# Códigos y Criptografía (GIINF)

**Practica Cifrado HILL**

| a | b | c | d | e | f | g | h | i | j | k | l | m | n |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 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 | |

**1. Construir la matriz cuadrada de orden 2 asociada a la palabra 'H I L L', y con ella cifrar usando el método de cifrado Hill el mensaje 'probando'.**

Matriz asociada a hill = $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$ el determinante es -11 que en modulo 27 seria 16 que es primo relativo con 27, con lo cual es una matriz valida.

Pasando '**probando**' a número = [(16 18) (15 01) (00 13) (03 15)] , cogemos bloques del mismo tamaño de la matriz usada, en este caso de dos en dos elementos.

$Y_{bi} = M X_{bi}$ , donde $_{bi}$ es el bloque a cifrar.

b1 - $$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 16 \\ 18 \end{pmatrix} = \begin{pmatrix} 13 \\ 23 \end{pmatrix} mod\ 27$$

b2 - $$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 15 \\ 01 \end{pmatrix} = \begin{pmatrix} 5 \\ 14 \end{pmatrix} mod\ 27$$

b3 - $$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 00 \\ 13 \end{pmatrix} = \begin{pmatrix} 23 \\ 08 \end{pmatrix} mod\ 27$$

b4 - $$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 03 \\ 15 \end{pmatrix} = \begin{pmatrix} 06 \\ 09 \end{pmatrix} mod\ 27$$

Cifrado = [(13 23) (5 14) (23 08) (06 19)]
Cifrado a letra= "nwfñwigs"

**2.¿Cuál de los siguientes vectores representa una permutación de S4 ?**

- {1, 3, 2, 5, 4}, queda descartado por ser S5.
- {4, 4, 3, 1}, queda descartado, porque en una permutación de este tipo no puede haber repetición.
- {2, 5, 3, 1}, queda descartado , porque no existe el número 4 y se excede en S4.
- **{4, 1, 2, 3}, valido en S4.**

**3.Escribir la matriz cuadrada asociada a la permutación del ejercicio anterior.**

Al ser una matriz boleana el determinante sera 1 o -1 y sera mcd con cualquier modulo.

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

**4.Volver a cifrar**

Pasando 'probando' a número = [(16 18 15 01) (00 13 03 15)] , cogemos bloques del mismo del S4 usado en el ejercicio anterior.

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 16 \\ 18 \\ 15 \\ 01 \end{pmatrix} = \begin{pmatrix} 1 \\ 16 \\ 18 \\ 15 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 00 \\ 13 \\ 03 \\ 15 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ 13 \\ 3 \end{pmatrix}$$

Cifrado = [(01 16 18 15) (15 00 13 03)]
Cifrado a letra= "bprooand”

**5. Descifrar el texto cifrado obtenido en el apartado anterior con el cifrado de permutación.**
**NOTA: Sabemos lo que tiene que salir.**

Para ello calculamos la inversa de la matriz de S4: $inverse\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

Multiplicamos la matriz inversa por los respectivos vectores.

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 16 \\ 18 \\ 15 \end{pmatrix} = \begin{pmatrix} 16 \\ 18 \\ 15 \\ 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 13 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 13 \\ 3 \\ 15 \end{pmatrix}$$

El mensaje resultante en letra es [16 18 15 01 00 13 03 15], que significa **“probando”**.

**6. Criptoanálisis del cifrado Hill del ejercicio 1. Es decir, conociendo el texto llano, el texto cifrado que hemos obtenido y el tamaño de los bloques d = 2, hallar la matriz M que se ha utilizado para el cifrado.**
**NOTA: De nuevo sabemos lo que tiene que salir.**

$$b1 - \boldsymbol{M}\begin{pmatrix} \boldsymbol{X} & \boldsymbol{Y} \\ \boldsymbol{Z} & \boldsymbol{W} \end{pmatrix}\begin{pmatrix} 16 \\ 18 \end{pmatrix} = \begin{pmatrix} 13 \\ 23 \end{pmatrix} mod\ 27$$

$$b2 - \boldsymbol{M}\begin{pmatrix} \boldsymbol{X} & \boldsymbol{Y} \\ \boldsymbol{Z} & \boldsymbol{W} \end{pmatrix}\begin{pmatrix} 15 \\ 01 \end{pmatrix} = \begin{pmatrix} 5 \\ 14 \end{pmatrix} mod\ 27$$

