Criptografía

Profesor: Melvin Fernández Ch.

Video 5

fidélitas

Virtual

fidélitas Virtual

Criptografía clásica y cifra moderna

Módulo: 2

Criptografía moderna

- Existen tres hechos históricos que marcan el inicio de la criptografía moderna:

  - El primero de ellos son los trabajos sobre la teoría de la información y el secreto en los sistemas de cifra que el ingeniero y matemático Claude Shannon publica en 1948 y 1949, donde profundiza en los aspectos teóricos y matemáticos de la criptografía, dotándole así definitivamente de un marco científico.

Criptografía moderna

- El segundo hecho es la irrupción de la criptografía en la vida civil y en el ciudadano común, con la publicación en 1976 del algoritmo DES (Data Encryption Standard) estándar mundial autorizado para la cifra de datos no clasificados.

Criptografía moderna

- El tercer hecho se produce en 1976, cuando los investigadores de la Universidad de Stanford Whitfield Diffie y Martin Hellman proponen un protocolo para el intercambio seguro de una clave secreta.

Este intercambio de clave entre dos interlocutores separados físicamente había sido la piedra filosofal de la criptografía buscada durante siglos por los criptógrafos, puesto que la seguridad del sistema debía residir únicamente en la clave, y esta no podía ser intercambiada en un medio que por definición era inseguro.

La importancia de las claves

- La clave es el patrón que usan los algoritmos de cifrado y descifrado para manipular los mensajes en uno u otro sentido.

- El uso de claves añade más seguridad a los mecanismos de cifrado porque con distintas claves se pueden obtener distintos mensajes cifrados usando la misma función de cifrado.

- Para romper un sistema de cifrado es necesario conocer tanto las funciones correspondientes como la clave usada para cifrar un determinado objeto.

Características de los sistemas modernos

- Los procedimientos criptográficos sirven para proteger nuestra identidad, de ahí que se encuentren presentes en muchos aspectos de nuestro quehacer diario, como por ejemplo:

  - Comercio electrónico
  - Cifrado de comunicaciones
  - Cifrado de almacenamiento

Usos de la Criptografía moderna: Comercio electrónico

Compras en línea

Con dispositivos móviles

Pagos con tarjetas de crédito, debito, etc.

Pago de impuestos

Usos de la Criptografía moderna: Cifrado de comunicaciones

Correo electrónico

Redes inalámbricas

Redes sociales

Mensajería instantánea

Intercambio de documentos

Radio/TV

Usos de la Criptografía moderna: Cifrado de almacenamiento

Bases de datos

Dispositivo de almacenamiento

Almacenamiento distribuido

Gracias

fidélitas Virtual