UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

LABORATORIO 2:

SISTEMAS DE COMUNICACIÓN

JAVIER ARREDONDO

DIEGO MELLIS

ANDRÉS MUÑOZ

Profesor: Pablo Reyes

Ayudante: Tomás Child

Santiago - Chile

11 de enero de 2019

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1. INTRODUCCIÓN

En un contexto social la comunicación aborda la transmisión de información de un medio a otro; en donde la información se subentiende como un mensaje con cierta importancia. Para la investigación propuesta por el cuerpo docente, se hace referencia a un sistema de comunicación a aquel sistema tecnológico que es capaz transmitir un mensaje con información de un sistema a otro. Un campo importante dentro de la transmisión de información es la criptografía.

La palabra criptografía proviene del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje [Ang00]. La acción de aplicar la técnica de la criptografía para esconder un mensaje condifencial, se le puede llamar encriptar o cifrar, en donde el emisor "esconde" el mensaje y lo transmite por un canal que puede o no ser inseguro, para que posteriormente solo el receptor autorizado pueda leer el mensaje.

1.1. Objetivos

Para la investigación expuesta se abordan los siguientes objetivos a cumplir [Rey]:

- Diseñar un sistema de encriptación simétrico.
- Evaluar rendimiento y funcionamiento a partir de una serie de métricas.

1.2. Motivación

La motivación recae en los estudiantes, ya que para cumplir con los objetivos expuestos se debe abstraer los conceptos vistos en cátedra ligados a encriptación, para así poder implementar de manera didáctica los contenidos aprendidos.

El documento está constituido de manera que el lector comprenda en primera instancia los conceptos importantes abarcados en el presente documento, éstos son

explicados en un breve marco teórico, luego se procede a explicar el algoritmo de encriptación implementado por los estudiantes, para luego exponer una evaluación de éste. Posteriormente se realiza un criptoanálisis, en donde se explora las opciones y estrategias para descifrar un mensaje codificado. Finalmente, se presenta una conclusión a partir de la investigación realizada.

CAPÍTULO 2. MARCO TEÓRICO

2.1 ENCRIPTACIÓN

Es la técnica o proceso de ocultar datos mediante una clave. Comúnmente se utiliza para poder esconder información de un mensaje, el que será enviado a través de una línea de comunicación insegura. Luego los receptores autorizados podrán leer la información cifrada en el mensaje. Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo [Ang00].

2.1.1 Llave

Es una clave que se puede utilizar para encriptar o desencriptar mensajes utilizando un determinado sistema criptográfico.

2.1.2 Encriptación simétrica

Hace referencia a la metodología que permite tener comunicación segura entre las partes, donde dichas partes previamente han intercambiado la clave correspondiente. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

En el presente documento se abarca la criptografía simétrica de bloques o en inglés *block cipher*, el cual consiste en un sistema criptográfico que cifra de bloque en bloque, dichos bloques consisten en un grupo de bits de longitud fija, usualmente cada bloque es de 128 bits. Algunos sistemas conocido son: TDES, RC5, AES.

2.2 DESENCRIPTACIÓN

Es el proceso inverso a la encriptación, ya que consiste en convertir un texto cifrado a uno legible (texto original).

2.3 EFECTO AVALANCHA

Es la propiedad de los algoritmos de cifrado en virtud de la cual pequeños cambios en el texto de entrada producen cambios radicales en el texto cifrado (o encriptado).

En otras palabras, se dice que en promedio la mitad de los bits de salida debe cambiar cada vez que cambia una entrada de un solo bit. Esta es una característica deseable, ya que indica que cada bit de salida debe depender de todos los bits de entrada. Los algoritmos

con esta propiedad no representan correlación estadística entre la entrada y la salida, lo cual los hace más seguros [Aut].

2.4 CRIPTOANÁLISIS

Es el estudio de los métodos utilizados para romper textos cifrados, con el objetivo de recuperar la información original, sin usar una llave.

