

# Criptografía y Blockchain

Módulo 3

# Esteganografía

# Esteganografía: generalidades

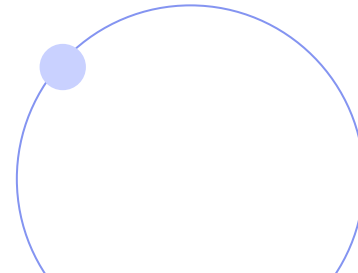
El término **esteganografía**, cuyo origen etimológico proviene de las palabras griegas *steganos* (oculto) y *graphein* (escribir), puede definirse como **escritura oculta**.

En general, se traduce del término inglés *steganography*, que a su vez proviene del título del libro *Steganographia*, escrito por el abad alemán Johannes Trithemius (1462-1516) en el año 1499.



## Términos y sus definiciones

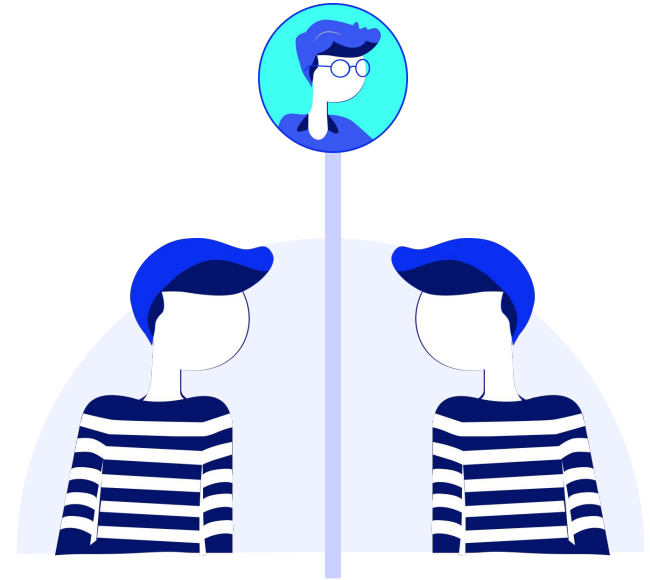
- La **esteganografía** estudia diferentes procedimientos para ocultar información, almacenándola en algún soporte o transmitiéndola por algún canal.
- El **estegoanálisis** estudia la seguridad de los diferentes algoritmos esteganográficos, aplicando diferentes procedimientos para detectar la posible presencia de información oculta en un medio o bien para eliminarla, se tenga certeza de que existe o no.
- El **estegomedio** es el medio o soporte de comunicación que se utiliza para enmascarar la información a transmitir sin levantar sospecha.
- El resultado de ocultar una información en un estegomedio da lugar a un **estegoobjeto**.



# El problema del prisionero

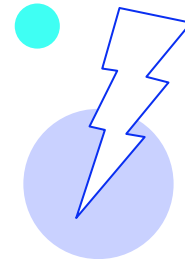
(G. J. Simmons, 1983). Dos personas **A** y **B**, arrestadas y confinadas en celdas separadas deben **coordinar un plan de fuga**, **intercambiando información a través de su guardián**, dado que se les impide una comunicación directa.

Si el guardián tiene la más mínima sospecha interrumpirá las comunicaciones. De este modo, **A** y **B** deben comunicarse usando algún tipo de **esteganografía**.



Los comportamientos posibles del guardián (atacante) son:

1. **Ataque pasivo:** el guardián puede analizar la información intercambiada, dejando que la comunicación tenga lugar si no advierte nada raro.
2. **Ataque activo:** el guardián podría modificar la información, accidentalmente o a propósito, e incluso dañándola significativamente.
3. **Ataque malicioso:** el guardián puede modificar a su antojo la información ocultada en una cubierta con la intención de provocar una acción determinada en las entidades receptoras de dicha información (casi imposible).



# Tipos de sistemas esteganográficos

## Estegosistemas de clave simétrica

Es el esquema **más común**. El emisor y el receptor comparten una **clave secreta (estegoclave)** y toda la seguridad del sistema descansa en ella.

Lo normal es que el algoritmo esteganográfico y el tipo de tapadera utilizados sean públicos y así un atacante no podrá detectar ni recuperar la información enmascarada sin la estegoclave.

## Estegosistemas de clave pública

Son aquellos sistemas que **requieren el uso de dos claves**:

- una **pública** para el proceso de ocultación y
- una **privada** para obtener el mensaje oculto.

## Estegosistemas cuánticos

Estos sistemas **aprovechan los conocimientos sobre física cuántica** para diseñar sistemas que faciliten la ocultación de información.

Existen varias formas de realizar esto, por ejemplo, aprovechándose del ruido cuántico o de los códigos correctores de errores cuánticos.

# Algoritmos esteganográficos

## Sus características son:

- **Capacidad** (cantidad de información que puede capacidad ser ocultada).
- **Seguridad / Invisibilidad** (probabilidad de detección por un estegoanalista).
- **Robustez** (cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta).

## Existen 3 grandes líneas de creación de algoritmos esteganográficos:

1. *La cubierta existe y la ocultación produce alteraciones.*
2. *Generación automática de la cubierta ocultando información en ella.*
3. *La cubierta existe y la ocultación de información no la modifica.*





# Técnicas esteganográficas

En las próximas diapositivas, veremos las siguientes técnicas esteganográficas:



- Ocultación en imágenes digitales.
- Ocultación en audio digital.
- Ocultación en sistemas de archivos y formatos.
- Esteganografía en código HTML/XML.
- Canales encubiertos en protocolos de comunicación.

## Ocultación en imágenes digitales

Existen **técnicas para formatos variados**, como PNG, GIF, BMP o JPEG.

