REDES DE COMUNICACIONES II

Práctica 2 - Seguridad y criptografía

Volver a: Prácticas

2 Funcionalidad

2.2 Cifrado y firma de archivos

Como se trata de un servicio seguro, los ficheros deberán ser subidos al servidor firmados y cifrados, utilizando la petición del API adecuada. Para ello, deberá utilizar un esquema híbrido, con el orden correcto para la firma y cifrado, el uso de clave de sesión, etc...

Para que todos los archivos protegidos sean compatibles entre distintos usuarios, el cliente deberá utilizar las siguientes primitivas criptográficas:

- *Cifrado simétrico*: AES con modo de encadenamiento CBC, con IV de 16 bytes, y longitud de clave de 256 bits.
- *Función hash*: SHA256
- *Cifrado asimétrico*: RSA con longitud de clave de 2048 bits.

Por otro lado, los adjuntos al mensaje (tanto firma como sobre digital) se concatenarán delante del mismo.

El cliente deberá también poder cifrar y firmar archivos de forma autónoma, sin que éstos sean subidos a SecureBox, con las opciones `--encrypt`, `--sign` y `--enc_sign`, para cifrar, firma y cifrar y firmar, respectivamente. Para comprobar el funcionamiento, aquí puedes encontrar un archivo firmado y cifrado para un usuario con ésta clave privada.

Volver a: Prácticas