2.5 MÉTRICAS DE RENDIMIENTO

Para estudiar el rendimiento de la implementación, se siguen los lineamientos expuestos por el cuerpo docente, en donde se debe cambiar el tamaño de los bloques y tomar el tiempo. Se debe realizar al menos 4 variaciones al tamaño de los bloques. Por otro lado se debe calcular el *throughput* de las variantes observadas. Para el diseño de sistemas de ecriptación simétrico el *throughput* está dado por la Ecuación 2.1.

$$throughput = \frac{Tamano_{bloque}}{Tiempo_{encriptacion}} \tag{2.1}$$

CAPÍTULO 3. EXPLICACIÓN DEL ALGORITMO DE ENCRIPTACIÓN

La implementación consta de un híbrido de dos procedimientos para poder encriptar y desencriptar, los cuales se explican a continuación:

3.1 CIFRADO DE FEISTEL

Corresponde a un cifrado por bloque, en donde se realiza ciertas operaciones un determinado número de veces. Para realizar este cifrado se deben realizar los siguientes pasos:

1. A partir de un texto que se quiera transmitir, éste se divide en dos subcadenas; cada una de las cadenas tiene el mismo tamaño.

2. Se selecciona una función F y una llave K_i.

3. Se opera con F y K_i con una de las subcadenas definidas en el primer paso.

4. La cadena obtenida se cambia por la subcadena que no ha sido operada, y se alterna el procedimiento.

Para comprender de mejor forma dicho método véase Figura *3-1*. El procedimiento de desencriptar opera de manera similar, ya que solo se cambia la entrada del cifrado de Feistel por un texto cifrado por el mismo encriptador.

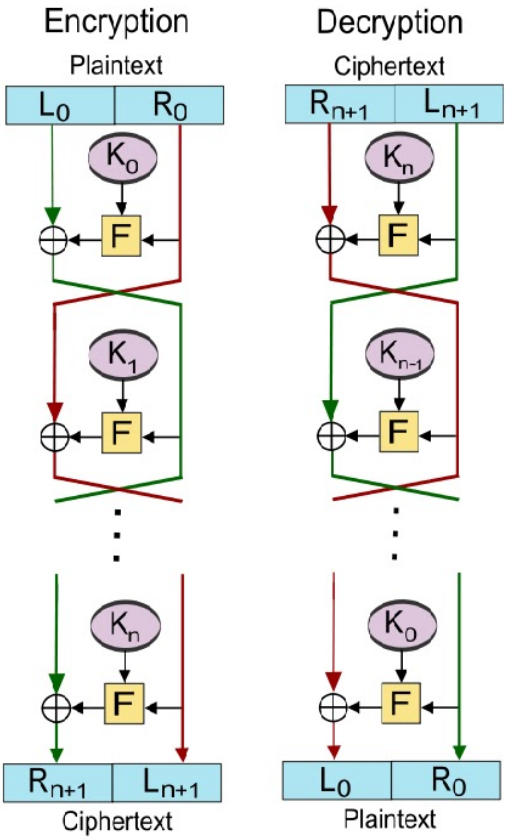

Figura 3-1: Cifrado de Feistel

3.2 CIPHER-BLOCK CHAINING

Este corresponde a un modo de operación de cifrado por bloques, en donde a cada bloque se le realiza un operación *exclusive-or* (XOR) con el bloque anteriormente cifrado. Con la funcionalidad de este modo, se genera una dependencia del bloque actual con respecto a los anteriores. Es importante destacar, que se necesita de un vector de inicialización para el bloque inicial, siendo este un bloque de bits que permite hacer el aleatorio el proceso de encriptación. Para entender el procedimiento que utiliza este modo véase Figura *3-2*.

