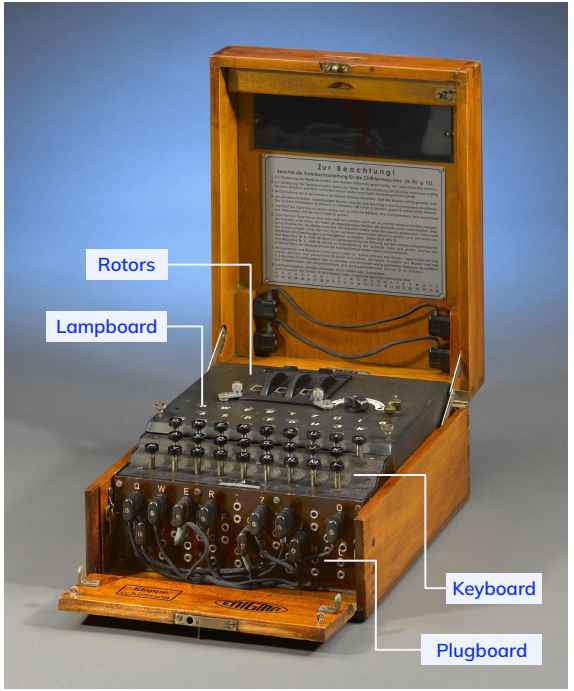


Las máquinas de rotores (1915)

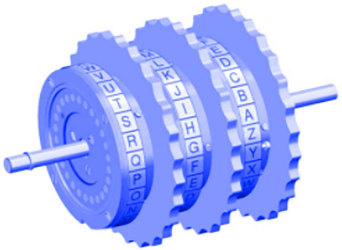
- En 1915 dos oficiales navales holandeses, **Theo A. Hengel y Rudolf Spengler**, fueron los primeros en idear una máquina de rotores para cifrar. Construyeron un prototipo que presentaron a la armada holandesa, aunque esta no apoyó la idea.
- En 1917 **Edward Hugh** Hebern patentó una máquina con un rotor que podía ser insertado en ambas orientaciones y así cifraba y descifraba.
- A partir del invento de Hebern, **William Friedman** mejoró el diseño y creó la máquina conocida como **SIGABA** o **ECM Mark II**. Esta incorporaba la rotación irregular de rotores, lo que la hacía más segura al aumentar la complejidad del texto cifrado.
- En 1918, **Arthur Scherbius y Richard Ritter** solicitaron la patente de una máquina de cifrar basada en discos móviles que variaban de posición durante el cifrado. Era la idea inicial de **Enigma**.

La máquina Enigma

- Una máquina Enigma tenía cuatro componentes principales: un teclado, los rotores un tablero de luces y un reflector.
- Las Enigmas militares sumaban un *plugboard* en la parte frontal.
- Teniendo en cuenta que una máquina Enigma M3 consta de tres rotores (elegidos de un conjunto de cinco), la adición de los ajustes del rotor con 26 posiciones y el *plugboard* con diez pares de letras conectadas significa que disponía de un total de 158, 962, 555, 217, 826, 360, 000 (casi 159 quintillones) configuraciones diferentes.



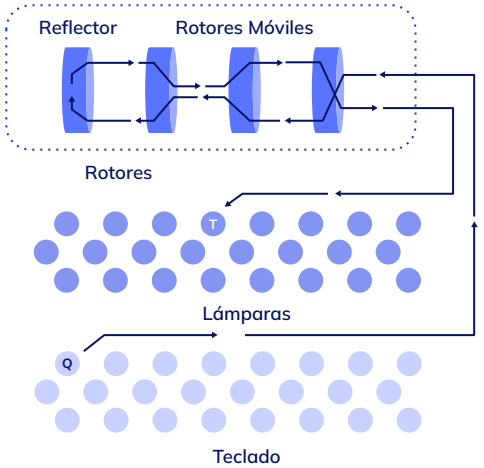
- El motor de cifrado se basaba en lo que se denominaba un *rotor*, que no es otra cosa que un disco con puntos metálicos, conectores eléctricos, en ambas caras.
- La versión más sencilla constaba de tres rotores conectados entre sí. Estos rotores tenían 26 conectores en cada una de sus caras, correspondientes a 26 letras.
- Los tres rotores no estaban fijos en la máquina, sino que se podían sustituir unos por otros. De igual forma, tampoco estaba establecido el orden de los mismos, por lo que el número de combinaciones se multiplicaba.



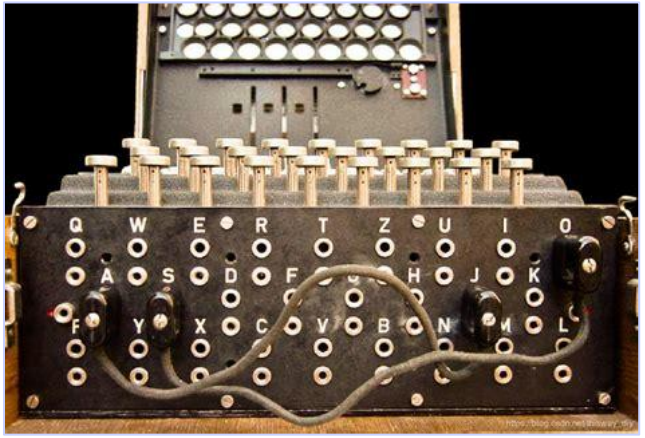
Motor de cifrado

Funcionamiento

- La corriente eléctrica entra en el primer rotor por un conector y, gracias al cableado interno, sale por un conector de la cara opuesta.
- El conector de salida del primer rotor está en contacto con un conector de entrada del segundo rotor, que a su vez está cableado hacia un conector de salida.
- Ocurre algo similar con el tercer rotor, y la salida de este llevaría a una letra del panel de luces, ya que cada conector de la cara de salida del último rotor activa una luz distinta.
- El reflector añadía complejidad y seguridad a la máquina, pero también tenía impedía que una letra en el texto en claro pudiera cifrarse como ella misma.



- Las Enigma militares tenían añadido un tablero de conexiones en la parte frontal que multiplicaba las opciones de configuración de la máquina y, por tanto, también su seguridad (el *plugboard*).
- Este tablero o panel de conexiones tenía 26 clavijas, cada una correspondiente a una letra, y había 10 cables que podían unir dos de estas letras como el operador quisiera.
- Durante la Segunda Guerra Mundial hubo diferentes versiones de Enigma, con algunos cambios. Por ejemplo, había Enigma con cuatro rotores.



¡Sigamos trabajando!