$$b3 - \boldsymbol{M}\begin{pmatrix} \boldsymbol{X} & \boldsymbol{Y} \\ \boldsymbol{Z} & \boldsymbol{W} \end{pmatrix}\begin{pmatrix} 00 \\ 13 \end{pmatrix} = \begin{pmatrix} 23 \\ 08 \end{pmatrix} mod\ 27$$

$$b4 - \boldsymbol{M}\begin{pmatrix} \boldsymbol{X} & \boldsymbol{Y} \\ \boldsymbol{Z} & \boldsymbol{W} \end{pmatrix}\begin{pmatrix} 03 \\ 15 \end{pmatrix} = \begin{pmatrix} 06 \\ 09 \end{pmatrix} mod\ 27$$

Texto llano: **'probando'**
Texto cifrado: **'nwfñwigs'**
Tamaño: 2

Debemos de formar la ecuación: $Y* = X*Mt$ ,siendo:

- $Y*$ : la matriz de d columnas formada por el mensaje cifrado escrito por filas.
- $X*$ : la matriz de d columnas formada por el mensaje llano escrito por filas.
- Mt : la matriz traspuesta de la clave M. Es decir, una matriz cuadrada de orden d.

Pasando '**probando**' a número = [(16 18) (15 01) (00 13) (03 15)] = **'probando'**
Cifrado = [(13 23) (5 14) (23 08) (06 19)] = **'nwfñwigs'**

$$\begin{pmatrix} 13 & 23 \\ 5 & 14 \\ 23 & 8 \\ 6 & 19 \end{pmatrix} = \begin{pmatrix} 16 & 18 \\ 15 & 1 \\ 0 & 13 \\ 3 & 15 \end{pmatrix} \cdot M^T$$

$$X = \begin{pmatrix} 16 & 18 \\ 15 & 1 \\ 0 & 13 \\ 3 & 15 \end{pmatrix}$$

***Transformaciones***
***1) F1 = F1-F2***
***2) F2 = F2-15F1***
***3) F2 = F2+3F3***
***4) F1 = F1-17F2***

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 13 \\ 3 & 15 \end{pmatrix}$$