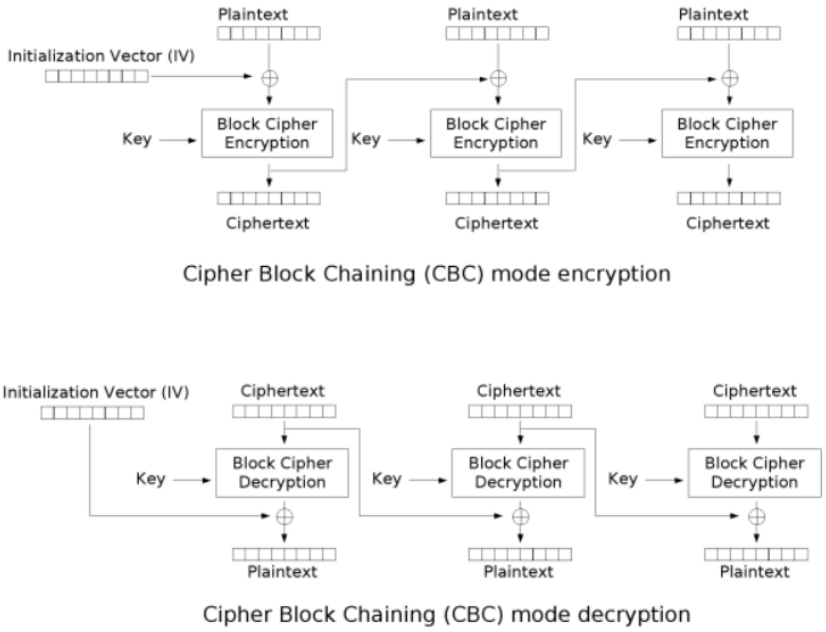

Figura 3-2: Modo de operación Cipher-block Chaining

3.3 HÍBRIDO

La encriptación propuesta se ha denominado cifrado de JAD (por el nombre de los autores del desarrollo de esta experiencia; Javier, Andrés y Diego), el cual es un acrónimo de los desarrolladores que lo implementaron. Cabe recalcar que el alfabeto utilizado corresponde al ASCII.

3.3.1 Encriptación

Para la encriptación del texto se realizan los siguientes pasos:

1. Generar las llaves, para este algoritmo se usan 16 llaves, ya que es una por cada ronda realizada en el método de cifrado de Feistel. Para generar las K_n se aplica el cifrado César con un corrimiento de n a *password*.

2. Encriptar el texto con cifrado de Feistel. Donde la función *F* que se muestra en la Figura 3-1 corresponde a un *OR* exclusivo (*XOR*) entre la llave generada y el bloque correspondiente. Es decir para la iteración cero, por ejemplo, aplica la función (*XOR*) entre la llave K_0 y el sub-bloque R_0.

3. Finalmente, se aplica CBC entre los bloques encriptados con Feistel, utilizando como vector de inicialización una lista de elementos nulos.

3.3.2 Desencriptación

Para la desencriptación del texto se realizan los siguientes pasos:

1. Generar las 16 claves,realizando el mismo método para generar las llaves de encriptación, ya que estas llaves deben ser las mismas.

2. Desencriptar el texto cifrado con Feistel.

3. Desencriptar el texto cifrado con César, utilizando la misma llave que se utiliza en el paso dos de encriptación.

El método implementado se encuentra en al archivo adjunto *jad.py*.

CAPÍTULO 4. EVALUACIÓN DEL ALGORITMO

Para evaluar el algoritmo se han realizado diversas pruebas, de tal forma se miden los tiempos de ejecución para cada contexto. Para calcular el *throughput* se ha ocupado la Ecuación 2.1 explicado en el Capítulo 2. Los diversos contextos están marcados por la variación de los tamaños del bloque, tal como se ve en el Cuadro 4.1.

Las condiciones para las pruebas fueron las siguientes:

- *Password*: holacomo

- Texto a cifrar: *Lorem ipsum dolor sit amet consectetur adipiscing elit lectus justo, class nam sed non scelerisque curae risus augue mi netus, nulla eget senectus fames ultricies cras natoque quisque. Cursus tempus hendrerit nisl lacinia integer mi, fermentum faucibus purus torquent condimentum a, risus donec velit quisque aptent. Et cras in fames lobortis eleifend cubilia nam nibh vulputate hendrerit, bibendum at scelerisque quam rutrum turpis quisque curae quis sem varius, sapien non velit mi imperdiet cursus semper laoreet volutpat. Viverra odio nulla conubia venenatis mi enim volutpat mauris aliquam, dignissim semper habitasse euismod sem massa nullam donec sollicitudin taciti, egestas feugiat facilisi nibh magnis habitant fringilla quisque.Vestibulum ultricies volutpat nibh ante purus accumsan suscipit ligula, eget vehicula tempus quis turpis lacinia torquent ullamcorper condimentum, pharetra fringilla semper vel praesent sociosqu aliquam. Netus donec curae leo ridiculus ac sociosqu, fusce feugiat sociis justo nec, ullamcorper porta quam platea massa. Nisl sociosqu velit sed hac urna purus augue viverra nulla lacinia sociis, eu habitasse parturient faucibus est erat aptent quisque interdum. Sagittis in dis aptent facilisi primis magna montes quisque facilisis eleifend magnis, sociis tempor hac vulputate orci dignissim nec tortor cum.*

