Objetivo

Implementar en equipo (1,2 o 3 personas) el esquema básico de firma digital haciendo uso de bibliotecas existentes para las funciones HASH y RSA.

Instrucciones

- Implementar la Función Hash SHA1
- Implementar RSA 1024 considerando que
  - Generación de parámetros. (solo una vez para cada actor)
  - 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 7 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. Candy debe hacer los ataques de modificación y usurpación (explicar en el vídeo paso a paso como Candy realiza dichos ataques y paso a paso cómo Betito lo detecta)