$$Y = \begin{pmatrix} 13 & 23 \\ 5 & 14 \\ 23 & 8 \\ 6 & 19 \end{pmatrix}$$

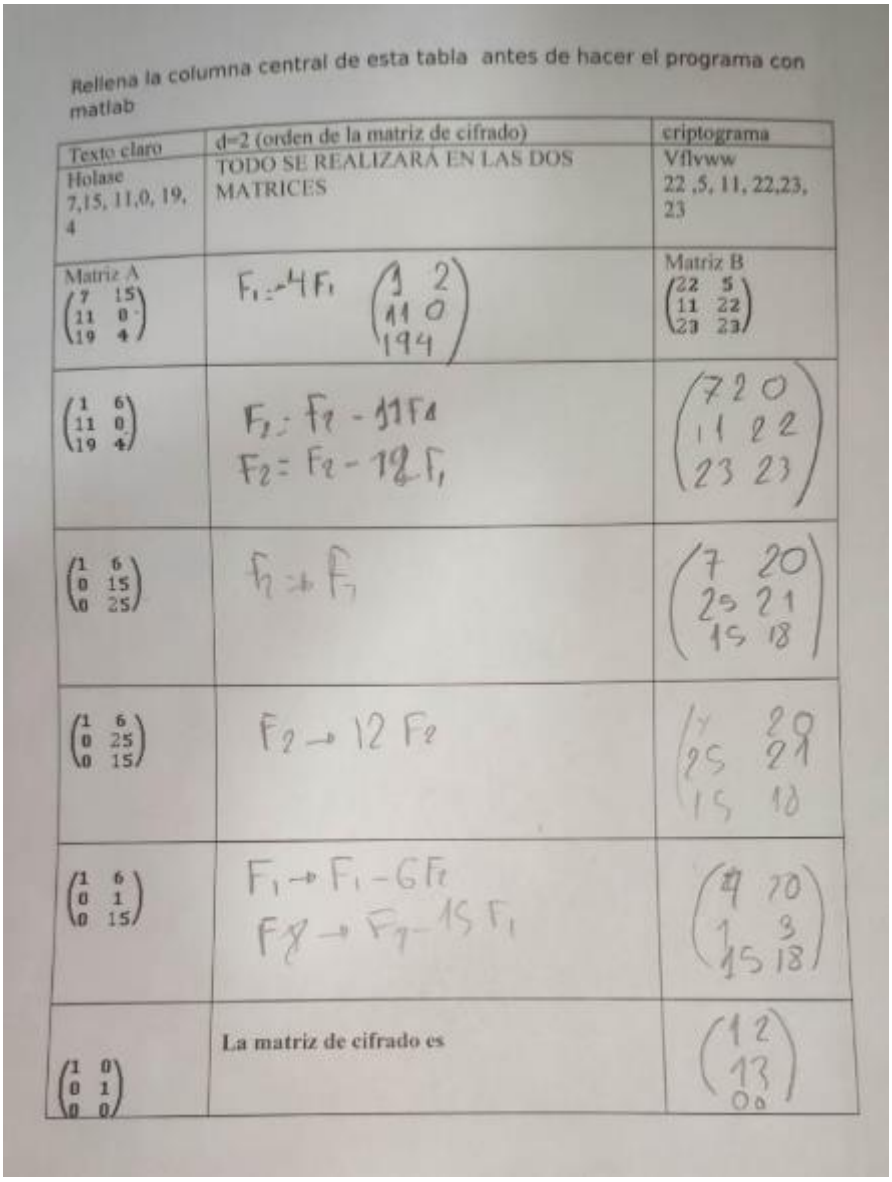
***Transformaciones***
***1) F1 = F1-F2***
***2) F2 = F2-15F1***
***3) F2 = F2+3F3***
***4) F1 = F1-17F2***

$$Y = \begin{pmatrix} 7 & 11 \\ 8 & 11 \\ 23 & 8 \\ 6 & 19 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 11 \\ 8 & 11 \end{pmatrix}^T = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

***Matriz M***

## 7. Ejercicio a mano



Rellena la columna central de esta tabla antes de hacer el programa con matlab

| Texto claro | d=2 (orden de la matriz de cifrado) | criptograma |
|---|---|---|
| Holase<br>7,15, 11,0, 19, 4 | TODO SE REALIZARÁ EN LAS DOS MATRICES | Vflvww<br>22 ,5, 11, 22,23, 23 |
| Matriz A<br>$\begin{pmatrix} 7 & 15 \\ 11 & 0 \\ 19 & 4 \end{pmatrix}$ | $F_1 \leftarrow 4F_1$ $\begin{pmatrix} 1 & 2 \\ 11 & 0 \\ 19 & 4 \end{pmatrix}$ | Matriz B<br>$\begin{pmatrix} 22 & 5 \\ 11 & 22 \\ 23 & 23 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 6 \\ 11 & 0 \\ 19 & 4 \end{pmatrix}$ | $F_2 \leftarrow F_2 - 11F_1$<br>$F_2 \leftarrow F_2 - 19F_1$ | $\begin{pmatrix} 7 & 20 \\ 11 & 22 \\ 23 & 23 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 6 \\ 0 & 15 \\ 0 & 25 \end{pmatrix}$ | $F_2 \leftrightarrow F_3$ | $\begin{pmatrix} 7 & 20 \\ 25 & 21 \\ 15 & 18 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 6 \\ 0 & 25 \\ 0 & 15 \end{pmatrix}$ | $F_2 \rightarrow 12F_2$ | $\begin{pmatrix} 7 & 20 \\ 25 & 21 \\ 15 & 18 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 6 \\ 0 & 1 \\ 0 & 15 \end{pmatrix}$ | $F_1 \rightarrow F_1 - 6F_2$<br>$F_3 \rightarrow F_3 - 15F_1$ | $\begin{pmatrix} 7 & 20 \\ 1 & 3 \\ 15 & 18 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$ | La matriz de cifrado es | $\begin{pmatrix} 1 & 2 \\ 13 & \\ 0 & 0 \end{pmatrix}$ |