CURSOS INTERSEMESTRALES

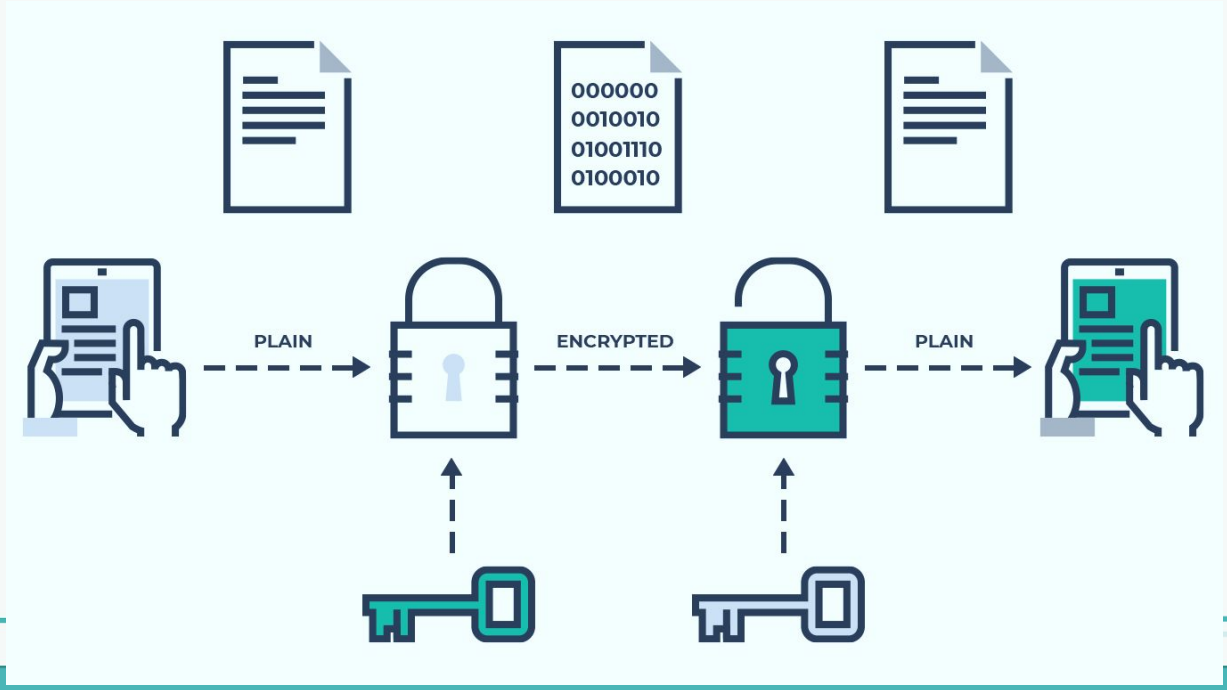
PROTECO

Seguridad

Cifrados..

Cifrado.

Método que permite transformer data legible a un formato ilgegible (cifrado) a modo que se mantenga confidencial y privado.



PROTECO

Cifrado.

Cosas a tomar en cuenta:

*)A pesar de ser una gran arma, no es una panacea.

*) Rara vez se rompen, generalmente se saltan.

*) Tanto el algoritmo como la llave, modifican la fuerza del cifrado.

*)Llave != contraseña

Ya que una es producto de la otra.

PROTECO

Cifrado.

Historia de la criptografía

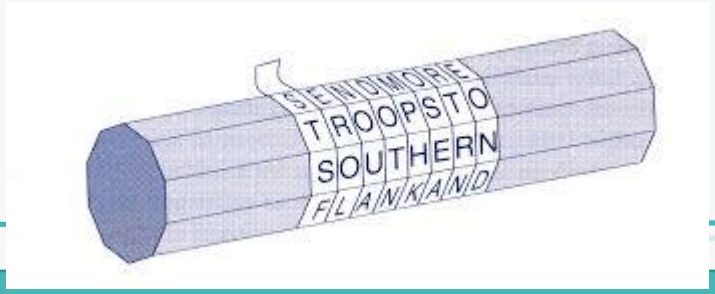
- Desde el principio hace miles de años, los seres humanos se han visto en la necesidad de ocultar toda aquella información que sea considerada privada, a fin de resguardar y mantenerla a salvo de intrusos que pudieran hacer un mal uso de ella si lo conocieran.
- Y con deseo de esconder la información valiosa para su poseedor es como nace la criptología. Del griego Kryptós, criptos "ocultar" y graphé, grafos "escribir"

PROTECO

Cifrado.

Momentos importantes de la criptografía:

- Durante la guerra entre Atenas y Esparta, se encuentra el primer registro formal del uso de escritura secreta, en el 400 a.C. los espartanos utilizaron la Scítala o Escítalo, que puede considerarse el primer sistema de criptografía por transposición.
- El mensaje solo podía leerse cuando éste se enrollaba sobre un bastón del mismo largo y grosor, que poseía un destinatario lícito.



PROTECO

Cifrado.

Momentos importantes de la criptografía:

- En el siglo I a.C surge el cifrado César, el cuál se considera que fue utilizado por Julio César (101 a.C – 43 a.C). El cifrado consiste en mover el carácter a representar 3 posiciones adelante dentro del alfabeto a utilizar.

PROTECO

Cifrado.

Momentos importantes de la criptografía:

- Carlomagno (siglo I d.C.) fue un factor importante por la comunicación que mantenía con sus ejércitos y aliados donde sustituía las letras por símbolos extraños, de manera que sus textos secretos los escribía de forma cifrada.

PROTECO

Cifrado.

Momentos importantes de la criptografía:

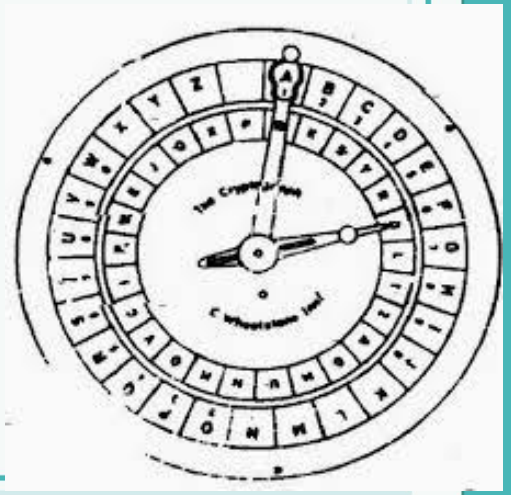
- En el siglo XV se escribe la que se considera por muchos cómo la primera y más antigua obra que existe sobre criptografía, "Liber Zifrorum", escrita por Cicco Simoneta (1410-1480) en la que se estudian diversos sistemas basados en la sustitución de letras y diversas representaciones en las que incluyen símbolos convencionales.
- Hacia 1466, Alberti escribe otra obra "De Compendis Cifris" y concibe el sistema poli alfabético, esto es, un cifrador que emplea varios alfabetos, saltando de uno a otro cada tres o cuatro palabras.