Tamaño de bloque [bytes]	Throughput	Tiempo[s]
1	1.6285	0.5780
2	6.8353	0.2925
4	24.4678	0.1634
8	77.1428	0.1037
16	239.3053	0.0668
32	856.6853	0.0347

Cuadro 4.1: Throughput y tiempos por tamaño de bloque

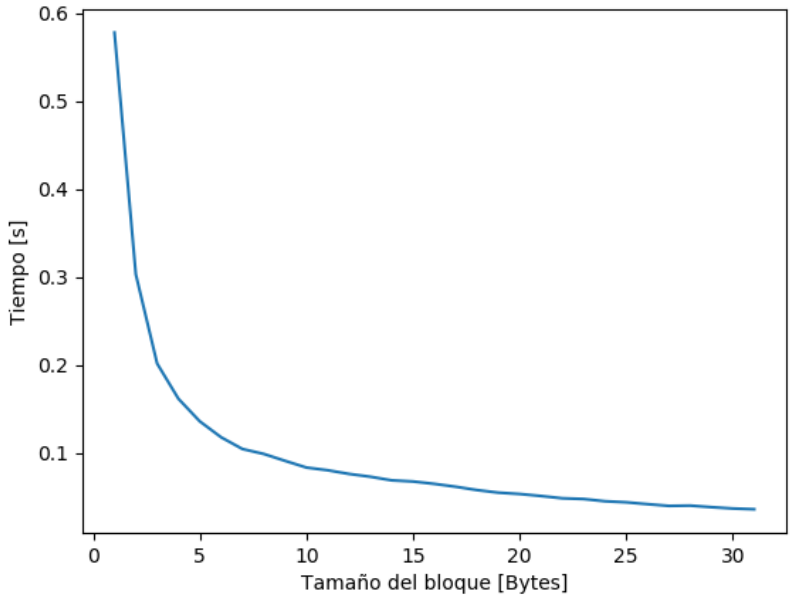

Figura 4-1: Tamaño del bloque versus tiempo

Como se puede apreciar en el gráfico anterior, el tiempo de encriptación de un texto, va disminuyendo a medida que el tamaño del bloque aumenta. Este fenómeno que se observa, es debido a que cuando aumenta el tamaño del bloque la cantidad de operaciones realizadas disminuye, al haber menos bloques en los cuales hay que operar.

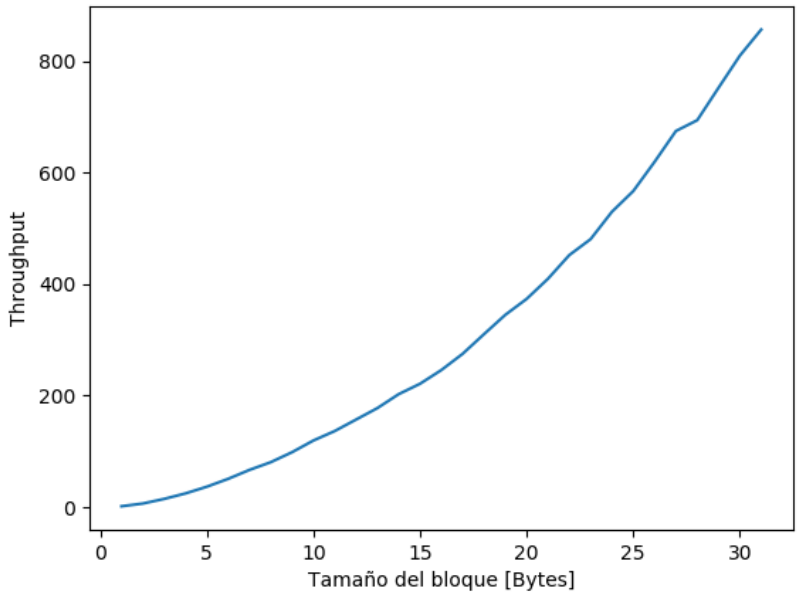

Figura 4-2: Throughput versus tiempo

Por otro lado, viendo la Figura *4-2* se observa un fenómeno contrario al analizado anteriormente, ya que a medida que el tamaño de los bloques aumenta, la tasa de transferencia efectiva de todo el texto va creciendo al momento de cifrar. Viendo esto desde otro punto de vista, como los tiempos decrecen, más caracteres del texto son cifrados, es por esto que se ve un crecimiento en el *througput* al realizar la encriptación.

