Bienvenidos a la cuarta clase de Hacking desde cero, por Roadd (o sea, yo :D).

Desde que los black hat acechan al mundo del hacking, se generaron distintas maneras de **protección** de los **datos**. Y **hoy** en día, la **información** es lo más rentable que existe en cualquier tipo de mercado, y se paga realmente bien.

Entonces, suponiendo que ellos ya **robaron** nuestros datos. ¿Cómo hacemos para que **no** puedan ser **leídos**?

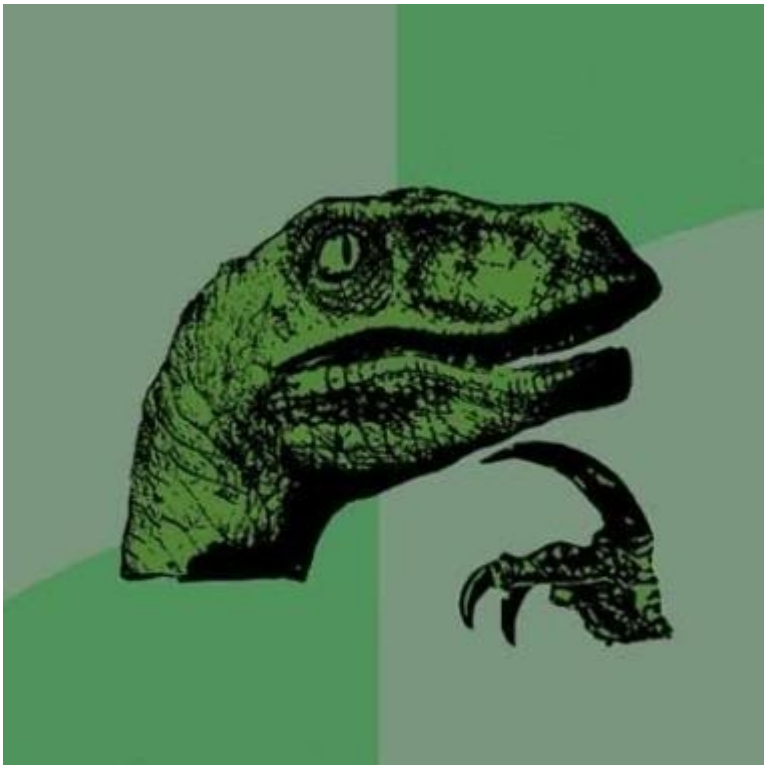
La respuesta, hoy en día aparece fácil en la mente de la nueva generación. Pero pensemos en épocas en las que los romanos debían cruzar un mensaje por un largo trecho, sabiendo que los mensajeros eran carne de cañón, y al mismo tiempo estar seguros de que el mensaje no podría ayudar de ninguna manera al enemigo.

“Bueno, lo mandar cifrado al mensaje. Con todos simbolitos raros que sólo ellos

sepan leer.”

Jajajajaj. Bueno Manolito, no estás más cerca de la realidad porque te chocarías contra ella.

Sí, hacían eso.



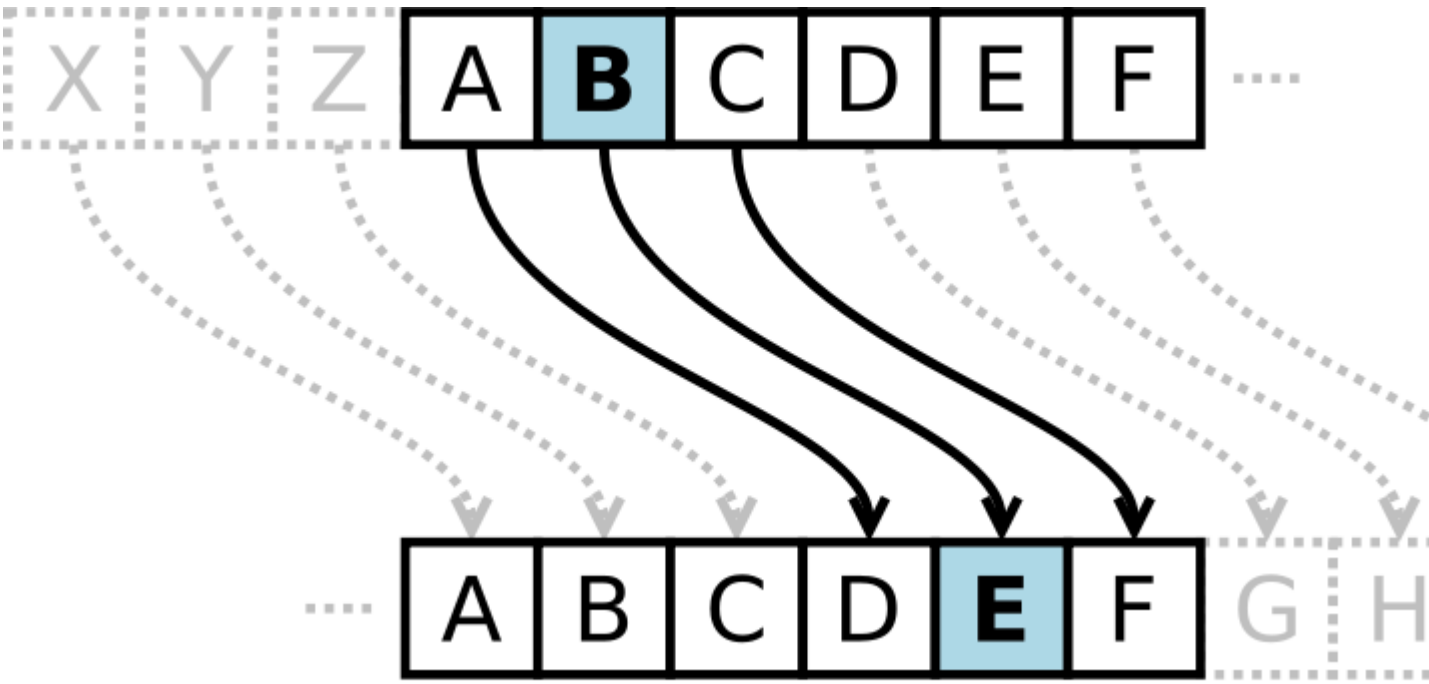
Cifrado.

