**UNIVERSIDAD AUTÓNOMA GABRIEL RENE MORENO**



**PROYECTO #1**

**NOMBRE:** ABASTO BERBETTY RODRIGO

**REGISTRO:** 210000491

**MATERIA:** CRIPTOGRAFIA Y SEGURIDAD

**FECHA:** 19 – JUN – 2018

SANTA CRUZ – BOLIVIA

1. **CIFRA DE DESPLAZAMIENTO**
   1. **PURO**

Tal vez el algoritmo de cifra clásica más conocido y popular sea el del César, a pesar de que su seguridad dejará mucho que desear como veremos en esta lección.

  
  
Figura 1.1. Cayo Julio César.

El primer uso documentado de una cifra monoalfabética por sustitución con propósitos militares aparece en el documento "La guerra de las Galias" de Julio César. En dicho libro, Julio César describe cómo envía un mensaje cifrado a Cicerón, que se encontraba sitiado y a punto de rendirse, aplicando una sustitución simple a las letras del texto en claro de forma que el mensaje fuera ininteligible para el enemigo.

Aunque en aquella ocasión César sustituyó las letras romanas por letras griegas, es común asociarle a su sistema de cifra un desplazamiento de 3 espacios a la derecha en el alfabeto, tal y como lo describe Suetonio en su libro "Vidas de los Césares" en la entrada LVI sobre Cayo Julio César.

De esta manera, el alfabeto de cifrado para las 27 letras en mayúsculas del castellano quedaría como se muestra en la figura.

http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/imagenes/AlfabetoCesar.png  
  
Figura 1.2. Alfabeto de cifrado del César mod 27.

Así, la famosa frase VENI VIDI VICI, atribuida Julio César también por Suetonio, se cifraría con este método y el alfabeto mostrado en la figura anterior como:

**M = VENI VIDI VICI             C = YHPL YLGL YLFL**

La cifra del César tiene por tanto una representación matemática para letras mayúsculas en castellano del tipo:

**C = M + 3 mod 27**

En donde M es el código de la letra del texto en claro que se cifra y C el criptograma resultante.

Por lo tanto, de forma genérica diremos que el cifrador del César con un desplazamiento de 3 espacios, es un caso particular de un cifrado de sustitución por desplazamiento puro de la forma:

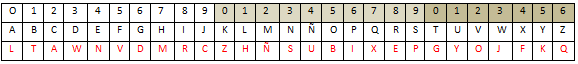
**C = M + b mod n**

Donde **n** es el tamaño del alfabeto y del cuerpo de cifra y **b** es la constante de desplazamiento. Observa que dicha constante puede tomar valores desde 1 hasta n-1, en tanto un desplazamiento b = 0 o bien b = n significaría enviar el texto en claro.

* 1. **PURO CON PALABRA CLAVE**

Seguramente habrás contestado de forma correcta a la pregunta del apartado anterior: *la cifra del César o por desplazamiento puro tiene una cantidad de claves tan baja que su fortaleza es mínima*. En el caso de trabajar en módulo 27, los valores de dicha clave serían sólo 26, esto es, los números 1 al 26, por lo que un simple ataque desplazando sucesivamente las letras del criptograma, bien hacia la izquierda o hacia la derecha, daría con el texto en claro en el peor de los casos en el vigésimo sexto intento. Aunque estemos hablando de criptografía clásica, este valor valor es ridículo.

Para aumentar algo la fortaleza de la cifra, una solución es no usar un desplazamiento constante sino variable y aleatorio entre las letras. En otras palabras, reordenar el alfabeto sin seguir un orden preestablecido ni una lógica, tal y como se muestra en la figura 1.3.

  
  
Figura 1.3. Alfabeto de cifrado por desplazamiento sin orden preestablecido.

Como se observa, para cifrar la letra **A** del texto en claro le aplicamos un desplazamiento de 11 espacios a la derecha (obteniendo la letra **L**); al cifrar ahora la letra **B**, ese desplazamiento será de **T** - **B** = 20 - 1 = 19 espacios a la derecha; para la cifra de la letra **C**, el desplazamiento será igual a **A** - **C** = 0 - 2 = 25 espacios a la derecha (recuerda que estamos trabajando en módulo 27), etc. Así, todos o una gran mayoría de los desplazamientos serán distintos.

