TÓPICOS SELECTOS DE CRIPROGRAFÍA I

AUTORES

Víctor Manuel Silva García

Rolando Flores Carapia

Marlon David González Ramírez

Editorial CIDETEC-IPN.

# CAPÍTULO I

**1.1. Introducción.**

Hay varios tópicos que se abordarán en el marco de la Criptografía. Uno de ellos se refiere al cifrado de imágenes utilizando criptosistema simétricos.

El cifrado de imágenes puede realizarse de varias formas, por ejemplo: utilizando un criptosistema asimétrico, empleando el Caos y en general, hay diversas maneras para cifrar imágenes y, algunas de ellas muy ingeniosas [1, 2, 3]. En esta obra se presentan algunos algoritmos originales de cifrado de figuras, los cuales son producto de algunos años de investigación de los autores. También, se señala que los autores usan como sinónimos las palabras imagen y figura en el cifrado de imágenes

Se aclara, que parte del material utilizado en este trabajo se toma de los estándares internacionales, como por ejemplo: FIP PUB 46-3, FIPS PUB 197, NIST Special Publication 800-67 y algunos otros que cuando se aborden serán citados. Por otro lado, se menciona que el tipo de imágenes que se encriptan tienen las siguientes características: pueden ser de diferentes niveles de gris (256), o a color, teniendo como colores básicos al rojo, verde y azul; donde cada uno de ellos a su vez tiene 256 niveles de intensidad.

El modo de encriptar una figura en este trabajo es sin compresión, ya que hay algunas áreas de aplicación donde no deben comprimirse las imágenes, como por ejemplo: el Ejército, la Astronomía y Cinematografía etc. De hecho, también lo establece la norma mexicana NOM - 151 - SCFI – 2002 prácticas comerciales. En este sentido, las figuras que se cifran están en el formato “Big Map” - BMP.

Otro tópico importante trata de la medición de la aleatoriedad de los diferentes colores en una figura encriptada, ya que es importante evaluar la calidad del cifrado. En este marco, se presentan las siguientes herramientas: Entropía de la información, Coeficiente de Correlación, algunas pruebas de la norma; NIST 800-22, además, se propone una medición de la aleatoriedad de acuerdo con una “Prueba de Bondad de Ajuste”, la cual usa la distribución . Dentro de las pruebas de la NIST 800-22 que se usan, está la Transformada Discreta de Fourier—TDF—la cual una herramienta importante en la medición de la aleatoriedad de las imágenes encriptadas, de hecho, TDF es una herramienta que consiste en una prueba de hipótesis.

Por otra parte, para determinar qué tan resistentes son los algoritmos de cifrado ante el ataque diferencial a imágenes cifradas, se emplean los siguientes instrumentos: Number of Pixels Change Rate – NPCR, Unified Changing Intensity – UACI y Avalanche Criteria – AC [4].

También, se expresa y se demuestra el Teorema JV, ya que éste es importante en el desarrollo de los algoritmos de encriptación de figuras. A grandes rasgos se menciona que este Teorema nos indica la manera de asociar a un entero no negativo una permutación. De hecho, es posible construir una permutación aleatoria de 300,000 posiciones en un tiempo menor a 10 milisegundos. En este sentido, es conveniente hacer un pequeño repaso de la aritmética modular.

Las cajas de substitución son un elemento importante en los algoritmos simétricos de cifrado; particularmente la no-linealidad y el Differencial Power Analysis – DPA de éstas son muy importante. En este orden de ideas, la medición de la no-linealidad es una herramienta que también se muestra en este trabajo, así como, un software para calcular el DPA. Por otro lado, se construirán cajas diferentes a la de las normas y con una no-linealidad bastante aceptable, además, de un DPA menor a la caja de la norma, esto es, Advanced Encryption Standard – AES. Lo anterior, para que no puedan realizarse los ataques diferencial y lineal [5, 6].

Las funciones Has Sha serán también objeto de estudio, ya que la firma digital como elemento de no-repudiación es importante en una estructura de comunicación segura. Además, se desarrolla una técnica para generar una llave de manera seudo-aleatoria, y hacerla depender de la imagen que se cifra, más adelante se ilustrará este punto.

En este libro no se analizan los tipos de cifrado antiguo y clásico, por ejemplo: cifrado Cesar, Vigenere, Substitución, Hill etc. Digamos que se parte del criptosistema simétrico Data Encryption Standard – DES en adelante. Aunque DES ya no está en uso, si lo está Triple – DES que es una consecuencia directa de él.