PROTECO

Cifrado.

Momentos importantes de la criptografía:

- En el siglo XVIII, el uso de la criptografía se extendió en todos los ambientes donde la información se encontraba vinculada con todo aquello que representa el poder, esto es, se relaciona directamente con secretos de estado, asuntos militares, de espionaje y diplomáticos.
- A principios del XIX nace el primer dispositivo mecánico conocido como la rueda de Jefferson, la cual tiene sus ideas fundamentales en lo estudiado por Alberti y Polybios y que más tarde se le conocería como disco Wheatstone.



PROTECO

Cifrado.

Momentos importantes de la criptografía:

- En el siglo XVIII, el uso de la criptografía se extendió en todos los ambientes donde la información se encontraba vinculada con todo aquello que representa el poder, esto es, se relaciona directamente con secretos de estado, asuntos militares, de espionaje y diplomáticos.
- Para 1919 se registra la primer patente de una máquina criptográfica, la cual corresponde a una máquina llamada Enigma, obra del holandés Alexander Koch y el alemán Arthur Scherbius

PROTECO

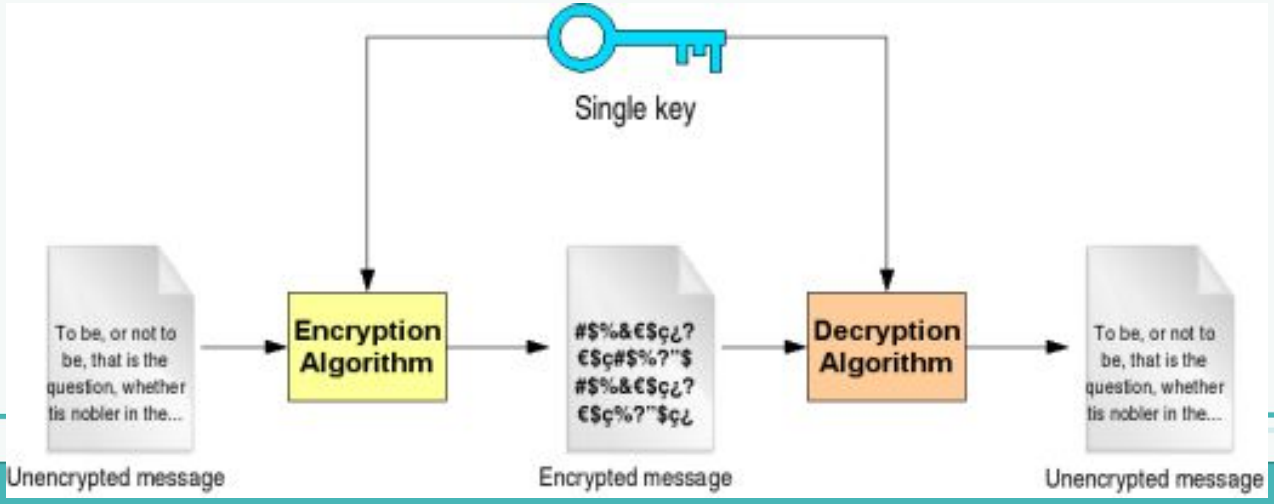
Cifrado.

Componentes de un cifrado.

Algoritmo: Suele ser publico y ha sido probado.

Llave: Cadena secreta.

*Se require de ambos para poder cifrar y descifrar.



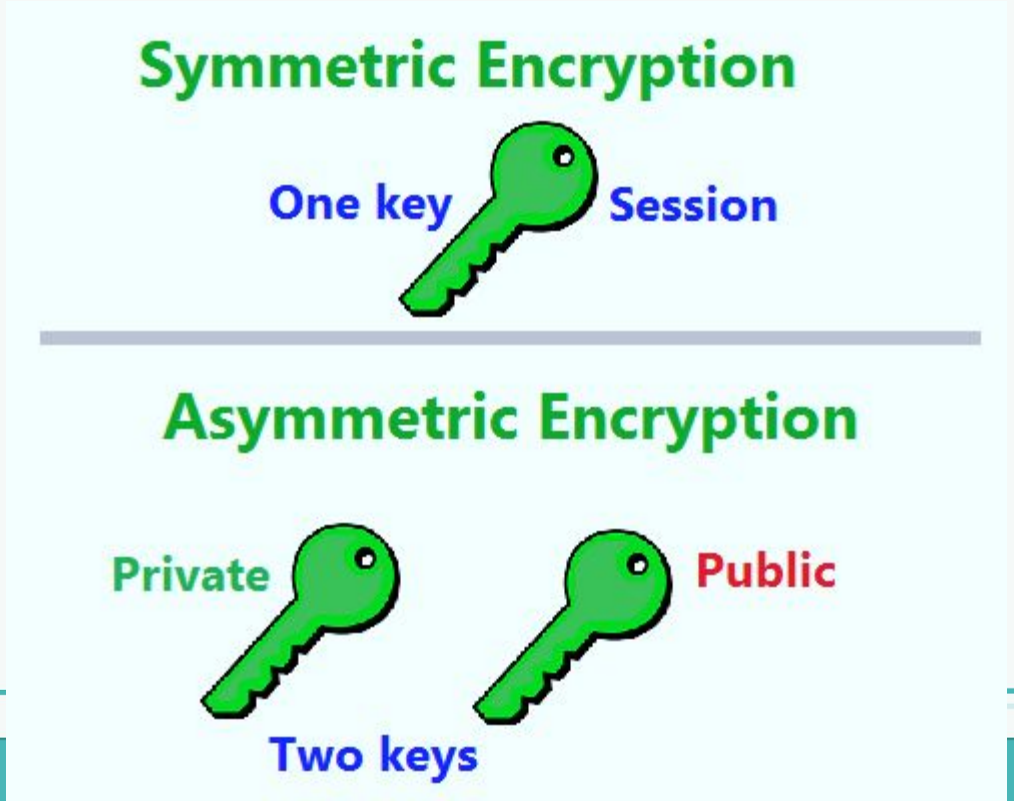
PROTECO

Cifrado.

Tipos de cifrado:

*)Simetrico Ej: AES, enigma, blowfish, etc.

*)Asimetrico Ej: RSA,ECC,DSA,etc.