Estas técnicas se utilizan principalmente como **herramientas de ocultación de comunicaciones digitales**, o en *malware* moderno para evasión de medidas de seguridad perimetral. Veamos en detalle cada una, a continuación:



- **Técnica *LSB* (último bit significativo):** es la técnica más común. Es de fácil aplicación, permitiendo ocultar grandes cantidades de información con poco impacto sobre el estegomedio. Resistencia media al estegoanálisis.
- **Utilización de *coeficientes cuantificados DCT* (transformada discreta de coseno):** es otra técnica muy habitual. A diferencia de LSB, que oculta mucha información, su capacidad de ocultamiento es menor. Alta resistencia al estegoanálisis.

- **Estegomalware:** en imágenes digitales, permite ocultar los datos de configuración del *malware* y la comunicación C&C (conexión *malware* servidor), o utilizar las imágenes como canal encubierto para el robo de información.
- **Polyglot:** permite que un archivo con un formato determinado se comporte como otro. De esta manera, se puede incrustar el código del *exploit* del *malware* mediante LSB para que la imagen sea interpretada como Javascript, HTML, pdf, etc.

## Ocultación en audio digital

Se destacan las **técnicas basadas en LSB**, en ocultación en la fase de una señal (***phase coding***), en el eco de una señal (***echo hiding***), ocultación estadística, etc. No es muy común.



## Ocultación en sistemas de archivos y formatos

Comprenden las técnicas de ocultación basada en la **fragmentación interna de los sistemas operativos** (*slack space*), mediante **borrado de archivos** (*unallocated file space*), **técnicas EoF** (*End of File*), **ocultación en flujos de datos alternativos en NTFS** (*ADS en NTFS*).

## Esteganografía en código HTML/XML

Ocultación basada en:

- **Caracteres invisibles.**
- **Codificación de caracteres.**
- El **orden de atributos** de una etiqueta.



## Canales encubiertos en protocolos de comunicación

Un *canal oculto* es aquel **canal de comunicación que viola alguna política de seguridad del sistema donde reside.**

Se utilizan para fuga de información y control remoto de equipos/software.

Hoy en día, se utiliza el **estegoanálisis mediante algoritmos de *machine learning***. Algunos de los protocolos de comunicación utilizados son: *HTTP, TCP, UDP, IPv4, IPv6, ICMP, IPSEC, IGMP, FTP, DNS, 802.2, 802.3*, redes inalámbricas, etc.

Otras técnicas son: *esteganografía multinivel (MLS)* e *Inter-protocolos (IPS)*.



# Técnicas de estegoanálisis

- **Detección estructural de LSB** (ataques estadísticos por análisis de pares de muestras, ataques RS, ataques triples, etc.).
- **Ataques de calibración a esteganografía JPEG** (se fuerza la recompresión de una imagen JPEG para obtener una nueva imagen con propiedades estadísticas similares a las de la imagen de cobertura).
- **Ataques de fuerza bruta.**
- **Estegoanálisis por *Machine Learning*.**



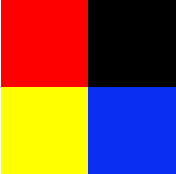
# Ejemplos

Imagen original

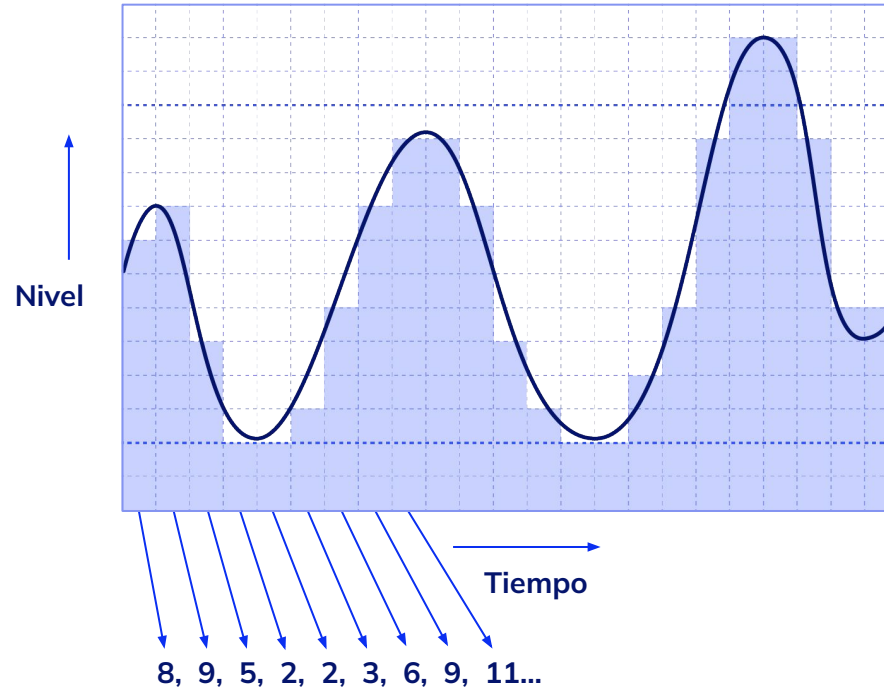
	11111111	00000000
	00000000	00000000
	00000000	00000000
	11111111	00000000
	11111111	00000000
	00000000	11111111

BIT MENOS  
SIGNIFICATIVO

Imagen modificada

	11111101	00000011
	00000010	00000001
	00000000	00000010
	11111100	00000011
	11111101	00000001
	00000001	11111100

c                      a                      t  
 01 10 00 11      01 10 00 01      01 11 01 00





**¡Sigamos  
trabajando!**