CAPÍTULO 5. CRIPTOANÁLISIS

El algoritmo de encriptación creado, utiliza una llave de 8 caracteres. Esto quiere decir de que el tamaño de la clave es de 8 bytes, ya que cada caracter tiene un tamaño de un byte. Como bien se sabe cada byte tiene 8 bits, por lo tanto el tamaño de la clave en bits, es de 64 bits. Expuesto lo anteriormente dicho, la cantidad de combinaciones posibles para la clave de este algoritmo es de 2^{64}, lo cual es una gran cantidad de combinaciones de caracteres. Esta clave está definida inicialmente, pero la forma en que se generan otras 16 claves a partir de esta, es una fórmula definida por los autores de este experiencia.

Clave	**Bit a bit**	**Byte a byte**
password bassword	9 %	25 %
password bbssword	26 %	50 %
password bbbsword	40 %	68 %

Cuadro 5.1: Efecto avalancha al cambiar la clave de encriptación

Por otro lado, a pesar de haber usado Feistel como base del algoritmo creado para la encriptación y el modo de operación por bloques *Cipher-block Chaining*, los cuales ayudan a proveer el efecto avalancha en los cifrados, estos no aseguraron completamente que el algoritmo creado cumpla con la difusión del mensaje, la cual nos dice que si cambia un bit en el texto de entrada, se modifica aproximadamente el 50 % del texto de salida. Una teoría de por que no se cumple este efecto, es porque no se realizan permutaciones en el texto de entrada inicial, lo cual afectaría enormemente, ya que al aplicar esto, la difusión sería mayor, debido al uso de CBC, la cual genera una dependencia en el bloque a cifrar con respecto al bloque anterior. Cabe recalcar que mientras mayor sea la cantidad de bloques, debería existir una mayor difusión, ya que los bloques cifrados irán dependiendo de una mayor cantidad de bloques.

CAPÍTULO 6. CONCLUSIÓN

Considerando los objetivos planteados en el Capítulo 1, se puede decir que el grupo de trabajo ha cumplido a cabalidad con estos; dado que se ha logrado aprender la teoría planteada en cátedra de una manera más práctica. En cierto rigor, se logró comprender como funcionan los encriptadores simétricos, llevándose a cabo el estudio en conjunto con la implementación del encriptador JAD.

Sin lugar a dudas, como en toda experiencia tecnológica se ha tenido una gran variedad de complicaciones, ya que no se sabía usar las herramientas de forma adecuada en base a la teoría de encriptadores; en donde, se ha tenido que estudiar a fondo la implementación de otros cifradores simétricos, con el fin de realizar un cifrador que funcione.

El cifrador implementado funciona de manera correcta, por otro lado, en base a los resultados obtenidos en el Cuadro 4.1, se puede decir que a mayor tamaño de bloque, el tiempo de ejecución disminuye de manera considerable; esto ocurre por la cantidad de operaciones que se realizan al cifrar o descifrar.

El desafío de esta experiencia ha sido enriquecedor, ya que se ha superado con éxito, lo cual indica que los estudiantes han aprendido la teoría expuesta en la sala de clases, es decir se ha llegado a la meta de este estudio. Se espera seguir aplicando los conocimientos adquiridos para las futuras entregas, ya que gran parte de esta experiencia es la base de las redes de computadores.

CAPÍTULO 7. BIBLIOGRAFÍA

[Ang00] José de Jesús Angel Angel. «Criptografía para principiantes». En: *Obtenido en la Red Mundial el* 5 (2000).

[Sta04] William Stallings. «Comunicaciones y Redes de Computadores». En: Pearson Educación, S.A., 2004.

[Aut] Varios Autores. *Simulación del Estándar de Cifrado Avanzado para VoIP*. URL: https://sg.com.mx/revista/simulaci%C3%B3n-del-est%C3%A1ndar-cifrado-avanzado-para-voip.

[Rey] Pablo Reyes. *Laboratorio 2 Sistemas de Comunicación*.