Trabajo Práctico Nº 1.

Criptografía simétrica (primera parte).

1) Cifrador/Descifrador de “Cesar”. Implementado en PHP.

   Git: jldevia/**ARS2018 – TP1/ejer_1.php**

2) Mecanismo de fuerza bruta para descifrar un mensaje cifrado con el algoritmo de “Cesar”. Implementado en PHP.

   Git: jldevia/**ARS2018 – TP1/ejer_2.php**

3) Cifrador/Descifrador “Vigènere”. Implementado en PHP.

   Git: jldevia/**ARS2018 – TP1/ejer_3.php**

4) Cifrado/descifrado de Hill.

   Cifrado.

   Mensaje = “*Vivir solo cuesta vida*”.

   K = ((11 , 8), (3 ,7)) ((L, I) , (D, H))

   (a) “VI” (22, 8)

   C_1 = (11 * 22 + 8 * 8) mod 27 = 9 (J).

   C_2 = (3 * 22 + 7 * 8) mod 27 = 14 (Ñ).

   (b) “VI” (22, 8)

   C_3 = 9 (J).

   C_4 = 14 (Ñ).

   (c) “RS” (18, 19)

   C_5 = (11 * 18 + 8 * 19) mod 27 = 26 (Z).

   C_6 = (3 * 18 + 7 * 19) mod 27 = 25 (Y).

   (d) “OL” (15, 11)

   C_7 = (11 * 15 + 8 * 11) mod 27 = 10 (K).

   C_8 = (3 * 15 + 7 * 11) mod 27 = 14 (Ñ).

   (e) “OC” (15, 2)

   C_9 = (11 * 15 + 8 * 2) mod 27 = 19 (S).

   C_{10} = (3 * 15 + 7 * 2) mod 27 = 5 (F).

   (f) “UE” (21, 4)

   C_{11} = (11 * 21 + 8 * 4) mod 27 = 20 (T).

C_{12} = (3 * 21 + 7 * 4) mod 27 = 10 (K).

(g) “ST” (19, 20)

C_{13} = (11 * 19 + 8 * 20) mod 27 = 18 (R).

C_{14} = (3 * 19 + 7 * 20) mod 27 = 8 (I).

(h) “AV” (0, 22)

C_{15} = (11 * 0 + 8 * 22) mod 27 = 14 (Ñ).

C_{16} = (3 * 0 + 7 * 22) mod 27 = 19 (S).

(i) “ID” (8, 3)

C_{17} = (11 * 8 + 8 * 3) mod 27 = 4 (E).

C_{18} = (3 * 8 + 7 * 3) mod 27 = 18 (R).

(j) “AZ” (0, 26). Z=*Relleno*

C_{19} = (11 * 0 + 8 * 26) mod 27 = 19 (S).

C_{20} = (3 * 0 + 7 * 26) mod 27 = 20 (T).

C = “JÑJÑZYKÑSFTKRIÑSERST”.

Descifrado.

$|K|$ = 53.

$|K|$ mod 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)) mod 27 = ((20, 8), (3, 16))

(a) “JÑ” (9, 14)

M_1 = (20 * 9 + 8 * 14) mod 27 = 22 (V).

M_2 = (3 * 9 + 16 * 14) mod 27 = 8 (I).

(b) “JÑ” (9, 14)

M_3 = 22 (V).

M_4 = 8 (I).

(c) “ZY” (26, 25)

M_5 = (20 * 26 + 8 * 25) mod 27 = 18 (R).

M_6 = (3 * 26 + 16 * 25) mod 27 = 19 (S).

(d) “KÑ” (10, 14)

M_7 = (20 * 10 + 8 * 14) mod 27 = 15 (O).

M_8 = (3 * 10 + 16 * 14) mod 27 = 11 (L).

(e) “SF” (19, 5)

M_9 = (20 * 19 + 8 * 5) mod 27 = 15 (O).

M_{10} = (3 * 19 + 16 * 5) mod 27 = 2 (C).

(f) “TK” (20, 10)

M_{11} = (20 * 20 + 8 * 10) mod 27 = 21 (U).

M_{12} = (3 * 20 + 16 * 10) mod 27 = 4 (E).

(g) “RI” (18 ,8)

M_{13} = (20 * 18 + 8 * 8) mod 27 = 19 (S).

M_{14} = (3 * 18 + 16 * 8) mod 27 = 20 (T).

(h) “ÑS” (14, 19)

M_{15} = (20 * 14 + 8 * 19) mod 27 = 0 (A).

M_{16} = (3 * 14 + 16 * 19) mod 27 = 22 (V).

(i) “ER” (4, 18)

M_{17} = (20 * 4 + 8 * 18) mod 27 = 8 (I).

M_{18} = (3 * 4 + 16 * 18) mod 27 = 3 (D).

(j) “ST” (19, 20)

M_{19} = (20 * 19 + 8 * 20) mod 27 = 0 (A).

M_{20} = (3 * 19 + 16 *20) mod 27 = 26 (Z). Relleno.

M = “VIVIRCUESTAVIDA”

5) Cifrador Affine.

Considerando que los métodos de encriptación 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 computo, ya que una vez conocido el método de encriptado, bastara aplicarlo reiteradas veces hasta obtener el texto plano. Por lo tanto, aplicar dos veces el mismo metodo no mejora la seguridad.

6) Algunos protocolos que utilizan DES **(Data Encryption Standard)** ó algunos de sus derivados/sucesores:

- **WiMAX** (*Worldwide Interoperability for Microwave Access - Interoperabilidad mundial para acceso por microondas*): es una tecnología de comunicación similar al WiFi pero por microondas con alcance superior a los 30 km y velocidades de hasta 1024 Mbps. Es la tecnología firme candidata a ofrecer conexiones a Internet súper rápidas y con una amplia cobertura. Este protocolo esta especificado en el standar IEEE 802.16. En cuanto a los aspectos de seguridad del mismo, entre algunos de los algoritmos de cifrado de datos que utiliza, se encuentra DES y su sucesor, 3DES (Triple DES).
    1. https://es.wikipedia.org/wiki/IEEE_802.16.
    2. http://www.ippt.pan.pl/Repository/o320.pdf.
- **IPSec**: conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet IP autenticando y/o cifrando cada paquete IP en un flujo de datos.
  IPSec utiliza para la confidencialidad de datos Triple *DES-CBC* y *AES-CBC*.

1. https://es.wikipedia.org/wiki/IPsec

- **TLS** (*Transport Layer Security – Seguridad de la capa de transporte*): este protocolo, y su antecesor (**SSL** – Secure Sockets Layer), es un protocolo criptográfico que añade una capa de seguridad sobre la capa de transporte (TCP/UDP) en internet. Provee cifrado de datos mediante el uso de algoritmos como AES-CBC (TLS 1.1), AES GCM (TLS 1.2), AES CCM (TLS 1.2), 3DES-CBC (SSL 2.0), DES-CBC (SSL 2.0), etc.
    1. https://es.wikipedia.org/wiki/Transport_Layer_Security#Ataques_contra_SSL/TLS
- **SSH** (*Secure Shell*): es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de Internet. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada. Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. Entre las técnicas criptográficas que utiliza para el encriptado de los datos transmitidos es AES.
    1. https://www.hostinger.com.ar/tutoriales/que-es-ssh