Índice

1. Retos Criptográficos I

1.1 Introducción a la criptografía

La criptografía, derivada de las palabras griegas 'kryptos' y 'graphein', que significan 'oculto' y 'escribir' respectivamente, es la ciencia de ocultar la información. Es una disciplina fundamental en el campo de la seguridad de la información que se utiliza para proteger la información de accesos no autorizados o para garantizar su integridad.

La criptografía se basa en el concepto de convertir un texto en claro, que es fácilmente comprensible, en un texto cifrado que es incomprensible para cualquier persona que no tenga la clave necesaria para descifrarlo. Este proceso de convertir el texto en claro en texto cifrado se conoce como **cifrado**, y el proceso inverso se conoce como **descifrado**.

1.1.1 Cifrado y Codificación

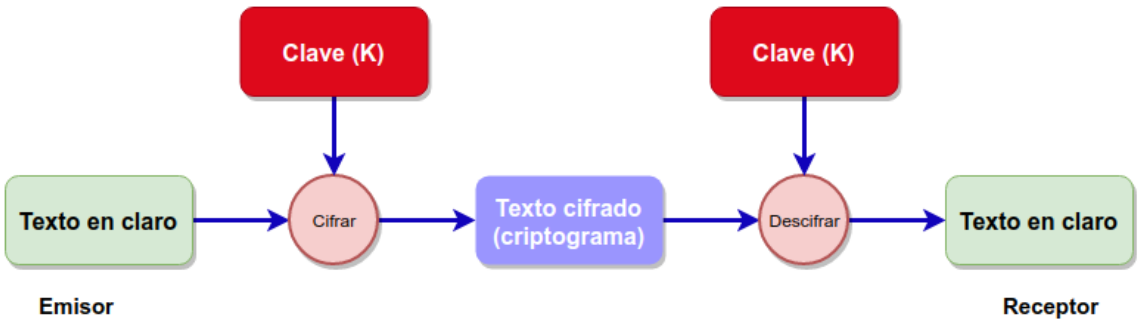
No hay que confundir cifrado y codificación.

- En el **cifrado** se transforma el mensaje original en otro mensaje distinto mediante un algoritmo de cifrado que **necesita una clave**. Su objetivo es mantener el mensaje en secreto.
- En la **codificación** se transforma el mensaje original en otro con un formato diferente utilizando un algoritmo conocido y **sin la necesidad de una clave**. Su objetivo es transformar el mensaje original en otro formato más manejable para otros fines. Ejemplos de códigos son ASCII, Base64, UTF-8, Código Morse, etc.

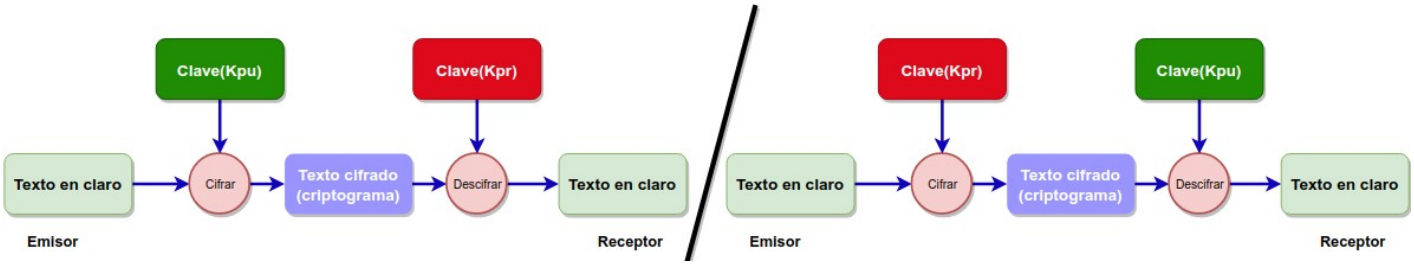
1.1.2 Criptografía simétrica y asimetrica

Existen dos categorías principales de criptografía: la criptografía simétrica y la criptografía asimétrica.

- En la criptografía **simétrica**, también conocida como criptografía de clave secreta, la misma clave se utiliza para cifrar y descifrar el mensaje. Ejemplos de algoritmos de cifrado simétrico son **DES** (*Data Encryption Standard*) y **AES** (*Advanced Encryption Standard*).



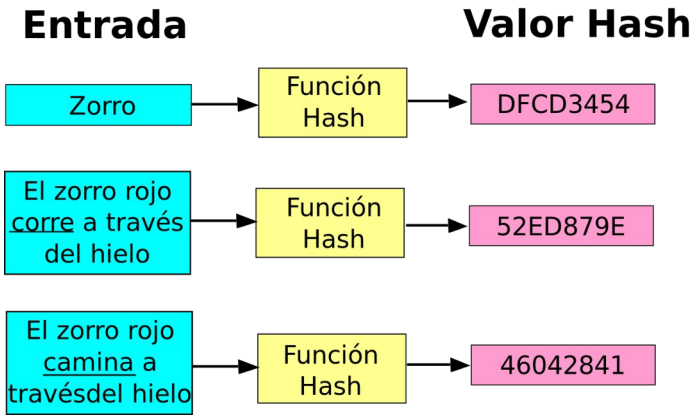
- Por otro lado, en la criptografía **asimétrica**, también conocida como criptografía de clave pública, se utilizan dos claves diferentes pero matemáticamente relacionadas. Una clave se utiliza para el cifrado y la otra para el descifrado. Ejemplos de algoritmos de cifrado asimétrico son **RSA** (son siglas de sus creadores: *Rivest, Shamir y Adleman*), y **DSA (***Digital Signature Algorithm***)**



1.1.3 Funciones Hash

Una función **hash** es un algoritmo matemático que permite calcular un valor resumen de unos datos de entrada, de tal forma que una mínima modificación de dichos datos de entrada producirá un valor resumen completamente diferente.

Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales.



Funete: *https://es.wikipedia.org/wiki/Funci%C3%B3n_hash#/media/Archivo:Hash_function2-es.svg*

1.2 Herramientas útiles

- **CyberChef** (*https://gchq.github.io/CyberChef/*)- Potente herramienta en línea desarrollada por el GCHQ (Cuartel General de Comunicaciones del Reino Unido) que ofrece una amplia gama de capacidades de manipulación de datos para descifrar y codificar mensajes. Su interfaz intuitiva y fácil de usar permite a los usuarios explorar y aplicar una variedad de operaciones criptográficas y de codificación de manera rápida y eficiente.
- **Multisolver** (*https://geocaching.dennistreysa.de/multisolver/index.html*)- Plataforma en línea que proporciona una variedad de herramientas para el cifrado, descifrado y análisis de mensajes y desafíos criptográficos. Esta plataforma está diseñada específica-

mente para resolver rompecabezas de geocaching y desafíos similares que requieren habilidades en criptografía y resolución de acertijos.

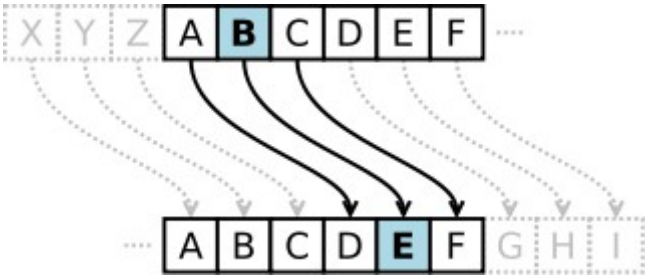
- **Dcode** (*https://www.dcode.fr/*)- plataforma en línea tipo cyberchef que proporciona una amplia variedad de herramientas criptográficas y de codificación para ayudar a cifrar y descifrar datos de forma segura. También ofrece herramientas para la resolución de acertijos y problemas matemáticos, así como para el análisis de criptogramas y códigos. (página web).
- **Hashcat** (*https://hashcat.net/hashcat/*) - Herramienta de cracking de contraseñas que admite una amplia variedad de algoritmos de hash.
- **John the Ripper** (*https://www.openwall.com/john/*) - Herramienta de cracking de contraseñas que admite varios tipos de cifrado y formatos de archivo (herramienta de línea de comandos).
- **AsecuritySite** (*https://asecuritysite.com/*) – Sitio web que trata sobre seguridad de la información y criptografía. Contiene muchísima información y diferentes herramientas para el análisis y la protección de la información.
- **Boxentriq** (*https://www.boxentriq.com*) - Plataforma en línea que ofrece diversas herramientas y desafíos para el aprendizaje y la práctica de habilidades en áreas como la criptografía, la esteganografía y la resolución de acertijos. Entre sus herramientas se incluyen generadores de claves criptográficas, cifradores y descifradores de mensajes, y herramientas de análisis de criptogramas. (página web).

1.3 Ejemplos de cifrados

1.3.1 Cifrados Rotacionales (ROT)

Los cifrados por desplazamiento, también conocidos como cifrados de rotación, son una forma simple de cifrado de sustitución de caracteres. En este tipo de cifrado, cada letra del texto a cifrar (texto plano) se sustituye por otra letra del alfabeto que está una cierta cantidad de posiciones por delante o por detrás en el alfabeto.

Por ejemplo, en un cifrado de desplazamiento de 3, cada letra del texto plano se reemplaza por la letra que está 3 posiciones por delante en el alfabeto. Así, la 'A' se convierte en 'D', la 'B' en 'E', y así sucesivamente.



Fuente: https://es.wikipedia.org/wiki/Archivo:Caesar3.svg

El cifrado Cesar

Un ejemplo de cfrado por desplazamiento es el conocido como “Cifrado Cesar”. El "Cifrado César" toma su nombre del líder militar y político romano Julio César, quien, según el relato del historiador romano Suetonio en su libro “La vida de los doce Césares”, lo utilizó en su correspondencia privada. Según Suetonio, César simplemente desplazaba cada letra hacia adelante en el alfabeto un cierto número de veces.

El cifrado Vigenère

El cifrado Vigenère es un método de cifrado clásico por sustitución, considerado como una extensión del cifrado Cesar, que se basa en el uso de tablas de cifrado, conocidas como tablas de Vigenère, para cifrar y descifrar mensajes.

Herramientas específica: https://es.planetcalc.com/2468/

1.3.2 Plataformas de retos criptográficos

- **MysteryTwister (MTC3)** (*https://mysterytwister.org*) Plataforma de retos criptográficos que forma parte del proyecto CrypTool y que ofrece una variedad de desafíos en cuatro niveles de dificultad. Estos desafíos pueden ser tan fáciles como descifrar un cifrado César (nivel I) y tan difíciles como romper un algoritmo de cifrado moderno como AES (nivel III). Los desafíos de nivel X son algo "misteriosos".
- **CipherCtf** (http://cipherctf.com) Plataforma de retos que forma parte de **Asecuritysite**. Los participantes pueden seleccionar su propio ID o permitir que se les asigne uno al azar. A partir de aquí, deben resolver diversos desafíos que implican el descifrado de diferentes tipos de algoritmos como el cifrado Caesar, Base64, Beaufort, Atbash, Vigenère, descubrir claves Diffie-Hellman, resolver cifrados de sustitución homofónica y mucho más. También existe una versión imprimible de los desafíos de cifrado para los profesores que deseen utilizar esta actividad en un aula.