Cifrado

Ing. Pablo Alejandro Godoy Díaz - Estructura de Datos II (2017)

1

Criptografía

Conceptos Clave

Concepto

- Es la práctica y estudio de técnicas de comunicación segura
  - ¿Por qué nos sirve?
  - Por la existencia de “terceros”

Concepto

- Intenta prevenir que terceros o el público entiendan el contenido de un mensaje
  - Matemática
  - Ciencias de la computación
  - Ingeniería eléctrica
  - Ciencias de la comunicación

Objetivos

- Confidencialidad de la información
- Integridad de los datos
- Vinculación con el emisor
- Autenticación de documentos

2

Cifrado

Conceptos Clave

Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger.

Rae

“La práctica de codificar y descodificar datos es lo que se conoce como "cifrado".

Kaspersky

Concepto

- Cuando se cifran datos, se aplica un algoritmo que los codifica para que no se muestren en su estado original y no se puedan leer

3

Criptografía

Los primeros cifrados

Cifrado por Transposición

- Reorganización de letras o caracteres
- Tanto el emisor como el receptor deben tener un acuerdo de cómo organizar de nuevo

Cifrado por Transposición

Algunos ejemplos de estos cifrados son:

- Cifrado en Zig-Zag
- Cifrado César
- Cifrado de Ruta
  - Vertical
  - Espiral

Ejemplo

Cifrar la frase:

My spider senses are tingling

4

Firmas Digitales

Concepto

- ¿Para qué sirve una firma?
- ¿Cuándo utilizamos nuestra firma?
- Al igual que la firma manuscrita, representa autenticidad
- A diferencia de una firma manuscrita, una firma digital está en un documento a parte.

Proceso de Firma

- Toma una “huella” digital
  - Hash
  - Es única del documento
- Se cifra matemáticamente la huella digital con la llave privada del firmante
- El documento original, la huella digital y la clave pública en un solo archivo se denomina archivo firmado

Proceso de Verificación

- Con la llave pública se descifra la huella digital
- Se obtiene la huella digital proveniente del documento firmado
- Se comparan ambas huellas y se define si el certificado es válido o no

Usos Conceptuales

- Valida la identidad del emisor
- Evita falsificación de documentos
- Promueve la seguridad de los datos confidenciales

Usos Prácticos

- Comunicación fiable entre empresas
- Facturas electrónicas
- Transacciones personales en línea

¡Gracias por su atención!