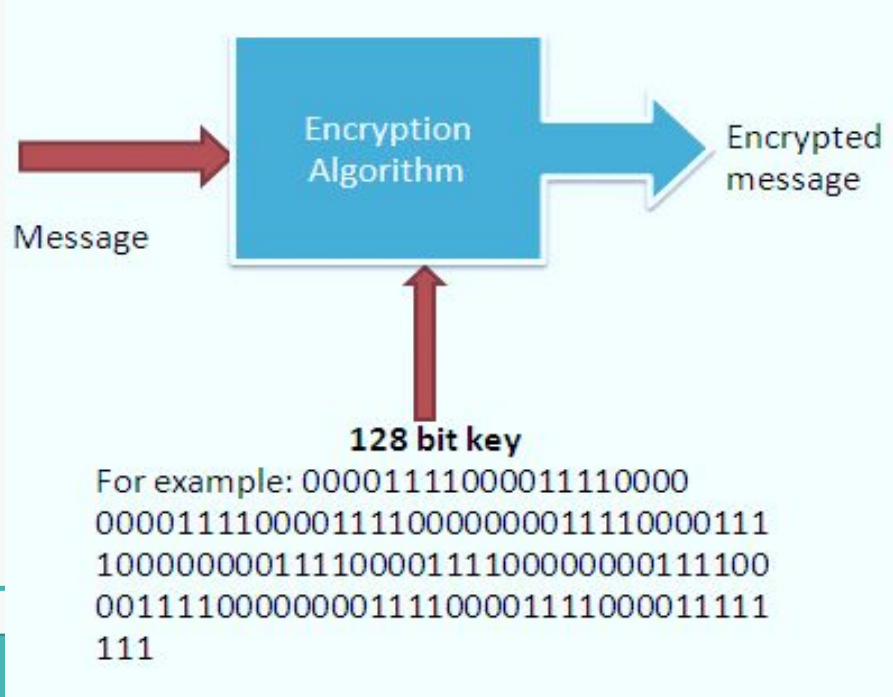
PROTECO

Cifrado.

Cifrado simetrico:

Bit length (Longitud de la llave creada con la contraseña) :

Podríamos verlo como (generalmente)la fuerza del propio algoritmo)´, aunque esto haría más lento el proceso.



PROTECO

Cifrado.

Cifrado simetrico:

Desventajas:

*) Si queremos enviar archivos cifrados, tendremos que enviar la contraseña.

*) No es escalable.

Ventajas:

*) Son relativamente rápidos.

*)Solo necesitas aprender la contraseña y el cifrado.

PROTECO

Cifrado.

Ciframos con la llave publica, lo que deseamos solo el posedor de la llave privada pueda abrir.(Confidencialidad)

PROTECO

Cifrado.

Ventajas:

*)En ningún momento se tuvo que intercambiar claves de forma insegura.

*) Podemos autenticarnos (no repudiation) o enviar información de forma confidencial.

*)Escalabilidad.

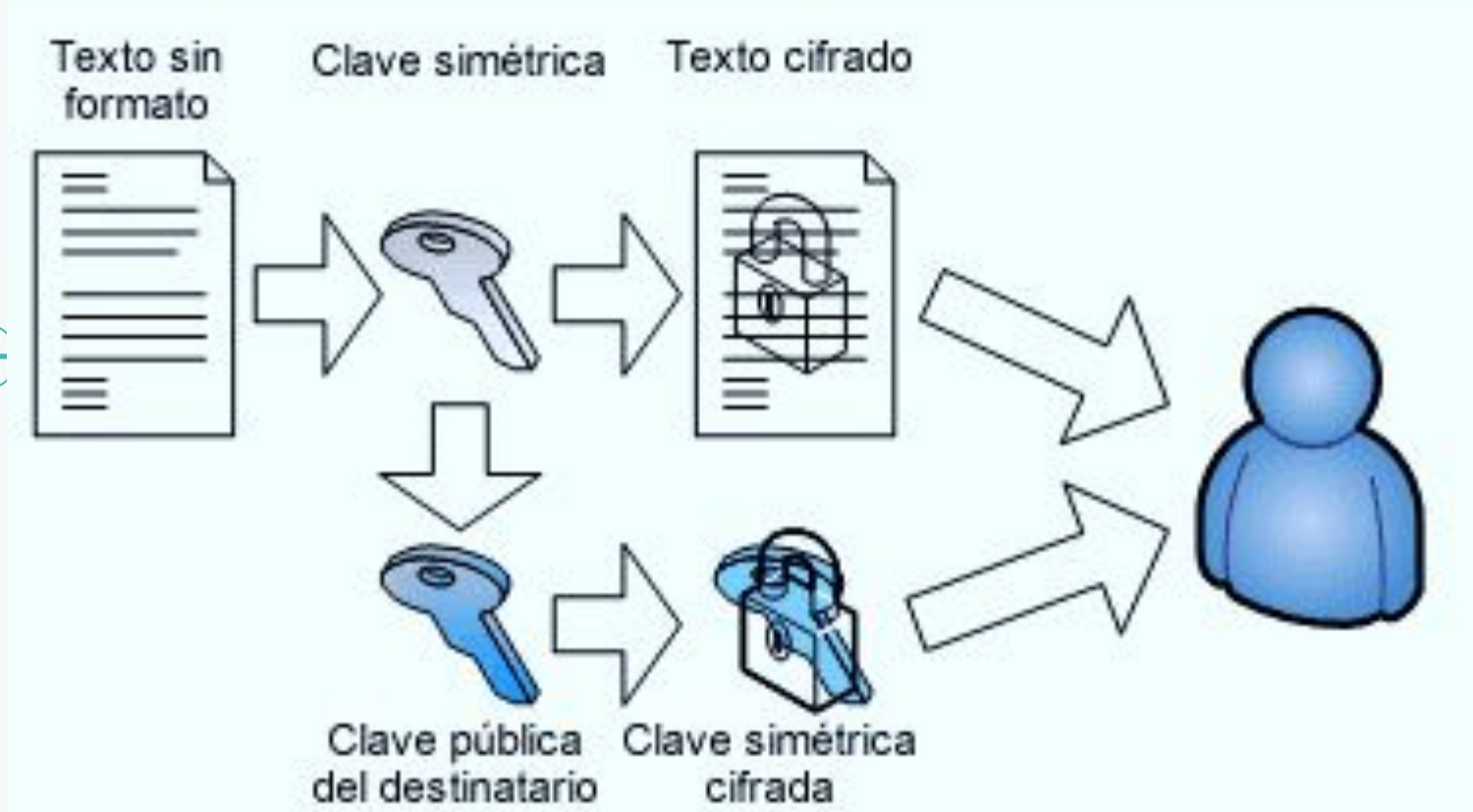
Desventajas:

*)Se trata de un proceso más lento e intensivo matemáticamente.

PROTECO

Cifrado.

