Criptografía

José Galaviz

Criptología

Disciplina encargada del estudio de los mecanismos que permiten el intercambio de información entre un emisor y un receptor autorizados, sin que un tercero pueda acceder a dicha información, así como de los medios que este último puede utilizar para tratar de accederla.

Criptografía

Estudio de los mecanismos, algoritmos, protocolos y sistemas usados para cifrar mensajes, es decir, ocultar a terceros el significado de los mensajes que se intercambian un emisor y un receptor autorizados.

Criptoanálisis

Estudio de las técnicas heurísticas usadas para tratar de descifrar mensajes cifrados sin poseer todos los elementos para hacerlo.

Esteganografía

Estudio de las técnicas y algoritmos usados para ocultar a terceros la existencia de los mensajes secretos que intercambian un emisor y un receptor autorizados.

Estegoanálisis

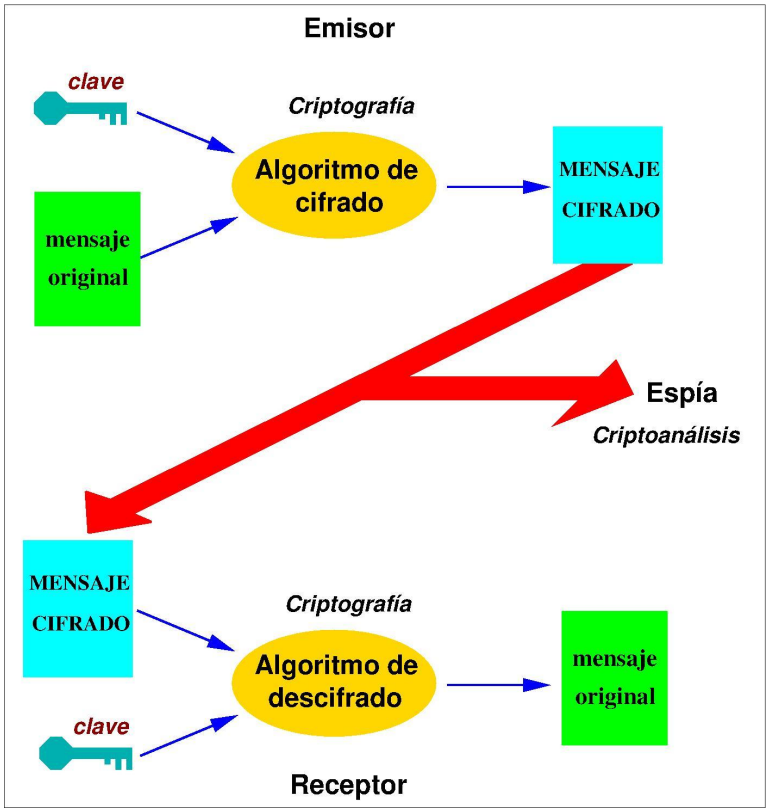
Estudio de las técnicas y heurísticas usadas para encontrar mensajes ocultos mediante técnicas esteganográficas, sin poseer todos los elementos para hacerlo.

Elementos presentes 1/2

- **Emisor** de mensajes cuyo significado debe ser conocido sólo por él y el receptor.
- **Receptor**, destinatario de mensajes cuyo significado puede conocer.
- **Enemigo** que está en escucha permanente del canal de comunicación usado por el emisor y el receptor. Puede escuchar y almacenar los mensajes que transitan por el canal. Desea conocer su significado.
- **Canal de comunicación**, confiable en términos de integridad de lo que transita, pero inseguro, permanentemente intervenido por el enemigo.

Elementos presentes 2/2

- **Mensaje claro** inteligible por cualquier persona en contexto, cuyo significado desean compartir el emisor y el receptor.
- **Mensaje cifrado** ininteligible para cualquiera, que viajará por el canal y que contiene oculto, el significado del mensaje claro original.
- **Claves** o **llaves** de cifrado y de descifrado. Elementos adicionales que se suministran respectivamente a los algoritmos de cifrado y de descifrado como parte de su entrada. Determinan el resultado obtenido a la salida de estos.
- **Algoritmo de cifrado**. Recibe como entrada el mensaje claro y la clave de cifrado y obtiene a la salida el único mensaje cifrado que corresponde con esa pareja.
- **Algoritmo de descifrado**. Recibe como entrada el mensaje cifrado y la clave de descifrado y obtiene a la salida el único mensaje claro que corresponde con esa pareja.



Nomenclatura

Texto claro (plain): Texto escrito de manera inteligible por los interlocutores y por el espía.

Criptograma: Mensaje cifrado, también llamado criptotexto.

Alfabeto: Conjunto de símbolos usados para escribir mensajes o para expresar los criptogramas.

Cifrar (encriptar). Acción de transformar un mensaje en texto claro en un criptograma.

Sistema criptográfico. El (los) algoritmos usados para cifrar, el (los) algoritmos usados para descifrar (funciones de cifrado y descifrado), el conjunto de todas las posibles claves de cifrado y de descifrado (espacio de claves), el conjunto de todos los posibles textos claros y de todos los posibles criptogramas (espacio de texto claro y espacio de criptotexto). También se llama **criptosistema**.