**1.2. Motivación.**

Es claro para todos que hay información sensible en las diferentes áreas de la actividad humana, por ejemplo: el Ejercito, los Bancos, grandes Corporativos, la Cinematografía etc. También, que esta información está en muchas ocasiones en imágenes.

Entonces, aquellos lectores que están interesados en el cifrado de información, específicamente de imágenes, en esta obra encontrarán algoritmos originales de encriptación usando criptosistemas simétricos; esto es, con la misma llave se cifra y descifra la información. Por otra parte, todos los criptosistemas utilizan un alfabeto para los textos planos y un alfabeto para los textos cifrados, digamos que en un caso particular se pueden emplean como alfabeto el código ASCI para ambos casos, textos planos y cifrados. Se aclara que el código ASCI tiene 256 símbolos. También, se sabe que los ataques o criptoanálisis tratan de averiguar alguna relación entre los textos cifrados con los textos planos.

En este orden de ideas, la explicación de por qué convertimos a los mensajes en imágenes se debe a lo siguiente: el alfabeto, tanto para texto plano como para texto cifrado son colores. Los colores se trabajan con pixeles o cadenas de 24 bits, en este sentido, se tiene posibles símbolos, lo que significa 16 777 216 posibilidades. Entonces, es sencillo observar que lo anterior complica mucho más a los ataques que pudieran presentarse, para los criptosistemas que serán propuestos.

En otro orden de ideas, la razón de proponer algoritmos simétricos para el cifrado de imágenes, se debe a que éstos son muy rápidos en el cifrado de las figuras, además, son seguros. El inconveniente que tienen los sistemas simétricos es la distribución de llaves. Sin embargo, este problema se resuelve con un criptosistema asimétrico. En el transcurso del libro se propone un caso en que la curva elíptica (un criptosistema asimétrico) nos sirve para construir un criptosistema simétrico, y en este caso, con la misma la curva se distribuyen las llaves.

El método de Diffie Hellman empleando la curva elíptica, es un procedimiento para construir una llave pública que conozcan solamente los involucrados en un esquema de comunicación segura, como por ejemplo, un PKI [7].

Por otro lado, también es posible realizar cifrado de figuras de buena “calidad” con criptosistemas asimétricos; pero, se tiene el problema que son demasiados lentos y si tratamos de cifrar película al mismo ritmo en que se está tomando, esto no sería posible. Asimismo, se hace hincapié en que el procedimiento de encriptación que se aplica aquí es sin compresión.

También, el cifrado de sonido puede llevarse a cabo utilizando criptosistemas simétricos. En principio, puede grabarse en un archivo un mensaje en forma oral; éste se cifra y posteriormente se envía por Internet. Después, el receptor descifra el mensaje encriptado y se entera de la información.

**I.3. Preliminares.**

Es conveniente revisar algunos conceptos básicos de criptografía. Iniciamos con el alfabeto de los mensajes claros o planos. Esto es, un mensaje debe ser escrito de acuerdo a un alfabeto; por ejemplo: Español, Inglés, binario, ASCI, colores etc.

Con base en lo anterior, el conjunto de posibles mensajes hechos de acuerdo con el alfabeto adoptado se denota como:.

De igual forma, hay un alfabeto para el texto cifrado, el cual no necesariamente es el mismo que el alfabeto del texto original o texto plano. En este sentido, puede ser; Español, Inglés, binario etc. Al conjunto de los mensajes encriptados se denota como sigue: .

También, se define el conjunto de claves o llaves como aquél cuyos elementos nos dan todas las posibles vías para encriptar un mensaje. Este conjunto se denota como: .

Se definen dos funciones que son uno a uno o inyectivas; a saber: la función que cifra y la que descifra. Generalmente, estas dos funciones se definen mediante un algoritmo.

La función que encripta se denota como: . Donde es el texto plano y es la llave, o sea, . Por otro lado, la función que descifra se escribe de la siguiente manera: . En este caso, representa el texto encriptado y la clave.

Más adelante se verá que la clave para encriptar y descifrar no necesariamente son iguales. De hecho, a los sistemas que cifran y descifran con la misma clave se llaman simétricos, y a los que utilizan claves diferentes se les llaman asimétricos o de llave pública.

Resumiendo; en todo criptosistema se requiere que este definida la siguiente tupla: {, , }, y además, dos funciones uno a uno y , las cuales sirven para encriptar y descifrar un mensaje.

Para revisar estos conceptos se muestra un procedimiento de cifrado del siglo XVI (1586). Este desarrollo se llama “Cifrado Vigenere”, y con el objeto de clarificar el proceso se construye la Tabla 1.3.1.