Cifrado híbrido:



PROTECO

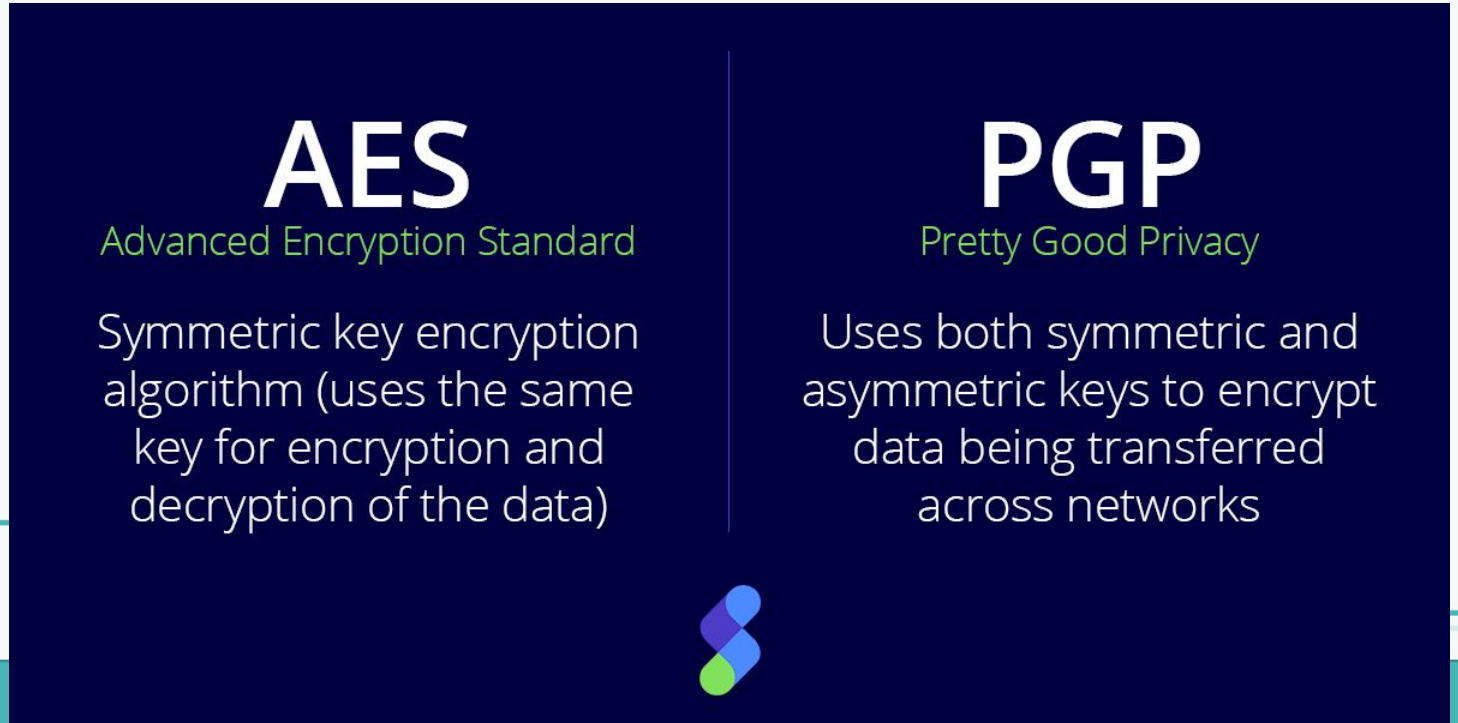
Cifrado.

Ventajas:

*)Tiene lo mejor de ambos mundos.

*)Pueden utilizarse llaves de sesión, las cuales son “desechables”.

Ej: PGP



PROTECO

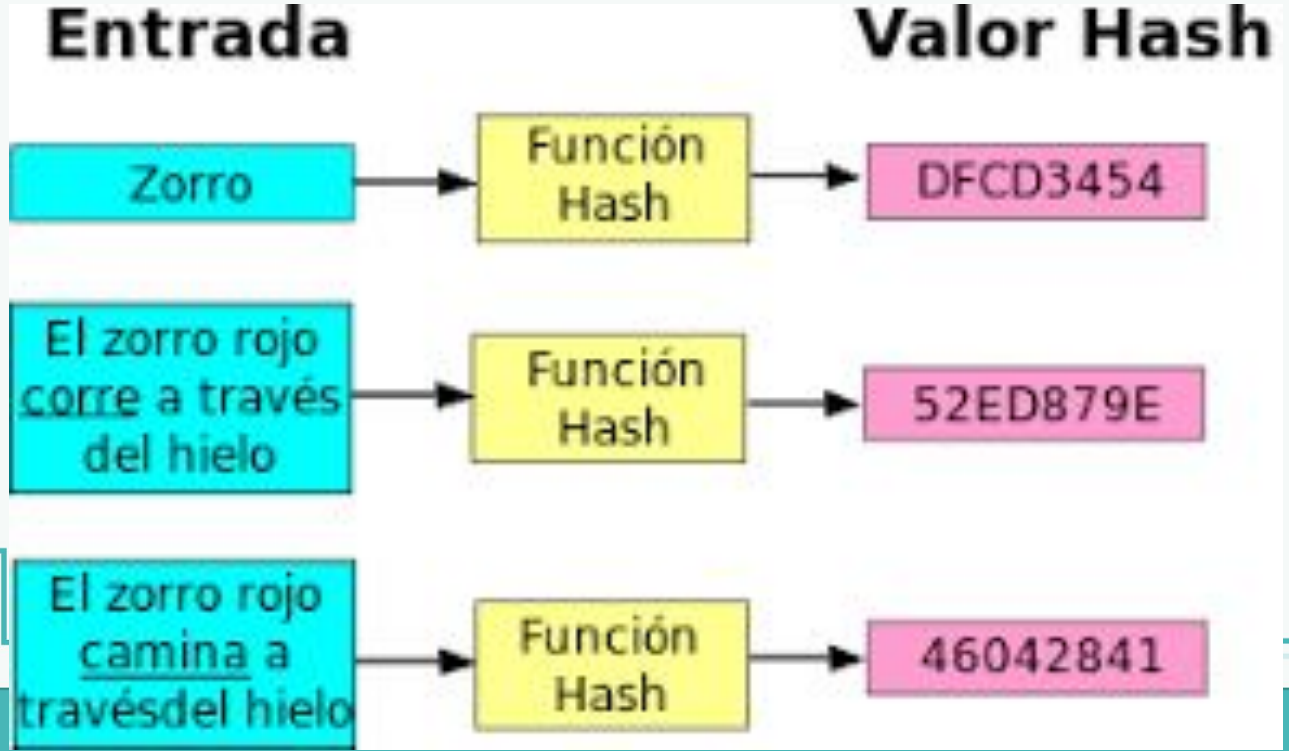
Cifrado.

Funciones Hash y Certificados Digitales:

*)Son funciones de una dirección

*)Salida de un tamaño fijo.