Como es obvio, en este caso habrá muchas más combinaciones posibles de alfabetos de cifrado que la indicada en la figura 1.3. Básicamente, los posibles alfabetos de cifrado serán aquellos que formen todas las posibles combinaciones de letras en dicho alfabeto de 27 elementos, dando lugar el valor conocido como factorial de 27:

27! = (27 \* 26 \* 25 \* 24 … 4 \* 3 \* 2 \* 1) = 10.888.869.450.418.352.160.768.000.000

1. **CIFRA POR TRANSPOSICIÓN POR:**
   1. **GRUPOS**

Si el texto en claro se agrupa en bloques de un cierto tamaño y sobre ese bloque se realiza alguna operación de permutación que se repite periódicamente, el sistema de cifra se conoce como transposición por grupos. Por ejemplo, si agrupamos el texto en claro en bloques de 8 letras y estos bloques sufren la permutación 13572468, es decir en cada bloque se transmiten primero las letras en posiciones impares de izquierda a derecha (1357) y a continuación las letras de las posiciones pares también de izquierda a derecha (2468), que obviamente son las que quedan de ese conjunto, el mensaje UN SECRETO ALGO EXTRAÑO se cifraría de la siguiente manera:

Texto en claro en bloques de 8 letras: UNSECRET OALGOEXT RAÑOXXXX (siendo XXXX el relleno)

Texto cifrado en bloques de 8 letras: USCENERT OLOXAGET RÑXXAOXX

Texto cifrado en formato group by five: USCEN ERTOL OXAGE TRÑXX AOXX

* 1. **SERIES**

Otra posibilidad es realizar una cifra no periódica utilizando series. Esta forma de cifra puede alcanzar una mayor fortaleza, pero como contrapartida requiere recorrer previamente todo el texto en claro para comenzar a cifrar.

Por ejemplo, se podría cifrar el texto de 22 caracteres AHORA CIFRAMOS POR SERIES usando primero la serie de números primos (2, 3, 5, 7, 11, 13, 17, 19), después los números pares (4, 6, 8, 10, 12, 14, 16, 18, 20, 22) y, por último, el resto de números no utilizados (1, 9, 15, 21). Es decir, se reordenan las letras del texto en claro según el siguiente orden:

Orden de permutación: 2, 3, 5, 7, 11, 13, 17, 19, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 1, 9, 15, 21

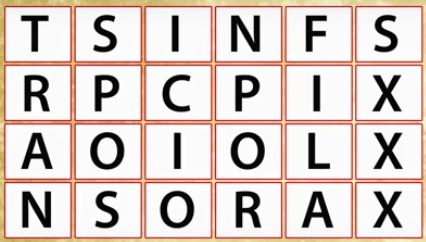
http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/imagenes/CifraPorSeries.jpg

Quedando el criptograma así: HOAIM SSRRC FAOPR EISAR OE.

* 1. **FILAS**

Si un texto en claro se escribe letra a letra hacia abajo con un nivel Fl de filas y luego se lee el resultado por filas de izquierda a derecha, diremos que se trata de una cifra por permutación de filas.

La figura 2.2 muestra un sistema de cifra por permutación de filas.

  
  
Figura 2.2. Cifrador por permutación de filas.

Observa que se escribe el texto en claro hacia abajo, en columnas, definiendo previamente con cuántas filas Fi se va a cifrar el texto en claro. En el ejemplo se han definido 4 filas de forma que si el mensaje a cifrar es M = TRANSPOSICION POR FILAS, éste se escribe de arriba hacia abajo como TRAN, SPOS, ICIO, NPOR, FILA, SXXX. Como se observa, si nos quedan cuadrículas en blanco, éstas se rellenan con una letra poco común que se haya asignado previamente como de relleno; en nuestro caso se ha elegido la letra X.

Un sistema similar de relleno se usará en los sistemas de cifra moderna conocidos como simétricos por bloques, como sería el caso por ejemplo del DES, el IDEA, el AES, etc. En estos sistemas el relleno del último bloque a cifrar se realizará mediante un conjunto de bits en 0, varios bytes indicando cada uno el número de bytes que faltan para completar ese último bloque, etc.

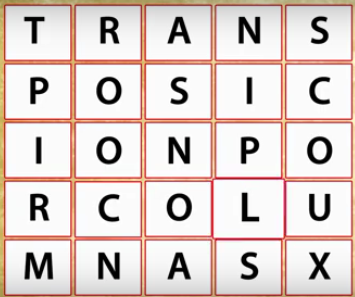
Hecho esto y como el cifrado es por filas, vamos leyendo las 4 filas que se han definido, ahora sí de izquierda a derecha, dando como resultado al agruparlo en bloques de 5 letras al criptograma C = TSINF SRPCP IXAOI OLXNS ORAX.

