**CRIPTOSISTEMA HILL**

Este sistema está basado en el álgebra lineal y ha sido importante en la historia de la criptografía. Fue Inventado por Lester S. Hill en 1929, y fue el primer sistema criptográfico poli alfabético que era práctico para trabajar con más de tres símbolos simultáneamente.

Este sistema es poli alfabético pues puede darse que un mismo carácter en un mensaje a enviar se encripte en dos caracteres distintos en el mensaje encriptado.

Suponiendo que trabajamos con un alfabeto de 26 caracteres. Las letras se numeran en orden alfabético de forma tal que A=0, B=1,..., Z=25

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Se elige un entero *d* que determina bloques de *d* elementos que son tratados como un vector de *d* dimensiones.

Se elige de forma aleatoria una matriz de *d × d* elementos los cuales serán la clave a utilizar.

Los elementos de la matriz de *d × d* serán enteros entre 0 y 25, además la matriz M debe ser inversible en  z.

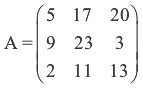
Para la encriptación, el texto es dividido en bloques de *d* elementos los cuales se multiplican por la matriz *d × d*

Todas las operaciones aritméticas se realizan en la forma módulo 26, es decir que 26 mod 26 = 0, 27 mod 26 =1, 28 mod 26 =2 etc. Para los negativos, -1 mod 26 = 25, -2 mod 26 = 24, …, -28 mod 26 = 24,etc.

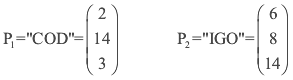
Dado un mensaje a encriptar debemos tomar bloques del mensaje de "d" caracteres y aplicar:

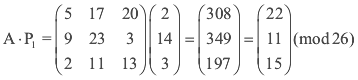
M×Pi=C, donde C es el código cifrado para el mensaje Pi

**Ejemplo:**

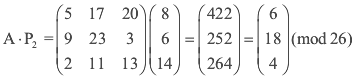
Si tomamos la matriz como matriz de claves.

Para encriptar el mensaje "CODIGO" debemos encriptar los seis caracteres de "CODIGO" en bloques de 3 caracteres cada uno, el primer bloque





El primer bloque "COD" se codificara como "WLP"



El segundo bloque "IGO" se codificara como "GSE"

Luego 'CODIGO' encriptado equivale a 'WLPGSE'.

Observar que las dos "O" se codificaran de forma diferente.

Para desencriptar el método es idéntico al anterior pero usando la matriz inversa de la usada para encriptar.

**Cálculo de la matriz inversa**

Antes que nada debemos verificar que la matriz elegida sea invertible en módulo 26. Hay una forma relativamente sencilla de averiguar esto a través del cálculo del determinante. Si el determinante de la matriz es 0 o tiene factores comunes con el módulo (en el caso de 26 los factores son 2 y 13), entonces la matriz no puede utilizarse. Al ser 2 uno de los factores de 26 muchas matrices no podrán utilizarse (no servirán todas en las que su determinante sea 0, un múltiplo de 2 o un múltiplo de 13)

Para ver si es invertible calculo el determinante de A



o también

La matriz A es invertible en módulo 26 ya que 26 y 9 son coprimos.

Para hallar la inversa de la matriz módulo 26, utilizamos la formula inversa

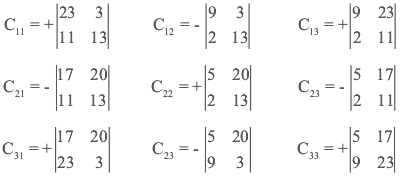
Donde CT es la matriz de cofactores de A transpuesta

Hay que tener en cuenta que detdebe realizarse en módulo 26 por lo tanto para el ejemplo la inversa de 9 (mod 26) es 3 (mod 26) ya que

Calculo del multiplicativo inverso:

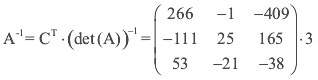
Por lo tanto 3 es la inversa multiplicativa de 9 en módulo 26.

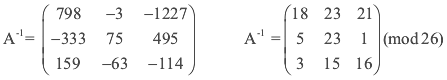
Para calcular C hay que calcular los cofactores de A





Ahora aplicamos la fórmula de la inversa





Esta última es la matriz que utilizamos para desencriptar.