ADMINISTRACIÓN DE REDES Y SEGURIDAD

TRABAJO PRÁCTICO 3

November 19, 2018

Cátedra:
Lic: Zappellini, Bruno Damian

Integrantes:
Toledo Margalef, Pablo Adrian
UNPSJB - Trelew

CRIPTOGRAFÍA Y SUS APLICACIONES

Conceptos Básicos

1. (a) Encriptación simétrica, pero intercambio de claves a través de algún medio seguro
   (b) Encriptación simétrica
   (c) Encriptación asimétrica
2. (a) Verdadero.
   (b) Falso. EL encriptado asimétrico hace crecer el payload considerablemente.
   (c) Falso. El mecanismo seguro de intercambio de claves es necesario para encriptación simétrica.

Aplicaciones de Criptografía

PKI

Para poder verificar la firma en un mail recibido es necesario conocer la información de la autoridad certificante, que figura en la información del correo electrónico envíado. CUando el cliente de corre recibe el mensaje con su firma, busca en la autoridad la información necesaria para verificar el mensaje y realiza el camino para obtener una nueva firma. Si la firma obtenida es igual a la que figura en el mensaje, quiere decir que la firma es auténtica y el mensaje no fue alterado en su camino de origen a destino.

Para poder enviar un mail encriptado es necesario tener generado mi par de claves pública y privada, para poder realizar la encriptación y decriptación de los mensajes. También es necesario que el otro extremo de la conversación reciba mi clave pública para poder descifrar el mensaje recibido.

Para poder recibir un mail encriptado y poder abrirlo es necesario poseer la clave pública del remitente.