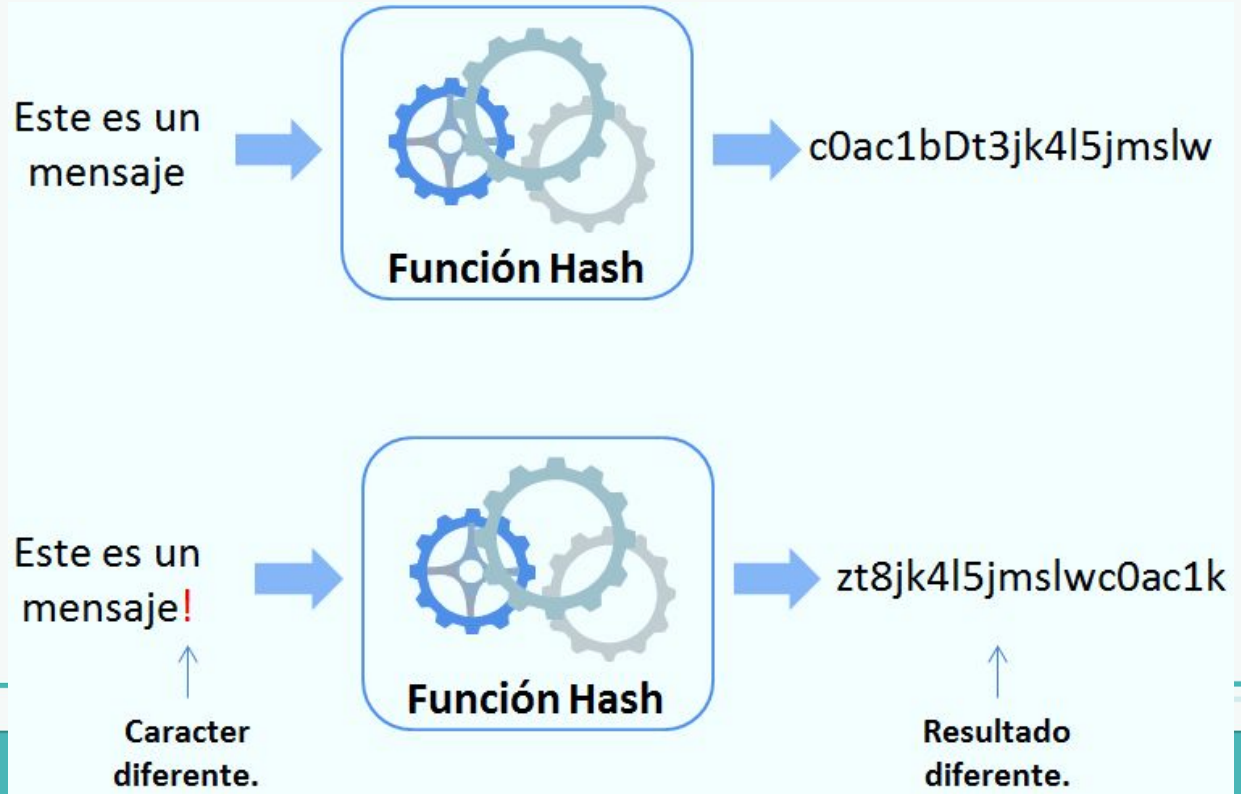
*) Detecta modificaciones.



PROTECO

Cifrado.

*)La función no permite (teoricamente) volver a la entrada original.



PROTECO

Rainbow tables:

Son tablas precomputadas que permiten obtener la entrada de la hash.

Password	Hash
123456	e10adc3949ba59abbe56e057f20f883e
password	5f4dcc3b5aa765d61d8327deb882cf99
12345	827ccb0eea8a706c4c34a16891f84e7b
12345678	25d55ad283aa400af464c76d713c07ad
football	37b4e2d82900d5e94b8da524fbeb33c0
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
1234567890	e807f1fcf82d132f9bb018ca6738a19f
1234567	fcea920f7412b5da7be0cf42b8c93759
princess	8afa847f50a716e64932d995c8e7435a
1234	81dc9bdb52d04dc20036dbd8313ed055
login	d56b699830e77ba53855679cb1d252da
welcome	40be4e59b9a2a2b5dffb918c0e86b3d7
solo	5653c6b1f51852a6351ec69c8452abc6
abc123	e99a18c428cb38d5f260853678922e03
admin	21232f297a57a5a743894a0e4a801fc3

PROTECO

Cifrado.

¿Como protegernos de esto? Salt bits

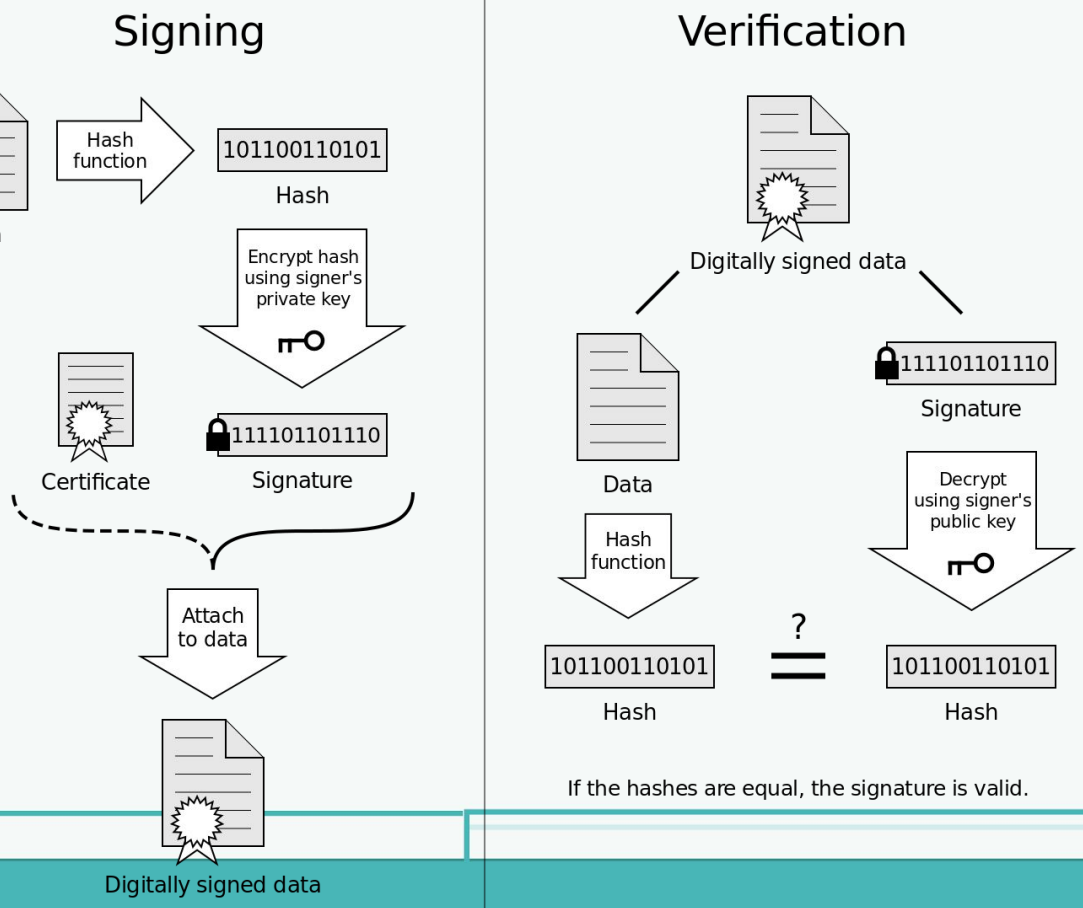
Datos que pueden ser aleatorios, y son tomados como una entrada de la función hash.

