U.T. Nº4: Sistemas de identificación. Criptografía

Horas: 20

Orientaciones

Esta unidad vuelve a tener un enfoque tanto teórico como práctico. Se comienza la unidad introduciendo al alumno en el concepto de criptografía, un concepto nuevo hasta el momento. Se proponen algunos métodos sencillos como introducción y, posteriormente, se introducen las diferentes técnicas utilizadas hoy en día. Una vez que el alumno o alumna comprende el funcionamiento de cada técnica, se le da a conocer los certificados digitales, asociándolos a algunas técnicas vistas anteriormente y mostrando un enfoque práctico con los certificados de usuario. Por último, se vuelven a poner en práctica los conceptos vistos en la primera mitad de la unidad, mediante la herramienta GPG sobre un entorno Linux.

Objetivos

Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

- Conocer el concepto de criptografía y comprender el funcionamiento de sus diferentes técnicas.
- Saber obtener y utilizar certificados digitales así como conocer su funcionamiento y relacionarlo con las técnicas criptográficas vistas.
- Comprender y saber utilizar las principales instrucciones de la herramienta GnuPG en un entorno Linux.

Criterios de evaluación

a) Conoce las razones que hacen necesaria la criptografía para afianzar la seguridad informática.
b) Conoce la evolución histórica de la criptografía.
c) Conoce diferentes tipos de cifrado actuales.
d) Conoce las principales aplicaciones de la criptografía moderna y sus algoritmos y

funciones.

Contenidos soporte

- Introducción a la criptografía.
  - Aspectos de seguridad.
  - Concepto de criptografía.
  - Historia.
  - Primeros métodos de cifrado.
- Técnicas criptográficas
  - Criptografía simétrica.
  - Inconvenientes de la criptografía simétrica.
  - Criptografía de clave pública.
  - Firmas digitales.
  - Funciones 'hash'.
  - Sobres digitales.

Contenidos organizadores:

- Certificados digitales.
  - Autoridades de certificación.
  - Obtener un certificado digital en España.
  - PKI.
- Herramienta GPG en Linux.
  - Comandos para el cifrado simétrico.
  - Comandos para el cifrado asimétrico (de clave pública).