






Criptografía asimétrica

Integrantes:

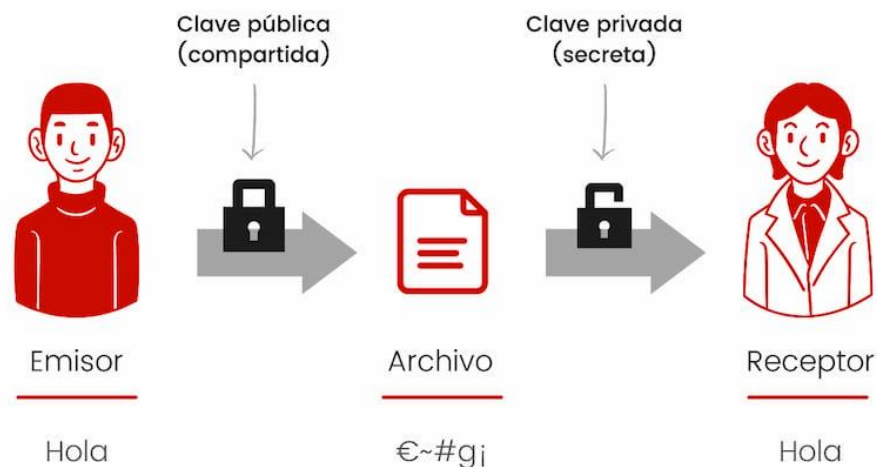
-  *Osorio Juárez Montserrat Judit*
-  *Pérez Ruiz Diego Enrique*
-  *Ramírez Chávez Nelly Jacqueline*
-  *Ramírez Espinoza Andrea Celeste*
-  *Resendiz Diaz Rebeca*

Grupo: 604 Informática

¿Qué es?

También llamada criptografía de clave pública, método que usa un par de claves para el envío de mensajes.

Garantiza que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.



Funcion



El sistema utiliza dos llaves para cifrar un mensaje: una llave pública y otra privada. Para encriptar un mensaje, se utiliza la llave pública del receptor (que se conoce a priori) y la privada del emisor. Para desencriptarlo se utiliza la llave pública del emisor (que se envía junto al mensaje cifrado) y la llave privada del receptor. La llave privada es secreta y es la única que permite descifrar los mensajes.

Algoritmo Cesar

También conocido como cifrado por desplazamiento, es una técnica de codificación muy simple.



Reemplaza una letra en el texto original por otra letra que se encuentra en un numero fijo de posiciones mas adelante en el alfabeto.

Ejemplo

HOLA

Para este reemplazaremos las letras que se encuentren 3 lugares después de la letra original.

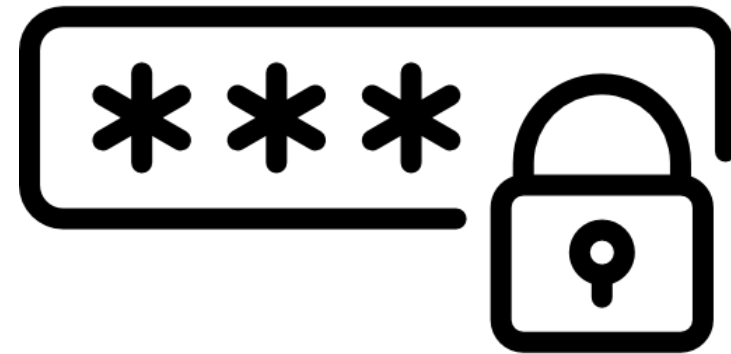
A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26	27

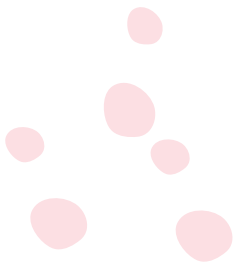
Ejemplo

HOLA

H se sustituye por K
O se sustituye por R
L se sustituye por O
A se sustituye por D



Entonces HOLA seria **KROD**



Gracias por su atención :3