				
Password	`p4s5w3rdz`	`p4s5w3rdz`	`p4s5w3rdz`	`p4s5w3rdz`
Salt	`-`	`-`	`et52ed`	`ye5sf8`
Hash	`f4c31aa`	`f4c31aa`	`lvn49sa`	`z32i6t0`

Cifrado.

Certificados y firmas digitales:

Valor hash(integridad) cifrado con la llave privada del emisor (Autenticación).



PROTECO

Cifrado.

Ventajas:

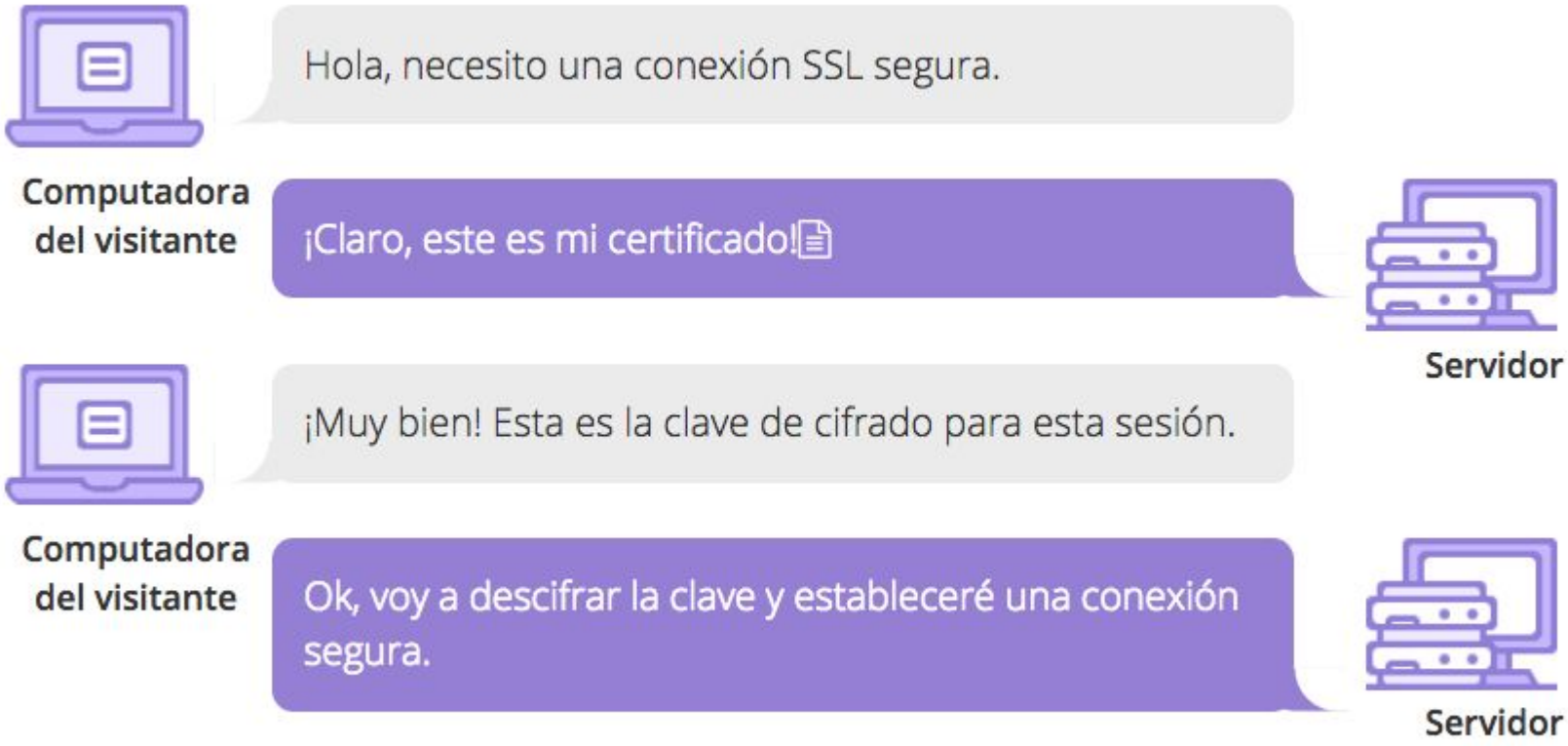
Autenticación, nonrepudiation e integridad.

Ej:

Podemos enviar archivos y demostrar que no han sido cambiados y que efectivamente los mandamos.

PROTECO

SSL y TLS


Hola, necesito una conexión SSL segura.
Computadora del visitante
¡Claro, este es mi certificado!
Servidor
¡Muy bien! Esta es la clave de cifrado para esta sesión.
Computadora del visitante
Ok, voy a descifrar la clave y estableceré una conexión segura.
Servidor

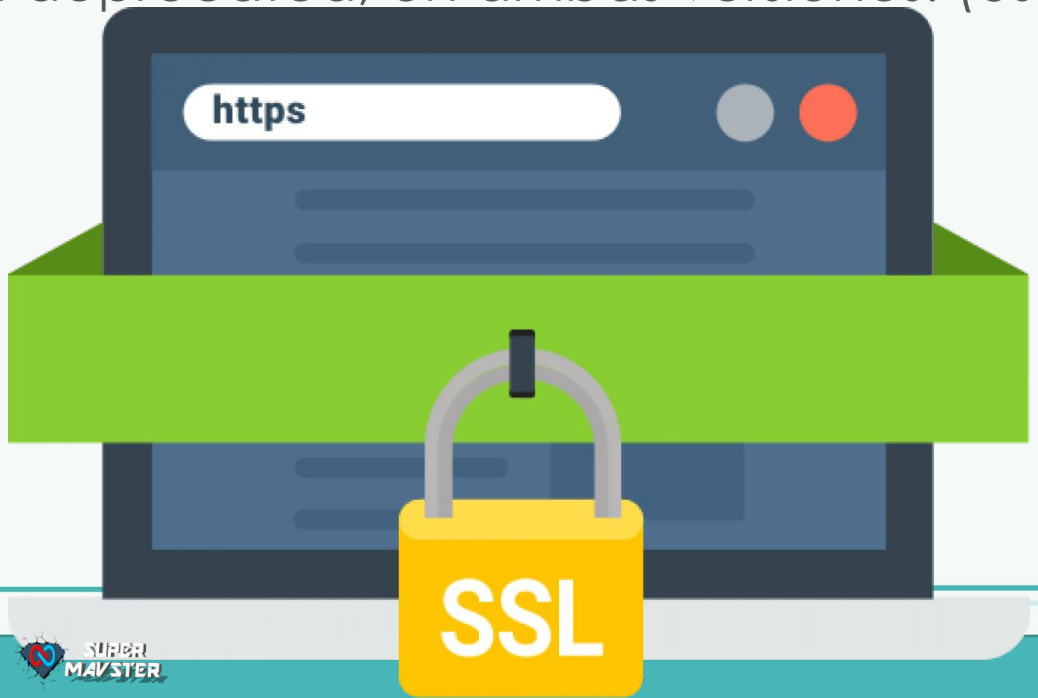
SSL.