Observa que, dependiendo de la longitud del texto en claro y del número de filas que vamos a utilizar como clave para la cifra, obtendremos el número de columnas de la matriz resultante. En este ejemplo como el texto en claro TRANSPOSICION POR FILAS tenía 21 letras, al dividirlo por la clave 4 filas obtenemos 21/4 = 5,25 es decir 6 columnas (como se aprecia en la figura 2.2) y la última de ellas con relleno al darnos esa división un número con decimales.

* 1. **COLUMNAS**

Si el texto en claro se escribe ahora por filas, letra a letra de izquierda a derecha y hasta un nivel de columnas Cl, y luego se lee el resultado por columnas, hablaremos de una cifra por permutación de columnas.

La figura 2.3 muestra un sistema de cifra por permutación de columnas.

  
  
Figura 2.3. Cifrador por permutación de columnas.

Observa que ahora se escribe el texto en claro de la forma común a como lo hacemos, esto es de izquierda a derecha y en filas, definiendo previamente con cuántas Columnas Cl se va a cifrar el texto en claro. En este ejemplo se ha definido como clave 5 columnas, de forma que si el mensaje a cifrar fuese M = TRANSPOSICION POR COLUMNAS, éste se escribe de izquierda a derecha como TRANS, POSIC, IONPO, RCOLU, MNASX.

Para obtener el criptograma, al ser un cifrado por columnas, leemos las 5 columnas por orden obteniendo C = TPIRM ROOCN ASNOA NIPLS SCOUX.

Aunque no suele ser muy habitual, en este ejemplo ha coincidido el número de las columnas con el número de las filas, dando lugar a una matriz cuadrada.

* 1. **ZIG-ZAG**

Si el texto en claro se escribe formando una figura típica de una valla de campo, estaremos frente a una cifra de permutación por vallas o rail fence. El número de raíles o líneas internas de esa valla será la clave.

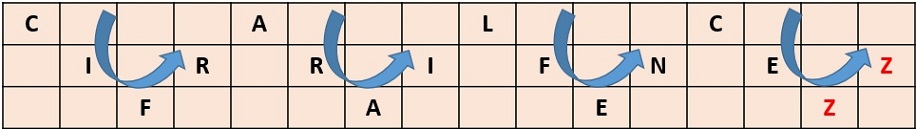
La figura 2.5 muestra el cifrado en valla del texto en claro M = CIFRA RAIL FENCE, definiendo 3 líneas o raíles en esa valla imaginaria, la línea superior, la línea interior y la línea inferior. Por lo tanto, vamos escribiendo el texto en claro haciendo un zig-zag y recorriendo dicha valla como si fuese una onda que se propaga.

  
  
Figura 2.5. Cifrador por vallas o rail fence.

Terminado de escribir el texto en claro, vamos leyendo cada fila de arriba hacia abajo y de izquierda a derecha, obteniendo el criptograma C = CALC IRRIFNE FAE = CALCI RRIFN EFAE.

Observa que en este caso, en principio no sería necesario incluir relleno, puesto que debido a la forma en que se descifra el criptograma esto no daría lugar a dudas sobre el mensaje en claro que esconde, siempre y cuando sigamos la misma figura de valla usada en la cifra. No obstante, veremos que sí es recomendable incluir rellenos de manera que se formen olas u ondas completas, que permiten obtener el texto en claro más fácilmente.

Como en este cifrado la forma de la figura con la cual se cifra generará olas, que se definirán en el siguiente párrafo, si fuera el caso habrá que introducir un relleno para que existan n olas completas, usando por ejemplo la letra Z para dicho cometido. Por lo tanto, para que se cumpla que la cifra tenga n olas exactas y todas del mismo tamaño, el cifrado de la figura 2.5 deberá tener un relleno de dos letras Z como se muestra en la figura 2.6.

  
  
Figura 2.6. Cifrador por vallas o rail fence con relleno por olas.

