educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

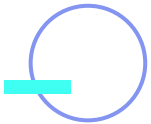
Módulo 1

Criptografía

Conceptos clave

- La **criptografía** es la ciencia que estudia cómo ocultar datos para que solamente aquellos entes autorizados puedan leerlos y/o modificarlos. Para ello, se utiliza un elemento denominado *clave*.
- El **criptoanálisis** es el intento de leer y/o modificar los datos ocultos sin disponer de la clave.
- La **criptología** es la ciencia que engloba tanto la criptografía como el criptoanálisis.
- La **esteganografía** estudia cómo enviar mensajes ocultos sin que terceras personas sospechen que se está enviando un mensaje
- El **estegoanálisis** intenta detectar si un mensaje aparentemente inocuo contiene otro oculto. No intenta descifrarlo.

- El **texto claro** o **plano** son los datos que se quieren ocultar.
- El **texto cifrado** o **criptograma** son los datos obtenidos luego de ser cifrado el texto claro.
- La **codificación** es la técnica que consiste en reemplazar unas palabras por otras. La clave es el diccionario de sustitución.
- El **cifrado** es la técnica de reemplazo de letras. La clave depende de la forma en que se realice.
- La **sustitución** es la técnica de cifrado que consiste en cambiar una letra por otra.
- La **transposición** o **permutación** es la técnica de cifrado que consiste en cambiar el orden de las letras (de a una o por grupos).



Criptosistema

Un **sistema criptográfico** es aquel que nos asegura que el proceso de cifrado es correcto.

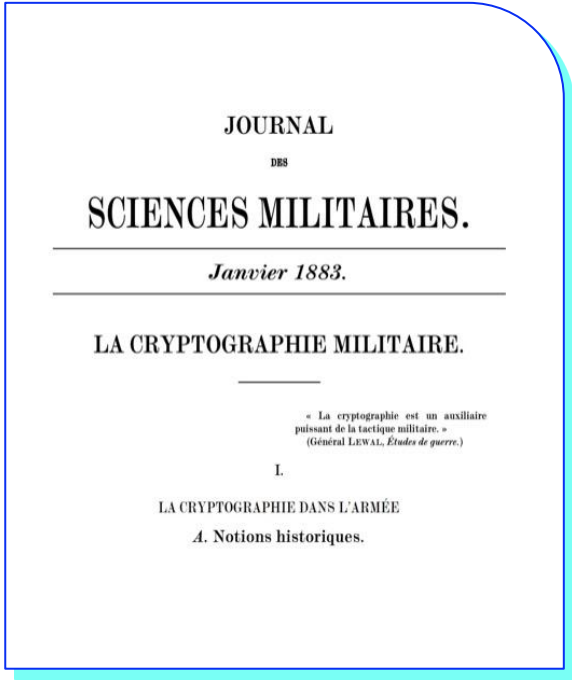
Las propiedades que debe cumplir son:

- **Integridad**: debe asegurar que los datos no sean modificados.
- **Confidencialidad**: debe asegurar que sólamente entidades autorizadas puedan acceder a los datos (aquellos que posean la clave).

- **Autenticación**: debe asegurar la identidad del remitente.
- **No repudio**: debe dejar constancia fehaciente del emisor, para que este no pueda negar que lo ha enviado.

Principios de Kerckhoffs (1883)

1. Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto
3. La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
4. Los criptogramas deberán dar resultados alfanuméricos.
5. El sistema debe ser operable por una única persona.
6. El sistema debe ser fácil de utilizar.



JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général LEWAL, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

¡Sigamos trabajando!