Secure Socket Layer Protocol (V2 y V3 -1999-):

Nos da:

- Privacidad
- Autenticación
- Verificación de la integridad

Esta deprecated, en ambas versiones. (Usar TLS)



PROTECO

Transport Layer Security (V1 -1999-,V2,V3):

Ofrece:

Mayor seguridad criptográfica,

Negociar una conexión cifrada entre cliente y servidor.

+ Los beneficios de SSL

PROTECO

HTTPS

HTTP over TLS or HTTP over SSL:

-Puerto 443

- Da los beneficios del cifrado SSL o TLS

-Actualmente esta usando las versiones:

HTTP V2 o V3 e idealmente TLS 1.3 y 1.2

https://en.wikipedia.org/wiki/Transport_Layer_Security

https://badssl.com/

Cifrado.

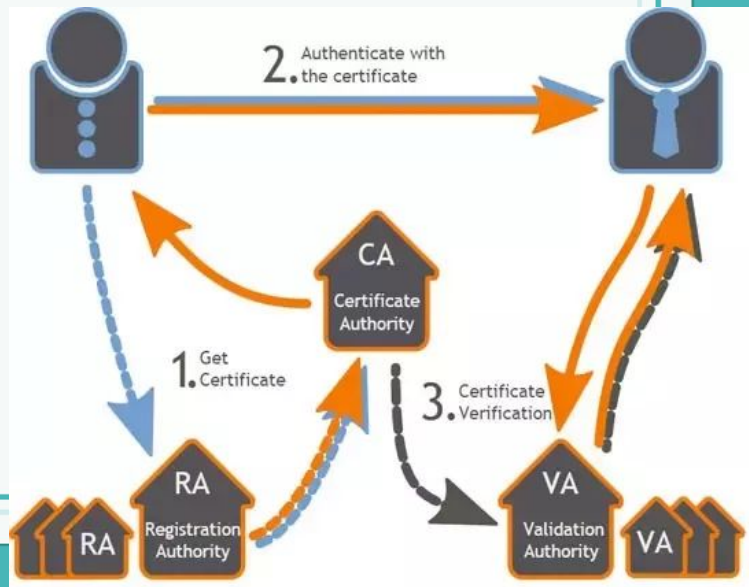
Entidades certificadoras.

-Pueden publicar certificados digitales.

-Certifica que una llave pública pertenece a alguien.

-Es confiada por el cliente como por el servidor.

-Firma las llaves públicas de los servidores



HSTS

HTTP Strict Transport Security:

-Obliga conexiones https.

-Evita ataques de:

-Man in the Middle

-SSL stripping

- Se carga la primera vez que entramos a un sitio.

- Aunque puede venir precargado:

https://hstspreload.org/

HTTP Strict Transport Security

PROTECO

HPKP

Http Public Key Pinning:

Hace que un cliente solo se pueda conectar a un sitio sí este tiene ciertas llaves publicas. Y solo esas funcionaran a futuro.

Debido a varios problemas con este protocolo, fue desechado en 2019

PROTECO

CURSOS INTERSEMESTRALES

PROTECO

Criptografía y Esteganografía

¿Qué es la Esteganografía?

Origen etimológico:

steganos → *Oculto / Encubierto*

graphein → *Escritura*

"El estudio y aplicación de las técnicas que permiten ocultar mensajes dentro de otro objeto."

PROTECO

¿Qué es la Esteganografía?

- Estudia diferentes procedimientos para ocultar información almacenándola en algún soporte o transmitiéndola por algún canal

- El arte de ocultar información en algún medio

PROTECO

¿Qué es la Esteganografía?

- La criptografía codifica un mensaje para que no se pueda entender.

- La esteganografía oculta el mensaje para que no se pueda ver.

PROTECO

Otros conceptos

- Estegoanálisis: Estudio de la seguridad en la aplicación de la esteganografía, empleando diferentes métodos para detectar la posible presencia de información oculta en un medio o bien para eliminarla.
- Estegomedio: Es el medio o conducto que es utilizado para ocultar la información.
- Estego-*objeto*.

PROTECO

El problema del Prisionero

- G. J. Simmons en 1983
- La descripción de este problema parte de la necesidad de comunicación entre dos prisioneros, A y B.
- A y B deben comunicarse de manera desapercibida

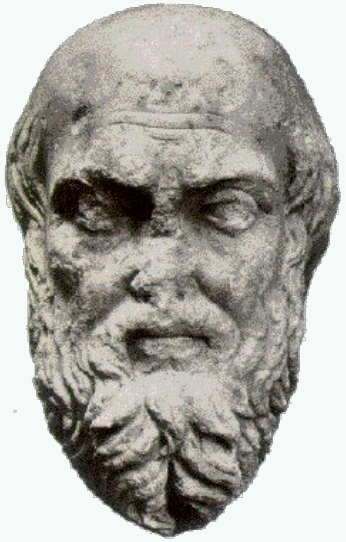
PROTECO

Antecedentes

PROTECO

Antecedentes

- Heródoto describió la manera que tenían los griegos para mandarse mensajes entre sí.
- Escribían sobre una tablilla de manera que luego tenia recubrían con cera.



PROTECO

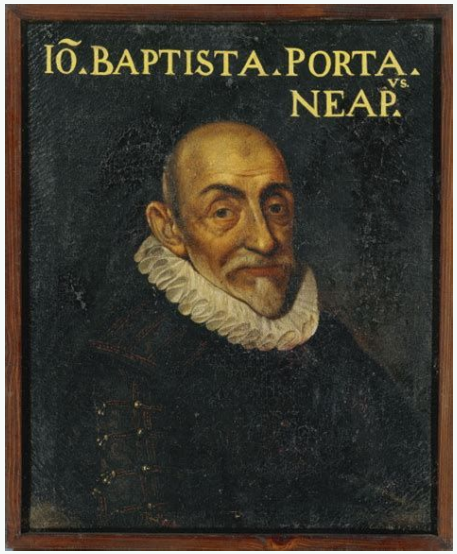
Antecedentes

- En la cultura milenaria china se escribían mensajes sobre seda fina.
- Luego era aplastada hasta formar una pelotita diminuta que se recubría de cera para facilitar que el mensajero ocultara la información tragándose la bola.

PROTECO

Antecedentes

- El italiano Giovanni Battista della Porta descubrió cómo esconder un mensaje en el interior de un huevo cocido.