Siguiendio la figura 2.6, se denominará ola a la forma que describe un recorrido, precisamente en forma de ola invertida, desde el carácter superior, descendiendo hasta el fondo de la valla y subiendo nuevamente hasta llegar al carácter inmediatamente anterior donde este recorrido se vuelve periódico, o bien comienza una nueva ola. En el caso de la figura 2.6, se observan 4 olas completas. Estas son: la ola 1 formada por CIFR, la ola 2 formada por ARAI, la ola 3 formada por LFEN y la ola 4 formada por CEZZ, donde ZZ es el relleno aplicado.

El criptograma resultante será C = CALC IRRIFNEZ FAEZ = CALCI RRIFN EZFAE Z.

Es fácil comprobar que para 2 raíles las olas tendrán 2 elementos, para 3 raíles las olas tendrán 4 elementos, para 4 raíles las olas tendrán 6 elementos, para 5 raíles las olas tendrán 8 elementos, para 6 raíles las olas tendrán 10 elementos, etc. Es decir, el número de elementos de la ola vendrá dado por la siguiente expresión:

Elementos de una ola = (número de raíles x 2) - 2

1. **CIFRA POR SUSTITUCIÓN**
   1. **MONO ALFABÉTICA**

En una cifra afín habrá dos variables, la constante de decimación a y la constante de desplazamiento b. Por lo tanto, en este caso vamos a plantear un sistema de dos ecuaciones independientes con dos incógnitas, asignando (en primera instancia) la letra más frecuente del criptograma a la letra E del texto en claro, y la segunda letra más frecuente del criptograma a la letra A; esto es, a las dos letras más frecuentes de nuestro alfabeto.

Si el ataque no prospera con estas correspondencias, se buscarán otras como por ejemplo suponiendo que la A es más frecuente que la E en el texto en claro, o bien elegimos otras letras del criptograma. No es recomendable elegir letras al azar para comenzar el criptoanálisis por frecuencias; las letras que más información nos entregarán serán las 3 o 4 más frecuentes del alfabeto: E, A, O, S.

Supongamos que las dos letras más frecuentes en un criptograma de 424 caracteres son la W (59 veces) con un 13,9% y la K (52 veces) con un 12,2%. Suponiendo entonces que la W se corresponde a la cifra de la letra E del texto en claro y la K se corresponde con la A, tenemos el siguiente sistema de 2 ecuaciones independientes que resolveremos de la manera más sencilla posible, sin aplicar matrices, aprovechando que la letra A tiene como código el número 0.

Ecuación 1: W = a \* E + b mod 27

Ecuación 2: K = a \* A + b mod 27

Es decir:

Ecuación 1: 23 = a \* 4 + b mod 27

Ecuación 2: 10 = a \* 0 + b mod 27

De la ecuación 2, resulta obvio que b = 10. Reemplazando este valor en la ecuación 1 se tiene:

Ecuación 1: 23 = a \* 4 + 10 mod 27

a = (23 – 10) \* inv (4, 27) mod 27 = 13 \* 7 = 91 mod 27 = 10

Como el valor a = 10 es uno de los valores válidos en módulo 27, podemos suponer que:

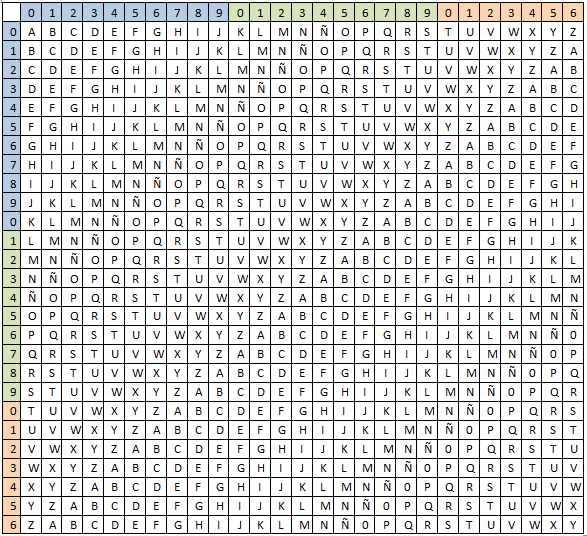
Ecuación de cifrado: C = 10 \* M + 10 mod 27

Ecuación de descifrado: M = (C – 10) \* inv (10, 27) mod 27 = (C – 10) \* 19 mod 27