El cifrado de la información, es la clara herramienta que buscamos. Pero, hay un inconveniente. Nosotros **no** deberíamos usar siempre la **misma** manera de **cifrado** porque sería **inseguro**. Imaginemos que el enemigo de roma interceptaba 4 mensajes y lograba descifrar uno. Si siempre usaran la misma manera de cifrado, el emperador no habría durado demasiado en decirle cuáles eran sus planes de ataque. Así que ideemos una manera de cifrado que **varíe** según la **clave** que le pongas. Y allí nació...

¡El Cifrado César! (también llamado cifrado por desplazamiento) Éste método es **rudimentario** y **fácil** de entender. Vamos a explicarlo y luego realizar algunos ejercicios.

El cifrado se compone de 2 **elementos**: el **mensaje**, y la **clave**. El **mensaje** estaba **encriptado**, sustituido por un abecedario que nadie puede leer a simple vista, aunque siempre conformado por letras. Y la **clave** era un número **entero** que variaba entre el 1 y el 25.

La clave, era la que decía cuantas letras se desplazaba el abecedario, de tal manera que si n=2 (ésta es la clave), A=C, B=D, y etcétera. Para descifrar el mensaje, sólo hay que aplicar la manera inversa.



Vamos con los ejemplos que van a entenderlo mejor.

Desplazamiento

0	A B C D E [..] X Y Z
1	B C D E F [..]+1 Y Z A
8	I J K L M [..]+8 F G H

Mensaje cifrado Mensaje descifrado

“ipmb” n=1 ----------> “hola”

“Kqnzilw” n=8 ----------->”Cifrado”

Ejercicios (les dejo adjunto, además, un excel con todas los desplazamientos posibles:

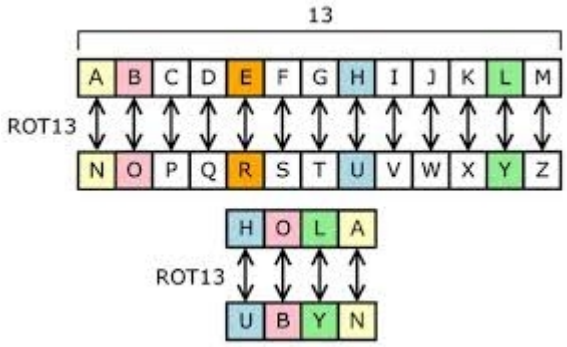
Cifrar:

“Hola mundo” ---------->n=3

Descifrar:

