Tarea 12-13. Correo electrónico seguro

Objetivos

- Comprender y utilizar mecanismos de comunicación segura (firma y cifrado digital).
- Aprender a enviar y recibir mensajes de correo electrónico firmados y/o cifrados.

Preparación

Para realizar el ejercicio se necesita un ordenador personal donde se pueda instalar el software adecuado.

- Instalar un cliente de correo electrónico con soporte para firma digital. Se recomienda "Thunderbird".
- Configurar el cliente de correo electrónico para acceder a una cuenta de correo de la que disponga el alumno. Se recomienda usar la cuenta proporcionada por la Universidad.
- Configurar el cliente para poder enviar y recibir correo cifrado/firmado. Dos opciones:
  - Usar un certificado tipo MIME (como el de la Fábrica Nacional de Moneda y Timbre –FNMT–). Instalar el certificado en el cliente de correo. Thunderbird soporta este tipo de certificados de fábrica.
  - Usar un certificado tipo OpenPGP. Necesita de la instalación del software PGP, generar un certificado y un módulo para el cliente de correo. El módulo Enigmail para Thunderbird permite hacer todo esto de forma sencilla. Es la opción a utilizar si no se dispone de un certificado MIME.

Procedimiento

1. Enviar un mensaje de correo electrónico al profesor (mensaje 1) firmado digitalmente.
2. El profesor responderá al mensaje (respuesta 1). Usar la dirección *jjchico@dte.us.es*.
3. Responder a la respuesta 1 con un mensaje firmado y cifrado para el profesor (mensaje 2). Para ello necesitará conseguir la clave pública del profesor.
4. El profesor responderá con otro mensaje (respuesta 2) que irá cifrado para el alumno.
5. Responder a la respuesta 2 con un nuevo mensaje (mensaje 3) para verificar que se ha podido acceder al contenido de la respuesta 2. El mensaje 3 debe ir cifrado para el profesor y firmado por el alumno.