Criptografía

Profesor: Melvin Fernández Ch.

Video 1

fidélitas

Virtual

fidélitas Virtual

Historia y Evolución de la Criptografía

Módulo: 1

Criptología

La criptología (del griego criptos=ocultos y logos=tratado, ciencia), se compone de:

- ***Criptografía:*** *procedimientos para cifrar, o enmascarar información de carácter confidencial.*

- ***Criptoanálisis:*** *procedimientos para descifrar y recuperar la información original.*

Definición de criptografía

Disciplina que incorpora los principios, medios y métodos para la transformación de datos con el fin de ocultar su contenido semántico, evitar su uso no autorizado o evitar su modificación no detectada.

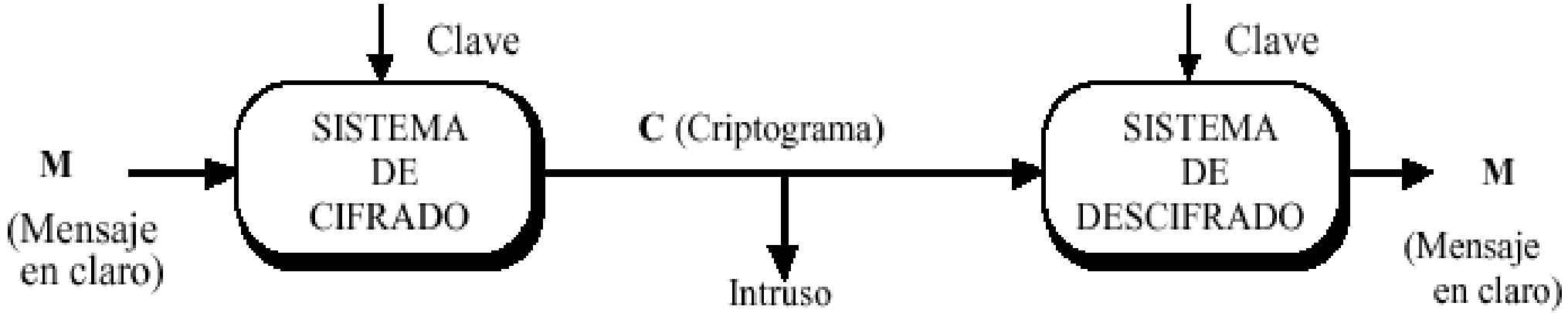
Definición de criptografía

Se trata de un conjunto de herramientas matemáticas, técnicas y algoritmos, que con el uso de una o más claves permiten cifrar la información y, por tanto, protegerla y dotarle al menos de los principios de confidencialidad y de integridad.

Definición de criptografía

Un sistema o producto que provee encriptación y desencriptación se refiere como un cripto sistema.

Sistemas Criptográficos



Esquema de transmisión segura de un mensaje

Sistemas Criptográficos

fidélitas Virtual

- Función de un sistema criptográfico
  - Es el encargado de calcular el mensaje cifrado C, a partir del mensaje en claro M y de la "clave de cifrado"; y de realizar el proceso inverso, el descifrado, y así determinar M a partir del mensaje cifrado y la "clave de descifrado".
  - Claves iguales: Algoritmos simétricos
  - Claves diferentes: Algoritmos asimétricos

Gracias

fidélitas Virtual