INTRODUCCIÓN AL CIFRADO

Javier N. González

¿Qué es el cifrado?

El **cifrado** es una técnica que transforma un mensaje en algo que no se puede entender… a menos que se tenga la clave para descifrarlo.

Sirve para proteger información, como si fuera un candado invisible: puedes escribir un mensaje secreto que solo tu amigo, que conoce la clave, podrá entender.

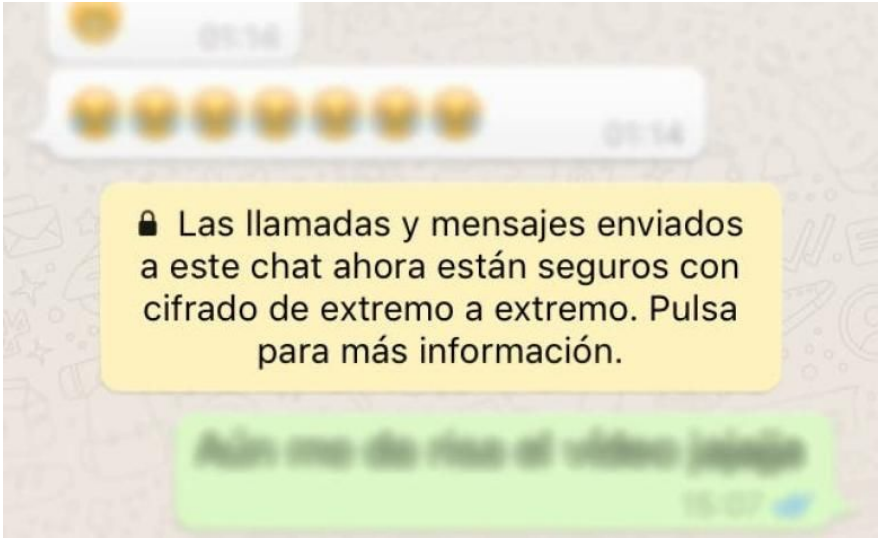
Cuando y donde se usa

Se usa en muchas situaciones:

En la **guerra**, para que el enemigo no intercepte tus planes.

En **Internet**, para que nadie lea tus mensajes o robe tus contraseñas. (Páginas **HTTPS** y tus contraseñas se guardan cifradas en **servidores**)

En tu móvil, para proteger tus **conversaciones** de WhatsApp.



🏛️ Un poco de historia

Julio César

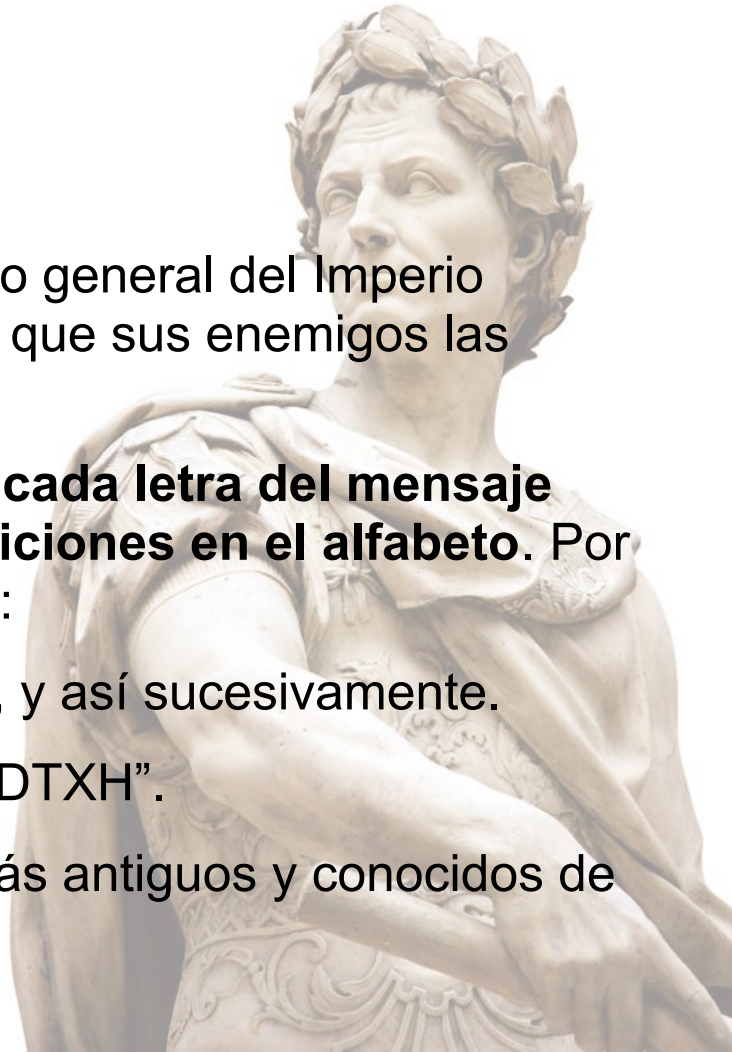
Hace más de 2.000 años, **Julio César**, el famoso general del Imperio Romano, quería enviar órdenes a sus tropas sin que sus enemigos las entendieran.

Para ello, inventó un sistema simple: **cambiaba cada letra del mensaje por otra desplazada un cierto número de posiciones en el alfabeto**. Por ejemplo, si usaba un desplazamiento de 3 letras:

- A se convertía en D, la B en E, la C en F, …, y así sucesivamente.

