**Cifrado Vernam**

**Resumen:**

Cifrado de flujo que usa una clave constituida por una sucesión de símbolos (bits o caracteres) llamada serie cifrante, operando o-exclusivo cada símbolo de ésta con el correspondiente del texto en claro. Debido a la definición de la función o exclusivo, el descifrado se realiza, igualmente, operando con dicha función cada bit de la misma serie cifrante con el correspondiente del texto cifrado. Si la serie cifrante no se repite, es aleatoria, y de longitud igual, al menos, al texto a cifrar éste cifrado alcanza el secreto perfecto. Además, es el único que verifica tal condición. Este cifrado fue ideado en 1971 por Gilbert S. Vernam -ingeniero de la compañía ATT- para ser usado en transmisión telegráfica con el código Baudot.

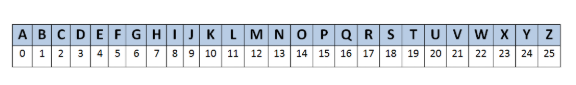
**Introducción:**

En terminología moderna, un cifrado de Vernam es un cifrado de flujo en el que el texto en claro se combina, mediante la operación XOR, con un flujo de datos aleatorio o pseudoaleatorio del mismo tamaño, para generar un texto cifrado.  
El uso de datos pseudoaleatorios generados por un generador de números pseudoaleatorios criptográficamente seguro es una manera común y efectiva de construir un cifrado en flujo. El RC4 es un ejemplo de cifrado de Vernam que se utiliza con frecuencia en Internet. Para dar un ejemplo realizaremos el cifrado en 4 pasos

Pasos:

**1:le damos valor numérico al alfabeto:**

Imagen1



**2: pasamos el alfabeto a binario:**

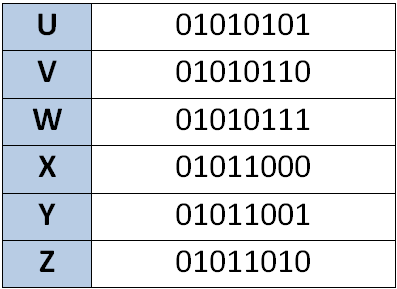
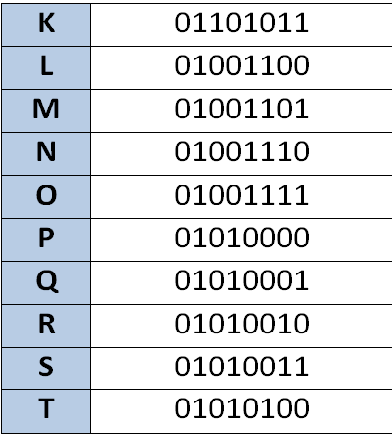
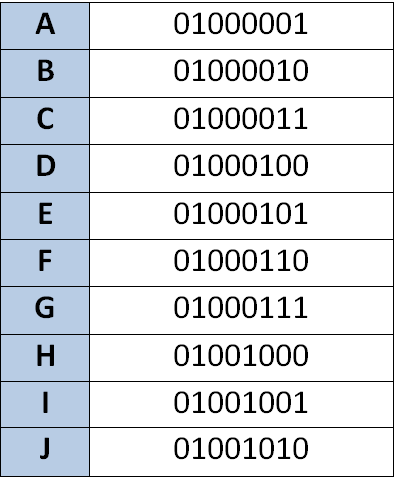


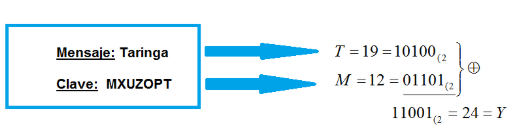
Imagen2

**3: elegimos una clave y mensaje y seguimos los pasos 1 y 2 para esta**:

Para este caso usaremos el mensaje: Taringa y la clave :mxuzopt

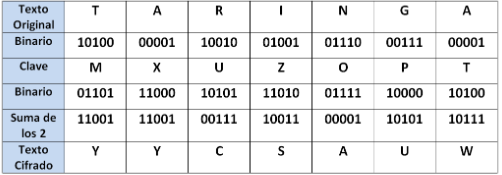
**4: juntamos los primeros caracteres del mensaje y la clave y juntamos sus primeros 5 digitos binarios**

Imagen3



**Y así seguimos con los demás hasta que nos quede algo así:**

Imagen4



**Referencias:**

* <https://www.taringa.net/+crypto/aprende-criptografia-cifrado-de-verman-con-este-post_hrjd2:imagen1,imagen2,imagen3,imagen4>
* <https://es.wikipedia.org/wiki/Cifrado_Vernam>
* <https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=219.html>