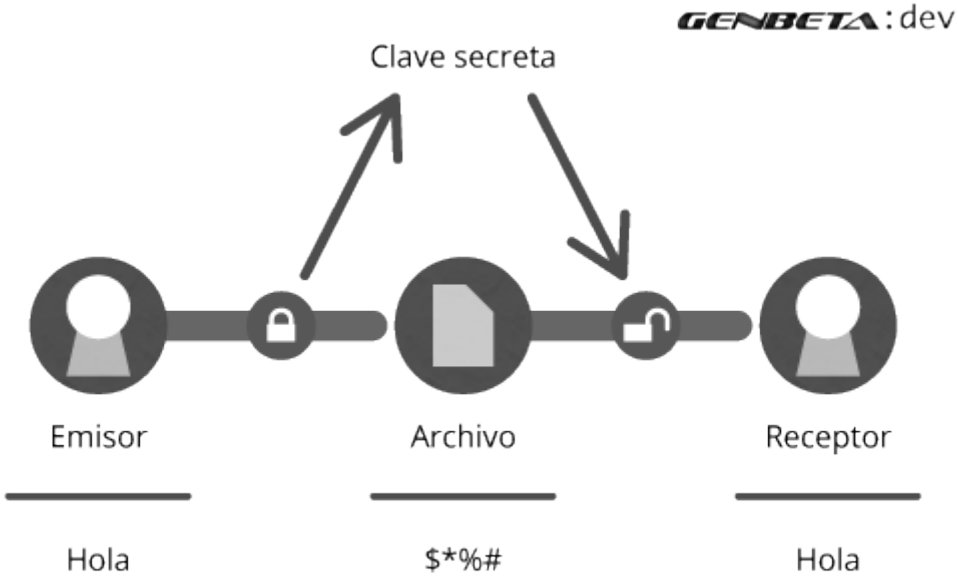
“Anaf Wtfii” n=5 ---------->

“Jvirj cf hlv uvsrj jvi, f ef jvirj erur.” n=17 ---------->



Obviamente, que este cifrado es simple incluso para un estudiante de primaria. Luego veremos cifrados que no vamos a poder calcular.

Este tipo de cifrado se le denomina, encriptación simétrica, porque usa la misma clave para cifrar y descifrar.



“Todo re lindo, che. Pero supongo que los romanos debían pasar el número para descifrar el mensaje. Eso era todo un tema de discusión ¿No?”

Claro Manolo, la **clave** es indispensable para pasar y al mismo tiempo un **problema**. Es un peligro que alguien que conozca tu forma de cifrado, robe ambas cosas. En ese caso estarías perdido. Incluso con robar 2 mensajes o más con sus respectivas claves, hay probabilidades de que empieze a entender tu técnica.

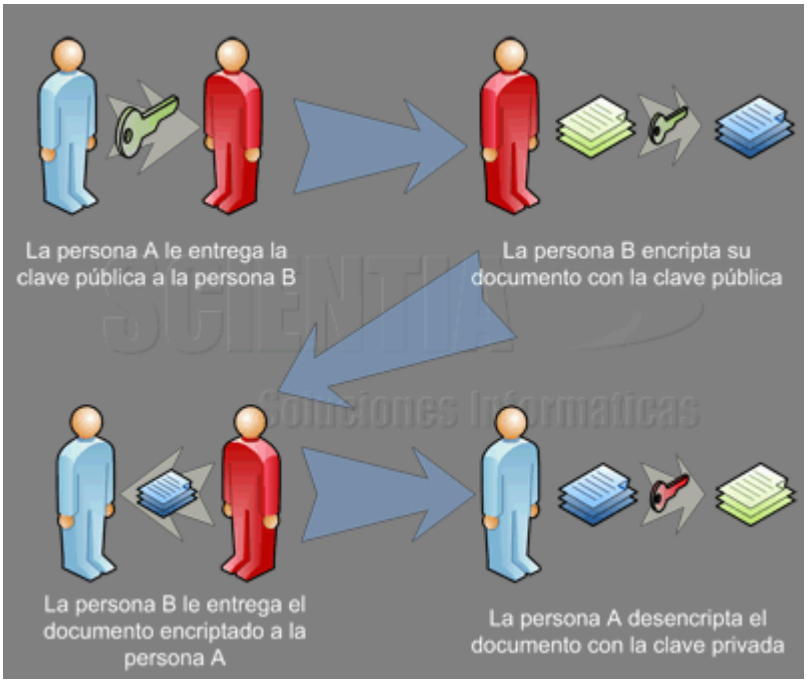
Ésto ya fue pensado, y crearon lo que se denomina **encriptación asimétrica**. Este tipo de cifrado esta compuesta por **2 claves: la clave privada y la clave pública.**

La clave **privada** es, como dice su nombre, privada. **Secreta**, incompartible. Únicamente debe saberla una persona.
La clave **pública** la pueden saber **todos**.

“Pero esto haría re fácil a cualquiera leer tus archivos.”

Manolo, aquí hay una trampa. La **clave pública**, sirve únicamente para **cifrar** un mensaje y no para descifrarlo. Así que la **clave privada** sirve únicamente para **descifrar** el mensaje.

Es decir que cualquiera puede mandarte un mensaje cifrado pero nadie mas que vos puede descifrarlo.



Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