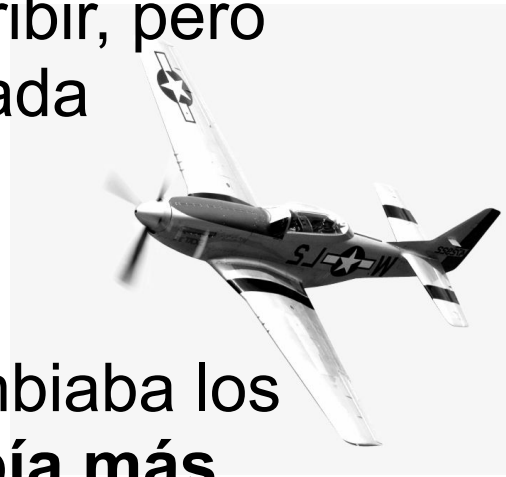
Entonces, “ATAQUE” podría convertirse en “DWDTXH”.

Este es el llamado **Cifrado César**, uno de los más antiguos y conocidos de la historia.



La Segunda Guerra Mundial

Durante la “**WWII**”, los alemanes usaban una máquina llamada **Enigma** para cifrar sus mensajes. Esta máquina parecía una máquina de escribir, pero transformaba cada letra en otra diferente cada vez que se pulsaba una tecla.



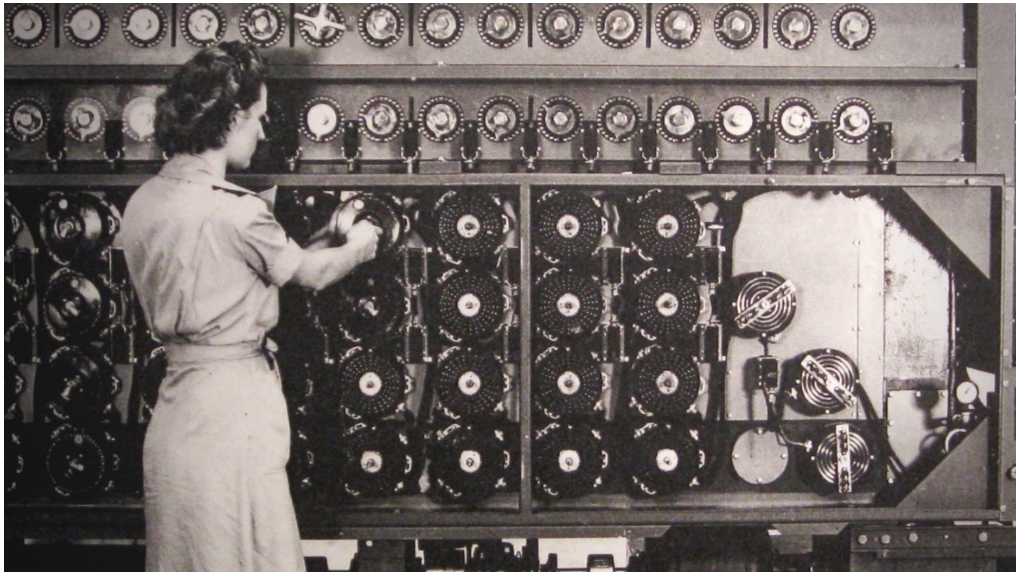
Era casi imposible de descifrar, porque cambiaba los códigos constantemente. Se decía que **había más combinaciones posibles que átomos en el universo**.

La Segunda Guerra Mundial

Pero un grupo secreto de matemáticos y expertos británicos, liderados por **Alan Turing**, logró romper el código de Enigma en 1940. Este logro:

- Permitió a los Aliados anticipar ataques enemigos, salvó millones de vidas y acortó la guerra en al menos 2 años.

Este momento marcó el **nacimiento de la criptografía moderna** y también de la computación.



Tipos de cifrado clásicos

- **Cifrado César**: como el de Julio César, simple desplazamiento de letras.
  Ejemplo: "HOLA" → con desplazamiento +3 → "KROD"

- **Sustitución simple**: cada letra se cambia por otra, o por un símbolo.
  Ejemplo: A = *, E* = # → *"ATAQUE"* → *"TQ#*"

- **Transposición**: se reordena el mensaje, como mezclar las piezas de un puzzle.
  Ejemplo: "MESA" → cambia a orden 3-1-4-2 → "AMES"

- **Cifrado Vigenère**: usa una palabra clave para cifrar cada letra de forma diferente, como si tuvieras muchos cifrados César en uno.

💻 Cifrado moderno

AES (cifrado simétrico): la misma clave cifra y descifra. Rápido y seguro.
Ejemplo: Cifras "mensaje" con clave secreta → Resulta en una cadena ilegible. Solo la misma clave puede recuperarlo.

RSA (cifrado asimétrico): se usan dos claves diferentes: una pública y otra privada.
Ejemplo: Tú cifras con la clave pública de María → Solo María puede descifrarlo con su clave privada.

Hashes: convierten cualquier información en un código único. No se puede descifrar, solo comparar.
Ejemplo: El hash de "1234" → `81dc9bdb52d04dc20036dbd8313ed055`
Si cambias una sola letra, el hash cambia totalmente.

¿Por qué aprender cifrado?

Porque es divertido y te hace pensar como un espía.

Porque te ayuda a entender cómo se protegen los datos hoy en día.

Porque es útil si quieres trabajar en informática, ingeniería, videojuegos o ciberseguridad.

Y porque… **ahora tú vas a intentar romper un cifrado real**