

Tp1 – Criptografía Simétrica

Primer parte

1. Resuelto en <https://github.com/poximan/ARS/tree/master/tp1/caesar>
2. Resuelto en https://github.com/poximan/ARS/tree/master/tp1/hack_caesar
3. Resuelto en <https://github.com/poximan/ARS/tree/master/tp1/caesar>

Para todos los casos anteriores, clonar <https://github.com/poximan/ARS.git>

4. Cifrar la frase

“Vivir solo cuesta vida” con el cifrador de Hill con la matriz $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ y luego descifrarla. Detallar todos los pasos.

Cifrado

Mensaje = “Vivir solo cuesta vida”.

$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} L & I \\ D & H \end{pmatrix}$

- “VI” (22, 8)

$$C_1 = (11 * 22 + 8 * 8) \bmod 27 = 9 \text{ (J)}.$$

$$C_2 = (3 * 22 + 7 * 8) \bmod 27 = 14 \text{ (Ñ)}.$$

- “VI” (22, 8)

$$C_3 = 9 \text{ (J)}.$$

$$C_4 = 14 \text{ (Ñ)}.$$

- “RS” (18, 19)

$$C_5 = (11 * 18 + 8 * 19) \bmod 27 = 26 \text{ (Z)}.$$

$$C_6 = (3 * 18 + 7 * 19) \bmod 27 = 25 \text{ (Y)}.$$

- “OL” (15, 11)

$$C_7 = (11 * 15 + 8 * 11) \bmod 27 = 10 \text{ (K)}.$$

$$C_8 = (3 * 15 + 7 * 11) \bmod 27 = 14 \text{ (Ñ)}.$$

- “OC” (15, 2)

$$C_9 = (11 * 15 + 8 * 2) \bmod 27 = 19 \text{ (S)}.$$

$$C_{10} = (3 * 15 + 7 * 2) \bmod 27 = 5 \text{ (F)}.$$

- “UE” (21, 4)

$$C_{11} = (11 * 21 + 8 * 4) \bmod 27 = 20 \text{ (T)}.$$

$$C_{12} = (3 * 21 + 7 * 4) \bmod 27 = 10 \text{ (K)}.$$

- “ST” (19, 20)

$$C_{13} = (11 * 19 + 8 * 20) \bmod 27 = 18 \text{ (R)}.$$

$$C_{14} = (3 * 19 + 7 * 20) \bmod 27 = 8 \text{ (I)}.$$

- “AV” (0, 22)

$$C_{15} = (11 * 0 + 8 * 22) \bmod 27 = 14 \text{ (Ñ)}.$$

$$C_{16} = (3 * 0 + 7 * 22) \bmod 27 = 19 \text{ (S)}.$$

- “ID” (8, 3)

$$C_{17} = (11 * 8 + 8 * 3) \bmod 27 = 4 \text{ (E)}.$$

$$C_{18} = (3 * 8 + 7 * 3) \bmod 27 = 18 \text{ (R)}.$$

(j) “AZ” (0, 7). H = Para completar la matriz.

$$C_{19} = (11 * 0 + 8 * 26) \bmod 27 = 19 \text{ (S)}.$$

$$C_{20} = (3 * 0 + 7 * 7) \bmod 27 = 23 \text{ (W)}.$$

C = “JÑJÑZYKÑSFTKRIÑSERSW”.

Descifrado

$$|K| = 53.$$

$$|K| \bmod 27 = 26.$$

$$ADJ(K) = ((7, -3), (-8, 11))$$

$$T_{ADJ}(K) = ((7, -8), (-3, 11))$$

$$K^{-1} = T_{ADJ(K)} * INV(26, 27) = ((182, -208), (-78, 286)) \bmod 27 = ((20, 8), (3, 16))$$

- “JÑ” (9, 14)

$$M_1 = (20 * 9 + 8 * 14) \bmod 27 = 22 \text{ (V)}.$$

$$M_2 = (3 * 9 + 16 * 14) \bmod 27 = 8 \text{ (I)}.$$

- “JÑ” (9, 14)

$$M_3 = 22 \text{ (V)}.$$

$$M_4 = 8 \text{ (I)}.$$

- “ZY” (26, 25)

$$M_5 = (20 * 26 + 8 * 25) \bmod 27 = 18 \text{ (R)}.$$

$$M_6 = (3 * 26 + 16 * 25) \bmod 27 = 19 \text{ (S)}.$$

- “KÑ” (10, 14)

$$M_7 = (20 * 10 + 8 * 14) \bmod 27 = 15 \text{ (O)}.$$

$$M_8 = (3 * 10 + 16 * 14) \bmod 27 = 11 \text{ (L)}.$$

- “SF” (19, 5)

$$M_9 = (20 * 19 + 8 * 5) \bmod 27 = 15 \text{ (O)}.$$

$$M_{10} = (3 * 19 + 16 * 5) \bmod 27 = 2 \text{ (C)}.$$

- “TK” (20, 10)

$$M_{11} = (20 * 20 + 8 * 10) \bmod 27 = 21 \text{ (U)}.$$

$$M_{12} = (3 * 20 + 16 * 10) \bmod 27 = 4 \text{ (E)}.$$

- “RI” (18, 8)

$$M_{13} = (20 * 18 + 8 * 8) \bmod 27 = 19 \text{ (S)}.$$

$$M_{14} = (3 * 18 + 16 * 8) \bmod 27 = 20 \text{ (T)}.$$

- “ÑS” (14, 19)

$$M_{15} = (20 * 14 + 8 * 19) \bmod 27 = 0 \text{ (A)}.$$

$$M_{16} = (3 * 14 + 16 * 19) \bmod 27 = 22 \text{ (V)}.$$

- “ER” (4, 18)

$$M_{17} = (20 * 4 + 8 * 18) \bmod 27 = 8 \text{ (I)}.$$

$$M_{18} = (3 * 4 + 16 * 18) \bmod 27 = 3 \text{ (D)}.$$

- “SW” (19, 23)

$$M_{19} = (20 * 19 + 8 * 20) \bmod 27 = 0 \text{ (A)}.$$

$$M_{20} = (3 * 19 + 16 * 23) \bmod 27 = 20 \text{ (T)}. \text{ Para completar la matriz.}$$

M = “VIVIRCUESTAVIDA”

5. Si se aplica dos veces el cifrador Affine, ¿se mejora la seguridad?

Considerando que los métodos de encriptado son públicos, y la potencia radica en que la función de encriptado sea en un solo sentido, iterar n veces sobre el mensaje original no aumenta la complejidad del cómputo, ya que una vez conocido el método de encriptado, bastará aplicarlo reiteradas veces hasta obtener el texto plano. Por lo tanto, aplicar dos veces el mismo método no mejora la seguridad.

6. ¿Qué protocolos populares utilizan cifrado DES?

- IPSec: capa de seguridad sobre IP.
- IKE (Internet Key Exchange): protocolo implementado por Cisco para su SO.
- TLS 1.0.: seguridad en capa de transporte.
- WiMax.

<https://books.google.com.ar/books?id=WHg9YgZkx8YC> (caps 19 y 20).