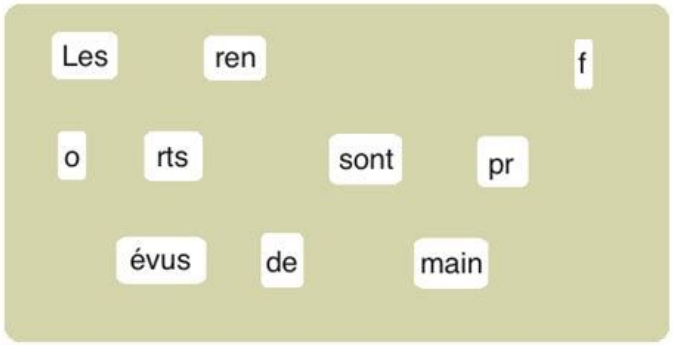


PROTECO

Antecedentes

Cardan Grille. (Girolamo Cardano S. XVI)

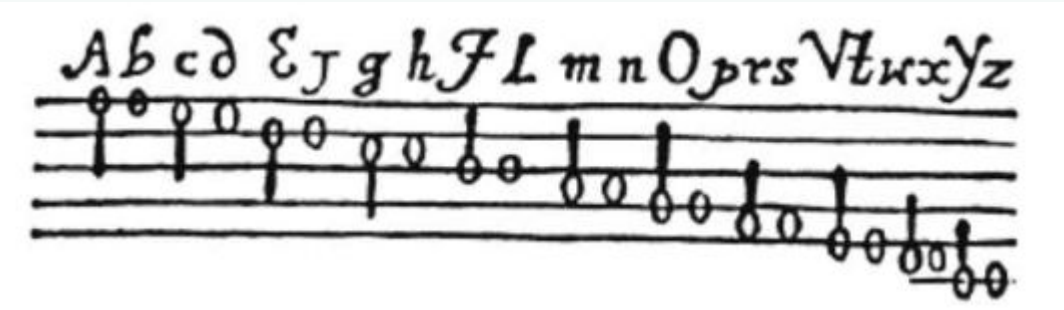
Les enfants rentrent lundi Ils seront neuf
Je vais leur coudre des manteaux bleus
ou verts Les pères sont surpris
que les retours des enfants sont
prévus vite depuis la maintenance
des trains



PROTECO

Antecedentes

- Jargon code .
- Newspapaer code .
- Gaspar Schott, en su libro *Shola Steganographica* mostro como ocultar mensajes en partituras de música.



Esteganografía Moderna

PROTECO

Esteganografía Moderna

Métodos de ocultación digital en:

- Imágenes
- Audio
- Video

www.jjtc.com/Steganography/tools.html

PROTECO

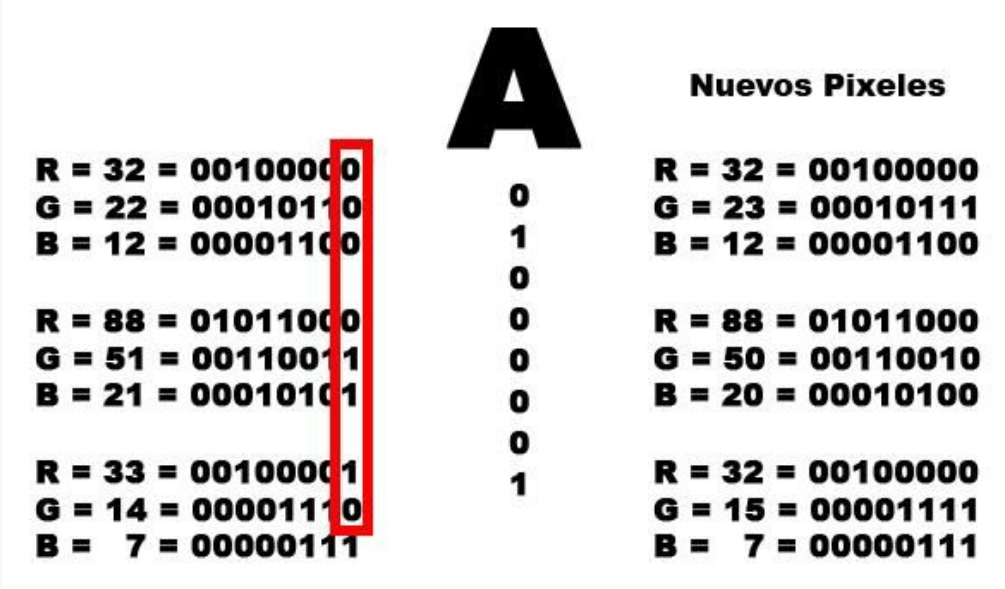
Esteganografía Moderna en imágenes

- Técnicas de sustitución LSB:
- Técnicas basadas en paleta de colores
- Técnicas basadas en coeficientes cuantificados.

PROTECO

Técnicas de sustitución LSB:

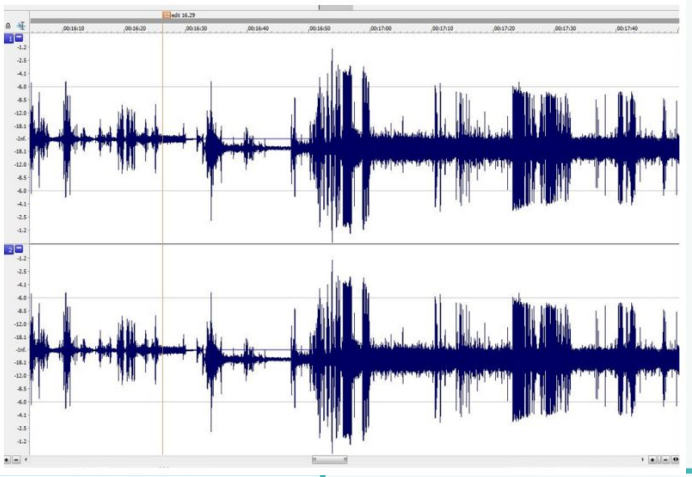
- Es un procedimiento de sustitución que permite modificar el bit menos significativo de la codificación de cada píxel de una imagen por el bit del mensaje a ocultar.



PROTECO

Esteganografía Moderna en audio.

- Técnica de ocultación en la fase de una señal.
- Técnica de ocultación en el eco de una señal.
- Ocultación aprovechando características estadísticas de las señales de audio.



PROTECO

https://www.coppercloudmusic.com/enscribe

http://www.baudline.com/

PROTECO

Esteganografía Moderna en video.

- Video: Conjunto de frames (imágenes)
- Puede ocultarse texto o imágenes en videos

MSU StegoVideo

PROTECO

Algunas Herramientas

- StegHide
- OpenStego
- MP3Stego
- OpenPuff
- StegoWav
- DeepSound

PROTECO

Diferencias con la Criptografía

- El objetivo básico de la criptografía ocultar su significado mediante un proceso de codificación o cifrado.

- Mientras que el de la esteganografía es ocultar la existencia de un mensaje.

PROTECO

¿Por que es importante?

PROTECO