“Criptografía Simétrica y Asimétrica”

Trabajo Preparatorio N°12

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el presente documento se presenta el fundamento teórico acerca de Criptografía Simétrica y Asimétrica, con el fin de comprender en la práctica cómo se desarrolla un intercambio de clave Diffie y Hellman DH, así como el problema del logaritmo discreto PLD asociado a dicho algoritmo y lograr realizar operaciones de cifrado y descifrado con diferentes algoritmos.**

***Index Terms*—Algoritmo, Asimétrica, Clave, Criptografía, Intercambio, Simétrica.**

I. Introducción

El acceso no autorizado a todo tipo de datos es un riesgo constante en el mundo cibernético actual. Los datos del sistema financiero y de pago son los datos más vulnerables, que pueden revelar información de identificación personal (PII) de consumidores y clientes o registros de tarjetas de crédito.

El cifrado es fundamental para proteger la información de identificación personal y mitigar las amenazas para las empresas que realizan transacciones de pago cada minuto del día. Esto hace que la criptografía sea crucial. Existen principalmente dos tipos de criptografía: criptografía simétrica y asimétrica [1].

La criptografía de clave simétrica, o cifrado simétrico, utiliza una clave secreta tanto para el cifrado como para el descifrado. Este enfoque es el inverso del cifrado asimétrico, que utiliza una clave para cifrar y otra para descifrar. Los datos se traducen a un formato que no puede ser interpretado o inspeccionado por alguien que no tenga la clave secreta utilizada para cifrarlos durante esta fase. A continuación se explorar definiciones asociados a estas claves.

II. Objetivos

- Comprender en la práctica cómo se desarrolla un intercambio de clave Diffie y Hellman DH, así como el problema del logaritmo discreto PLD asociado a dicho algoritmo.
- Lograr realizar operaciones de cifrado y descifrado en flujo con registros de desplazamiento LFSR y con algoritmo A5/1, comprendiendo qué es el código Base64.
- Realizar operaciones de cifrado y descifrado en bloque con el algoritmo DES y con el algoritmo AES.
- Calcular la función hash SHA256 a un documento.
- Generar una clave estándar RSA de 2.048 bits con el software genRSA, con la cual vas a firmar digitalmente el hash anterior

III. Cuestionario

A. Consultar (máximo 2 hojas):

- **El concepto de claves débiles en cifrado.**
  Las claves débiles generalmente representan un a fracción muy pequeña del espacio de clave total, lo que significa que si se genera una clave aleatoria para el cifrado, la posibilidad de que aparezca dicha clave débil es muy pequeña y que por lo tanto de que exista un problema de seguridad. Sin embargo, se considera deseable para un cifrador carecer de claves débiles [1].
- **Claves débiles en DES.**
  El cifrado de bloque DES tiene algunas claves específicas denominadas ”claves débiles” y ”claves semifábiles”. Estas son claves que hacen que el modo de cifrado de DES actúe de manera idéntica al modo de descifrado de DES (aunque potencialmente el de una clave diferente). En funcionamiento, la clave secreta de 56 bits se divide en 16 subclaves de acuerdo con la programación de claves DES; se utiliza una subclave en cada una de las dieciséis rondas DES [2]. Las claves débiles DES producen dieciséis subclaves idénticas. Esto ocurre cuando la clave (expresada en hexadecimal) es:
  - Alternando unos + ceros (0x0101010101010101)
  - Alternando ’F’ + ’E’ (0xFEFEFEFEFEFEFEFE)
  - ’0xE0E0E0E0F1F1F1F1’
  - ’0x1F1F1F1F0E0E0E0E’

  Si una implementación no considera los bits de paridad, las claves correspondientes con los bits de paridad invertidos también pueden funcionar como claves débiles:
  - Todos ceros (0x0000000000000000)
  - Todos unos (0xFFFFFFFFFFFFFFFF)
  - ’0xE1E1E1E1F0F0F0F0’
  - ’0x1E1E1E1E0F0F0F0F’ [2]
- **Ataque por fuerza bruta de algoritmo de cifrado.**
  En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las com-

binaciones posibles hasta encontrar aquella que permite el acceso. Dicho de otro modo, define al procedimiento por el cual a partir del conocimiento del algoritmo de cifrado empleado y de un par texto claro/texto cifrado, se realiza el cifrado (respectivamente, descifrado) de uno de los miembros del par con cada una de las posibles combinaciones de clave, hasta obtener el otro miembro del par. [3].

El esfuerzo requerido para que la búsqueda sea exitosa con probabilidad mejor que la par será operaciones, donde es la longitud de la clave (también conocido como el espacio de claves). Otro factor determinante en el coste de realizar un ataque de fuerza bruta es el juego de caracteres que se pueden utilizar en la clave. Contraseñas que sólo utilicen dígitos numéricos serán más fáciles de descifrar que aquellas que incluyen otros caracteres como letras, así como las que están compuestas por menos caracteres serán también más fáciles de descifrar, la complejidad impuesta por la cantidad de caracteres en una contraseña es logarítmica. Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, son muy costosos en tiempo computacional. La fuerza bruta suele combinarse con un ataque de diccionario [3].

Es una técnica de criptoanálisis u otro tipo de método de ataque que implica un procedimiento exhaustivo que prueba todas las posibilidades, una por una. Caso particular de ataque sólo al texto cifrado en el que el criptoanalista, cociendo el algoritmo de cifra, intenta su descifrado probando con cada clave del espacio de claves. Si el cardinal de este último es un número muy grande, el tiempo invertido en recorrer el citado espacio es fabuloso, y las probabilidades de éxito escasísimas. [4].

B. Descargar los siguientes programas:

A continuación, se presentan las interfaces de los diferentes programas descargados.

