ESTACIONES CHARLANTES DE CIFRADOS

Cifrados por Sustitución

Descripción: Un cifrado por sustitución toma un mensaje en texto plano y cambia cada letra por otra letra o símbolo.

3 Datos / Estadísticas / Características:

1. La "clave" del cifrado César representa cuántos espacios debe girar el alfabeto.
2. Los patrones de letras dobles, las palabras de una letra y la colocación de vocales hacen que este método sea vulnerable.
3. Susceptible a ataques de fuerza bruta y análisis de frecuencia.

https://www.csfieldguide.org.nz/en/chapters/coding-encryption/substitution-ciphers/

Substitution table:

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	**U**	**P**	**T**	**B**	**Z**	**O**	**K**	**F**	**V**			**A**	**G**	**M**	**J**			**Y**	**C**	**H**	**N**	**W**	**I**		**D**	

Ejemplos:

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

Cifrado César

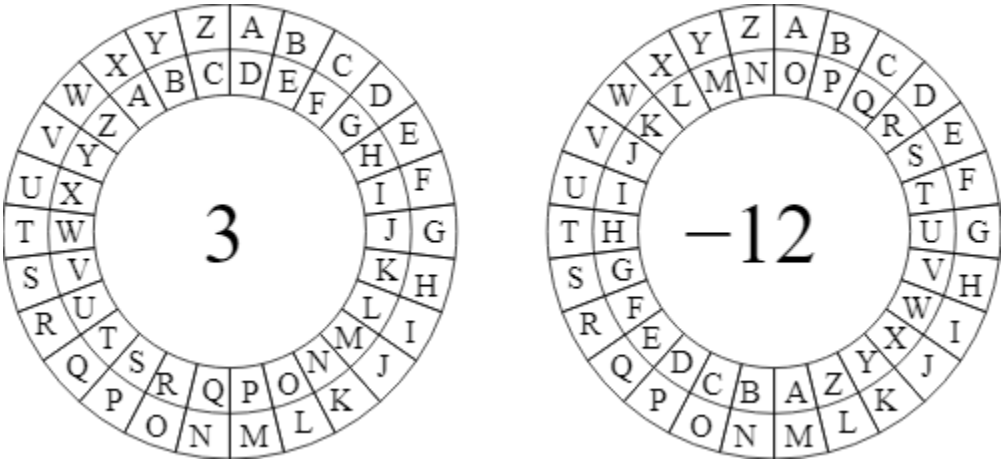

Imagen acreditada a https://cscx.org/caesar

Cifrado Atbash

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

Información sobre la seguridad:

https://en.wikipedia.org/wiki/Substitution_cipher#Security

Aplicaciones:

Pasando notas secretas a tus amigos en la escuela

No apto para:

Transacciones monetarias

Secretos comerciales

Información clasificada

Cualquier cosa relacionada con la salud/seguridad u otra información personal

Sustitución Lingüística

La sustitución lingüística es un método para proteger información sensible comunicándose en un idioma desconocido para los interceptores.

Datos / Estadísticas / Características:

1. Depende de que el lenguaje cifrado sea secreto

Ejemplo: "...miembros del servicio de Estados Unidos durante las Guerras Mundiales que usaron su conocimiento de las lenguas nativas americanas como base para transmitir mensajes codificados" (de https://en.wikipedia.org/wiki/Code_talker).

Aplicaciones:

Conversaciones informales

Invasiones alienígenas

Contrainteligencia

Limitaciones:

Tras el éxito de los locutores de claves en la Segunda Guerra Mundial, es mucho más difícil llevar esto a cabo en escenarios de alto perfil.

https://fronterasdesk.org/content/1005301/navajo-code-talkers-miracle-ended-world-war-ii

https://www.nationalww2museum.org/war/articles/american-indian-code-talkers

Cifrado Simétrico

El cifrado simétrico usa un secreto compartido entre dos usuarios como clave para cifrar los datos. Es “simétrico” porque cada persona en la comunicación usa la clave para codificar y descodificar los mensajes.

https://www.csfieldguide.org.nz/en/chapters/coding-encryption/storing-passwords-securely/

Ejemplos:

https://en.wikipedia.org/wiki/One-time_pad

Algunos ejemplos de algoritmos de clave simétrica conocidos son Twofish, Serpent, AES (Rijndael), Camellia, Salsa20, ChaCha20, Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer y IDEA.

(de https://en.wikipedia.org/wiki/Symmetric-key_algorithm#Implementations)

Aplicaciones:

Firmas digitales

Cifrado de datos

Comunicación

Limitaciones:

- Proteger un único secreto compartido es difícil debido a los hackers y a la forma en que prolifera la información en Internet.
- Romper el cifrado simétrico recibe mucha atención e interés por parte de los hackers. Hay muchas herramientas y técnicas disponibles para ayudar a "descubrir" el secreto compartido.
- Establecer un secreto compartido requiere una forma preexistente y segura de comunicarse.

Cifrado Asimétrico (también conocido como criptografía de clase pública)

El cifrado asimétrico usa una combinación de claves privadas y públicas de dos partes para cifrar datos. Es “asimétrico” porque cada persona que participa en la comunicación usa una clave distinta para codificar y descodificar los mensajes.

https://www.csfieldguide.org.nz/en/chapters/coding-encryption/the-key-distribution-problem/

Datos / Estadísticas / Características:

1. Cualquiera puede usar la clave pública para cifrar.
2. Sólo el poseedor de la clave privada puede descifrar un mensaje codificado.

Ejemplos:

Intercambio de claves Diffie-Hellman

Algoritmo de cifrado RSA

Criptografía de curva elíptica

Aplicaciones:

- Seguridad en Internet. Casi toda la seguridad en Internet se implementa con criptografía de clave pública.
- Firmas digitales robustas
- Moneda digital

Limitaciones:

- Puede ser difícil de entender
- Mantener a salvo las claves privadas puede ser difícil