Criptografía Visual

Erick M.

22 de agosto de 2024

Índice

Resumen

Breve descripción de criptografía visual.

1. Introducción

Supongamos que María quiere transmitir un mensaje a Pedro, de tal forma que si alguien obtiene o intercepta el mensaje, no sepa que información contiene. Para lograr esto se han creado métodos que permiten el cifrado de un mensaje, de tal forma que solo los receptores autorizados puedan descifrarlo. La ciencia encargada del estudio de sistemas de cifrado y descifrado de mensajes es la criptología.

La criptología se divide en dos grandes áreas principalmente, la criptografía que es el estudio de métodos para cifrar y descifrar mensajes y el criptoanálisis que estudia los procedimientos para descifrar un mensaje cifrado sin conocer la clave.

Los términos usados frecuentemente en la criptología:

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

1.1. Antecedentes

El cifrado de texto ha sido ampliamente usado a lo largo de la historia humana, principalmente en el ámbito militar y en aquéllos en los que es necesario enviar mensajes con información confidencial a través de medios no seguros.

1.1.1. Criptografía clásica

Uno de los sistemas criptográficos mas antiguos conocido se debe a Julio César. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante en el alfabeto latino.

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I	...	A	B	C

Tabla 1: Correspondencia del cifrado de Julio César en la mayoría de los idiomas actuales

Así, si queremos cifrar un mensaje sencillo como ≪CRIPTOGRAFIA VISUAL≫ basta con sustituir cada letra según la correspondencia de la Tabla 1 por lo que el mensaje cifrado sería ≪FULSWRJUDILD SLVXDO≫.

Debemos considerar que cualquier símbolo que aparezca en el mensaje original debe estar relacionado con otro, de tal manera que cuando el receptor reciba el mensaje cifrado pueda descifrarlo correctamente y sin ambigüedad, es decir, que para cada símbolo del texto cifrado debe estar seguro de que uno y sólo un símbolo del texto claro le corresponde; en otras palabras, la función de cifrado debe ser biyectiva.

A este tipo de criptosistemas, en el que la correspondencia entre el alfabeto de escritura y cifrado es la misma y se mantiene fija durante todo el proceso de cifrado y descifrado, se les conoce como *"sustitución monoalfabético"* o *"cifrado monoalfabético"*.

El criptosistema mencionado anteriormente pertenecen al grupo de la criptografía simétrica. La criptografía simétrica es un método criptográfico en el que se usa la misma clave para cifrar y descifrar. Su seguridad radica en la clave, es decir, aunque un atacante conozca perfectamente el algoritmo, esto no le ayuda a descifrar el criptotexto; sin embargo, tanto el emisor como el receptor deben conocer la clave, por lo que es fundamental mantenerla en secreto, lo que nos lleva a las principales desventajas de estos sistemas, la distribución de las claves, el peligro de que varias personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

En contraparte está la criptografía asimétrica, la cual usa dos claves, una para cifrar y otra para descifrar. Existen criptosistemas en los cuales conociendo la clave de cifrado es fácil obtener la clave de descifrado o viceversa. Un caso particular de estos criptosistemas, en donde esto no ocurre, son conocidos como criptosistemas de llave pública.

1.1.2. Criptografía moderna

La criptografía moderna tiene sus comienzos con Claude E. Shannon. En 1949 publicó el artículo *Communication Theory of Secrecy Systems* en la Bell System Technical Journal y poco después el libro *Mathematical Theory of Communication* con Warren Weaver. Estos trabajos, junto con algunos otros que publicó, sentaron las bases téoricas para la criptografía y el criptoanálisis moderno.

Por mucho tiempo la criptografía estuvo restringida a organizaciones gubernamentales secretas, como la NSA, por lo que muy pocos trabajos se hicieron públicos; sin embargo, a mediados de la década de los setenta esto cambió.

2. Criptografía Visual

La criptografía visual es una técnica de encriptación especial para ocultar información en imágenes de tal manera que pueda ser desencriptada por la visión humana si se usa la imagen clave correcta. La técnica fue propuesta por Naor y Shamir en 1994. La criptografía visual utiliza dos imágenes transparentes. Una imagen contiene píxeles aleatorios y la otra imagen contiene la información secreta. Es imposible recuperar la información secreta de una de las imágenes. Se requieren tanto imágenes transparentes como capas para revelar la información. La forma más sencilla de implementar la criptografía visual es imprimir las dos capas en una hoja transparente.

Referencias

[Cri] *Visual Cryptography*. https://www.ciphermachinesandcryptology.com/en/visualcrypto.htm.