Digital Signature

Objetivo

Implementar en parejas el esquema básico de firma digital haciendo uso de bibliotecas existentes para las funciones HASH y RSA.

Instrucciones

- Implementar la Función Hash de su preferencia (SHA1, SHA2)
- Hacer uso de su implementación de RSA considerando que
  - Generación de parámetros. (solo una vez para emisor y una vez para receptor)
  - Cada usuario deberá tener en su página web el link para descargar su llave pública

- En la figura 1, se muestra el proceso de Firma/Verificación con lo que se ofrece autenticación.
- Elaborar un vídeo (máximo 5 minutos) en donde Alicia firme un documento, muestren y vayan explicando todo sobre los parámetros que se utilizan. Betito tiene que hacer el proceso de verificación descargando en ese momento la llave de la página de Alicia para corroborar que es de ella el mensaje y mostrar que pasaría si se utiliza una llave incorrecta. (Ej. Candy)