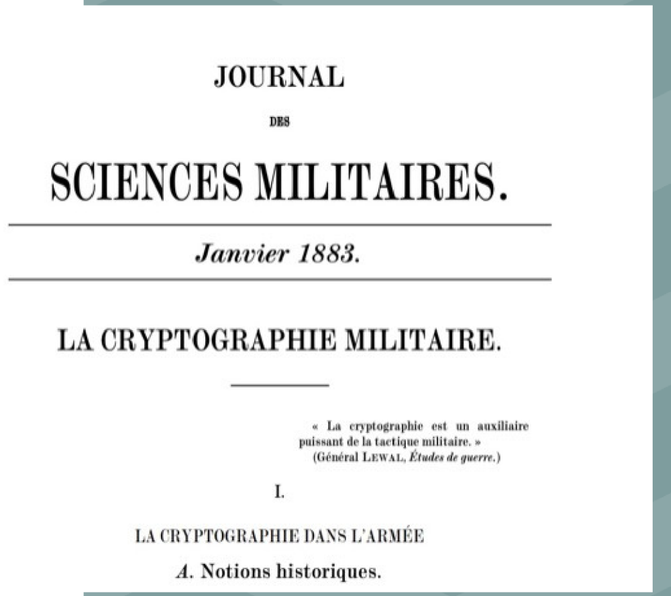
PRINCIPIOS DE LA CRIPTOGRAFÍA

SEGUN EL ENSAYO DE AUGUST KERCKHOFFS (1883)

PRINCIPIOS DE KERCKHOFFS

Augusto Kerckhoffs, criptógrafo holandés, quien fue publicado en el ensayo "La criptografía militar" (La cryptographie militaire) en el Journal des Sciences Militaires en 1883 es el paradigma fundamental de la criptografía y establece que:



JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

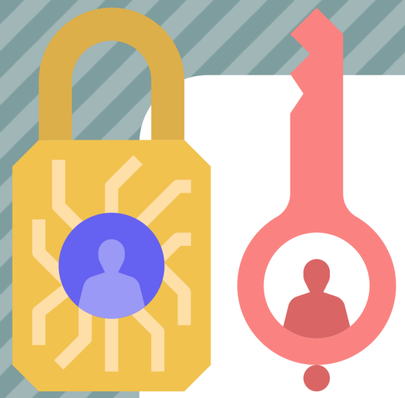
LA CRYPTOGRAPHIE MILITAIRE.

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

I.

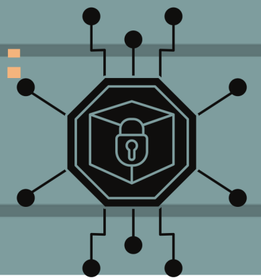
LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.



"La seguridad de un criptosistema no debe depender de mantener secreto el algoritmo de cifrado empleado. La seguridad depende solo de mantener secreta la clave.”

ES POR ELLO QUE LOS 6 PRINCIPIOS DE KERCKHOFFS ESTABLECEN QUE:



- Si el sistema debe ser en la práctica indescifrable, en caso de que no lo sea matemáticamente.

- El sistema no debe ser secreto y no debe ser problema que este caiga en las manos del enemigo. (En la actualidad es mejor utilizar sistemas de cifrado estandarizado).

- La clave del sistema debe ser fácil de memorizar y comunicar a otros sin necesidad de escribirla, podrán cambiarla y modificarla los interlocutores válidos.

- De ser aplicable a la correspondencia telegráfica. (Correspondencia digital en la actualidad).

- El sistema debe ser portable y no deberá requerir la intervención de varias personas.

- El sistema debe ser fácil de utilizar, no deberá requerir de conocimientos especiales ni tendrá una serie de largas reglas.