UNIVERSIDAD DEL VALLE DE GUATEMALA

historia de criptografia

Andre Marroquin Tarot - 22266

Cifrados de la Información

Cifrado de César dentro de la historia de la criptografía

El Cifrado de César es de los más antiguos de la criptografía. Se le atribuye a Julio César, esta persona lo utilizaba para enviar mensajes militares que no pudieran ser entendidos fácilmente si eran interceptados.

Es un cifrado por sustitución monoalfabética: cada letra del mensaje se reemplaza por otra letra del mismo alfabeto, desplazada una cantidad fija de posiciones.

¿Cómo funciona?

1. Se elige una clave: un número que indica cuántas posiciones se va a desplazar el alfabeto.
2. Cada letra del mensaje se reemplaza por la letra que está "clave" posiciones más adelante.
3. Si se llega al final del alfabeto, se regresa al inicio (comportamiento circular).

Ejemplo (key = 3)

Alfabeto:
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

Desplazado 3:
d e f g h i j k l m n o p q r s t u v w x y z a b c

Texto original: historia

Transformación letra por letra:

- h → k
- i → l
- s → v
- t → w
- o → r
- r → u
- i → l
- a → d

Texto cifrado: klvwruld

Para descifrar, se hace el desplazamiento inverso 3 letras hacia atrás.

Ejemplo de aplicación

Se le manda un mensaje a un amigo por WhatsApp, pero no se quiere que en caso de si alguien agarra tu teléfono, lo entienda rápido. El mensaje es: **te veo mañana**

Entonces se decide usar el cifrado de César con clave 3. Entonces se deja todo junto y sin tildes: **teveomanyana**

Luego, cada letra se recorren 3 posiciones en el alfabeto. Al final, el mensaje queda asi **whyhropdqdbd**

Entonces Si alguien más lo ve, no entiende nada. Pero el amigo, que sí conoce la clave (3), puede hacer el proceso al revés y recuperar: **teveomanyana A te veo mañana**

¿Por qué se eligió el Cifrado de César?

Lo elegi porque:

- Es históricamente relevante, es uno de los primeros intentos sistemáticos de proteger información.
- Es muy fácil de entender ya que es únicamente desplazamiento 3 a la derecha del abecedario y es muy bueno para ilustrar los conceptos básicos de cifrado, clave, cifrado y descifrado.
- Sirve como conector entre la historia de la criptografía con los sistemas modernos más complejos.

Ventajas

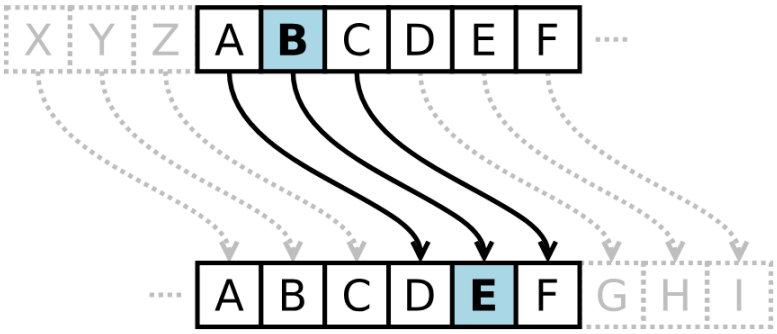
- Es muy simple porque se puede implementar a mano, en papel o en cualquier lenguaje de programación.
- Muy fácil de entender porque es bueno para enseñar los términos de criptografía.
- Es muy rápido ya que el proceso de cifrado y descifrado es muy rápido de procesar ya que solo hay que seguir pasos.

Vulnerabilidades

- Espacio de claves muy pequeño porque solo hay 25 posibles desplazamientos sin contar el 0 en el abecedario tradicional inglés. Es demasiado fácil de romper por fuerza bruta

probando todas las claves.

- Se puede analizar su frecuencia siguiendo el patrón estadístico del idioma, un atacante puede analizar la frecuencia de letras y deducir el desplazamiento.
- Hoy en día por ser tan antiguo y fácil de resolver cualquier persona con conocimientos básicos puede romperlo de manera rápida.



Referencias:

- EduEscapeRoom.com. (2018, 8 julio). *Cifrado César - EduEscapeRoom*. EduEscapeRoom. https://eduescaperoom.com/cifrado-cesar/
- *Client challenge*. (s. f.). https://es.khanacademy.org/computing/computer-science/cryptography/ciphers/a/shift-cipher