Tabla 1.3.1. Alfabeto Español

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |  |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |  |

La Tabla 1.3.1 define un mapeo que va del alfabeto a los naturales, esto es, se cuentan. El algoritmo de cifrado procede como sigue:

(1.3.1) mod. 27.

La expresión (1.3.1) utiliza la aritmética modular, o sea, los residuos [8]. Veamos un caso particular para ilustrar el punto. Suponga que el texto plano es: CURSODECRIPTOGRAFIA y la clave es ROLANDO.

Tabla 1.3.2. Procedimiento de cifrado, usando el método Vigenere.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Mensaje | C | U | R | S | O | D | E | C | R | I | P | T | O | G | R | A | F | I | A |
| Clave | R | O | L | A | N | D | O | R | O | L | A | N | D | O | R | O | L | A | N |
| Mensaje cifrado | T | J | C | S | B | G | S | T | G | S | P | G | R | U | J | O | P | I | N |

Hagamos el análisis de cómo se procedió con la primera letra; C y R tienen asociados los números 2 y 18, por lo tanto la suma es 20. El número 20 tiene asociado la letra T, tal y como aparece en la Tabla 1.3.2. Por otra parte, como estamos utilizando una clave de 7 letras, el número de elementos del conjunto es de .

**I.4. Contenido.**

Este trabajo está distribuido de la siguiente forma: el capítulo II muestra los criptosistemas simétricos más importantes; esto es, los que están o estuvieron en la norma internacional NIST [9]. También, se añade un criptosistema que fue propuesto por los autores [10]. En el capítulo III se hace una revisión de las herramientas que miden el grado de aleatoriedad de una imagen encriptada, además, se presentan algunos parámetros para medir la fortaleza de los sistemas criptográficos.

En el cuarto, se construye un algoritmo que define una función biyectiva, la cual nos es de utilidad para generar cajas de substitución y permutaciones.

Del capítulo V al VII, se hace una presentación de los siguientes criptosistemas asimétricos: RSA – Rivest, Shamir y Adleman; Curva Elíptica y ElGamal. Estos criptosistemas nos serán de utilidad para distribuir las llaves de los simétricos, además de la firma digital.

En el octavo se ven dos modelos dinámicos para producir el Caos, y en el capítulo IX se aborda los modelos para la firma digital, incluyendo un esquema de firmado que usa un modelo pos-cuántico.

El capítulo X, el último, aplica algunos modelos de cifrado a las imágenes a color.

Ejercicios.

1. Construya un Sistema de cifrado Vigenere, utilizando como clave su nombre y como texto plano Escuela Superior de Cómputo, además, conteste las siguientes preguntas:
2. Diga cuál es el conjunto de textos planos .
3. Diga cuál es el conjunto de textos cifrados .
4. Diga cuál es el conjunto de llaves .
5. Proponga un texto plano, y posteriormente aplique una permutación sobre las posiciones para obtener el texto cifrado. Por otro lado, resuelva el siguiente inciso.
6. Diga cuál es el conjunto de las llaves .

Bibliografía

[1] Jian Li and li Gan, Study on Chaotic Cryptosystem for Digital Image Encryption, Third International Conference Measuring Technology and Mechatronics Automation, IEEE 426-430, 2011.

[2] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, Vol. 20, Optics Express, 2012.

[3] Mohamed Amin and Ahmed Abd El-Latif, Efficient modified RC5 based on chaos adapted to image encryption, Journal of Electronic Imaging 19(1), 013012, 2010.

[4] X. Wang, H. Zhao, and M. Wang, “A new image encryption algorithm with nonlinear diffusion based on multiple coupled map lattices”, Opt. Laser Technol., vol. 115, pp. 42-57, Jul, 2019.

[6] Biham E. and Shamir A., Differential cryptanalysis of the full 16-round DES. Lecturer Notes in computer Science, pp. 494-502, 1993.

[6] Matsui M. Linear Cryptanalysis for DES cipher. Lecture Notes in Computer Science, pp. 386-397, 1994.

[7] Höglund J, Joel and Lindemer, Samuel and Furuhed, Martin and Raza, Shahid, Towards public key infrastructure for the Internet of Things, Computers & Security, Vol. 89, pp. 101658, 2020.

[8] Koblitz M., A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1987.

[9] FIPS PUB 46-3. Federal Information Processing Standards Publication, 1999

[10] V.M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso,”Triple-DES-96 Cryptographic System”, Vol. 8 No 19, pp. 925-934, Hikari LTD, 2013.