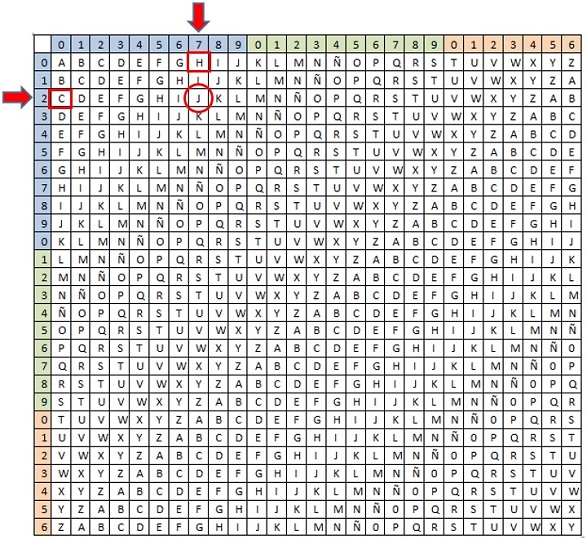
* 1. **POLI ALFABÉTICA**

La cifra de Vigenère es muy sencilla, bien sea a través de su tabla o bien usando matemáticas discretas.

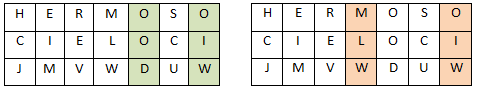
La tabla de Vigenère consiste en una matriz cuadrada de nxn elementos, siendo n el número de letras del alfabeto, que en el caso del español en mayúsculas será 27. En la primera fila se escribe el alfabeto desde la A hasta la Z, lo que sería el alfabeto del texto en claro, en la segunda fila el mismo alfabeto, pero desplazado un espacio a la izquierda, en la tercera dos veces, y así sucesivamente hasta la última fila en que el desplazamiento será igual a n-1.

  
Figura 1.3. Tabla de Vigenère para español en mayúsculas mod 27.

Así, si el mensaje es HERMOSO y la clave CIELO, en la columna de la letra H se busca la intersección con la fila de la letra C, dando como resultado el criptograma J, como se muestra en la figura 4. A continuación repetimos el mismo procedimiento para la letra E del texto en claro y la letra I de la clave, y así sucesivamente. Cuando la clave se termina, porque por lo general será menor que el mensaje, ésta se repite de forma cíclico, es decir CIELOCIELOCIELO. Por lo tanto como la clave CIELO tiene 5 letras, la sexta letra S del mensaje HERMOSO se volverá a cifrar con la primera letra C de la clave CIELO.

  
Figura 1.4. Cifrando con la tabla de Vigenère la letra H con la clave C mod 27.

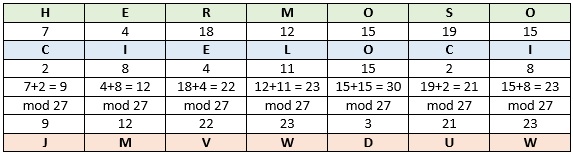
Realizando esta operación en todo el mensaje, el texto en claro HERMOSO se cifrará con Vigenère y la clave CIELO como JMVWD UW.

  
Figura 1.5. Destruyendo relaciones del alfabeto con el cifrado de Vigenère.

Como ya sabemos, la cifra polialfabética destruye esa relación directa y proporcional que se observaba en los sistemas de cifra monoalfabéticos entre el texto en claro y el criptograma. En este simple ejemplo esto se ve claramente en la figura 1.5 puesto la letra O, presente dos veces en el texto en claro HERMOSO, se cifra como D o W, en función de la posición relativa que tenga esta letra con respecto a la clave (figura izquierda). Y algo parecido sucede si observamos la letra W del criptograma, que en este caso procede bien de la M o de la O del texto en claro (figura derecha).

En vez de la tabla, para cifrar podemos usar matemáticas discretas módulo n de la siguiente manera: escribimos la clave debajo del mensaje tantas veces como sea necesario y vamos reemplazando el código de las letras para realizar posteriormente la operación suma.

http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/imagenes/Alfabetomod27.png  
Figura 1.6. Alfabeto mod 27.

  
Figura 1.7. Cifra de Vigenère aplicando matemáticas discretas.

Las operaciones de la figura 1.7 siguen la siguiente ecuación genérica de cifra de Vigenère:

**ci = mi + ki mod n**

En donde el subíndice i se refiere al carácter iésimo del texto en claro y de la clave, esta última repetida tantas veces como sea necesario, o lo que es lo mismo, representada en forma cíclica o módulo L, siendo L la longitud de la misma.