- FlujoLab

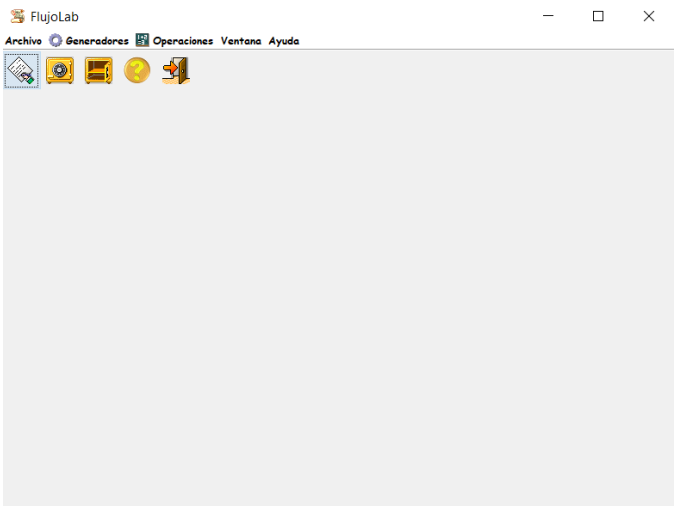

Fig. 1. Interfaz de FlujoLab

- SafeDES

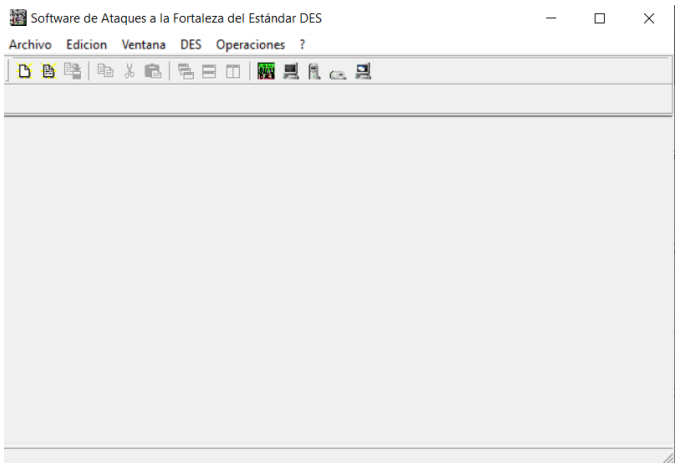

Fig. 2. Interfaz de SafeDES

- AESPhere

Fig. 3. Interfaz de AESPhere

- SAMCript

Fig. 4. Interfaz de SAMCript

- DILOG

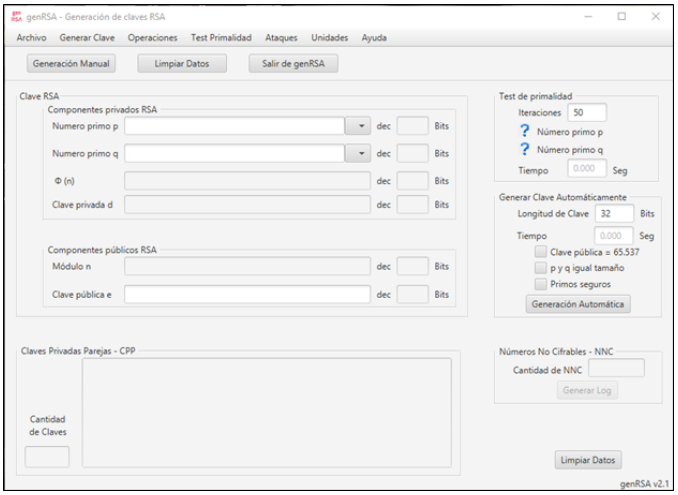

Fig. 5. Interfaz de DILOG

- Hashcalc

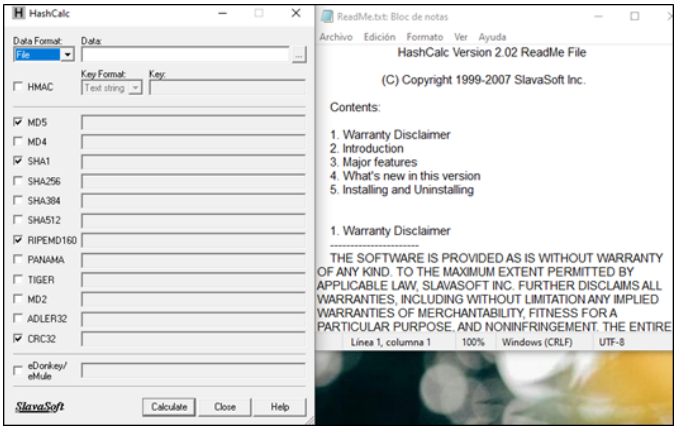

Fig. 6. Interfaz de Hashcalc

- Online Tools

Fig. 7. Interfaz de Online Tools

- genRSA v2.1

Fig. 8. genRSA v2.1

REFERENCES

[1] "Symmetric And Asymmetric Key Cryptography: A Detailed Guide In 2021". https://www.jigsawacademy.com/blogs/cyber-security/symmetric-and-asymmetric-key-cryptography (accedido sep. 02, 2021).
[2] "Weak Key - Weak Keys in DES — Weak Keys DES". https://www.liquisearch.com/weak_key/weak_keys_in_des (accedido sep. 02, 2021).
[3] "Ataque de Fuerza Bruta" https://sites.google.com/site/delitosinformaticos final/ataque-de-fuerza-bruta. accedido (sep. 01, 2021).
[4] "ATAQUE POR FUERZA BRUTA " http://www.dit.upm.es/ pepe/401/index.html#!1807. accedido (sep. 01, 2021).