DESCIFRADO DEL MECANISMO DE HILL

CABALLERO HUESCA CARLOS EDUARDO

MARTÍNEZ GARCÍA BRANDO JOSUÉ

GRUPO 3CV1

¿CÓMO DESCIFRAR CON EL MECANISMO DE HILL, SI SE USÓ UNA LLAVE K, QUE ES UNA MATRIZ DE 3X3?

- **El algoritmo hace uso del Álgebra Lineal y debe cumplir con ciertas reglas:**
  - El determinante de matriz clave debe ser diferente de cero.
  - El determinante inverso de la matriz clave, debe ser un valor entero, para que el mensaje pueda ser cifrado y descifrado.

PARA PODER DESCIFRAR NECESITAMOS:

- Comprobar si **la matriz es invertible** en modulo n (26)
- Si el determinante de la matriz es 0 o tiene factores comunes con el módulo 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).

$A^{-1}=C^{T}(DET(A))^{-1}$

- Calcular el determinante inverso de la matriz clave en su forma modular.
- Multiplicarlo por la matriz clave traspuesta, esta operación nos dará la matriz clave inversa.
- Esta nueva matriz se multiplicará por el vector del criptograma a descifrar.

$MCla=EA^{-1}$

EJEMPLO: WLPGSE

Sea:

$$A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$$

Para verificar que sea invertible, calculamos el determinante de A.

$$\det \mathbf{A} = \begin{vmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{vmatrix} = 5 \cdot \begin{vmatrix} 23 & 3 \\ 11 & 13 \end{vmatrix} - 17 \cdot \begin{vmatrix} 9 & 3 \\ 2 & 13 \end{vmatrix} + 20 \cdot \begin{vmatrix} 9 & 23 \\ 2 & 11 \end{vmatrix} = 503$$

= 9 mod 26

$(9 \bmod 26)^{-1} = \mathbf{3}\ \boldsymbol{mod}\ \mathbf{26}$ *inversa multiplicativa*

Para calcular C, calcular los cofactores de A

$$C_{11} = +\begin{vmatrix} 23 & 3 \\ 11 & 13 \end{vmatrix} \qquad C_{12} = -\begin{vmatrix} 9 & 3 \\ 2 & 13 \end{vmatrix} \qquad C_{13} = +\begin{vmatrix} 9 & 23 \\ 2 & 11 \end{vmatrix}$$

$$C_{21} = -\begin{vmatrix} 17 & 20 \\ 11 & 13 \end{vmatrix} \qquad C_{22} = +\begin{vmatrix} 5 & 20 \\ 2 & 13 \end{vmatrix} \qquad C_{23} = -\begin{vmatrix} 5 & 17 \\ 2 & 11 \end{vmatrix}$$

$$C_{31} = +\begin{vmatrix} 17 & 20 \\ 23 & 3 \end{vmatrix} \qquad C_{23} = -\begin{vmatrix} 5 & 20 \\ 9 & 3 \end{vmatrix} \qquad C_{33} = +\begin{vmatrix} 5 & 17 \\ 9 & 23 \end{vmatrix}$$

$$C = \begin{pmatrix} 266 & -111 & 53 \\ -1 & 25 & -21 \\ -409 & 165 & -38 \end{pmatrix} \qquad C^T = \begin{pmatrix} 266 & -1 & -409 \\ -111 & 25 & 165 \\ 53 & -21 & -38 \end{pmatrix}$$

Formamos C con los cofactores de A y aplicamos la Transpuesta.

Ahora estos valores los sustituimos en la fórmula $\mathbf{A^{-1}=C^{T}(det(A))^{-1}}$

$$A^{-1}= C^{T}\cdot\left(\det(A)\right)^{-1}=\begin{pmatrix}266 & -1 & -409\\ -111 & 25 & 165\\ 53 & -21 & -38\end{pmatrix}\cdot 3$$

$$A^{-1}=\begin{pmatrix}798 & -3 & -1227\\ -333 & 75 & 495\\ 159 & -63 & -114\end{pmatrix} \qquad A^{-1}=\begin{pmatrix}18 & 23 & 21\\ 5 & 23 & 1\\ 3 & 15 & 16\end{pmatrix}(\mathrm{mod}\,26)$$

Obtenemos la matriz $\mathbf{A^{-1}}(\mathrm{mod}\ 26)$,que usaremos para desencriptar.

Si la llave K es una matriz de 3x3, el vector del criptograma a descifrar tiene que tener la misma cantidad de filas que las columnas que tiene la llave K

$$\boldsymbol{WLP} = \begin{pmatrix} \mathbf{22} \\ \mathbf{11} \\ \mathbf{15} \end{pmatrix} \qquad \boldsymbol{GSE} = \begin{pmatrix} \mathbf{6} \\ \mathbf{18} \\ \mathbf{4} \end{pmatrix}$$

$$\begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} \cdot \begin{pmatrix} 22 \\ 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 964 \\ 378 \\ 471 \end{pmatrix}$$

$$\begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 18 \\ 4 \end{pmatrix} = \begin{pmatrix} 606 \\ 448 \\ 352 \end{pmatrix}$$

$$\boldsymbol{WLP} = \begin{pmatrix} \mathbf{2} \\ \mathbf{14} \\ \mathbf{3} \end{pmatrix} (\boldsymbol{mod}\ \mathbf{26}) = \boldsymbol{COD}$$

$$\boldsymbol{GSE} = \begin{pmatrix} \mathbf{8} \\ \mathbf{6} \\ \mathbf{14} \end{pmatrix} (\boldsymbol{mod}\ \mathbf{26}) = \boldsymbol{IGO}$$

“CODIGO”