Seguridad de la Información – CURSO 2025-2026

Práctica 3: Cifrado asimétrico

Los objetivos de esta práctica son el manejo de comandos de la herramienta OpenSSL para la realización de operaciones criptográficas, relativas al cifrado asimétrico, como la generación y gestión de claves criptográficas, el cifrado de resúmenes (integridad y autenticación) y el cifrado de claves simétricas (confidencialidad).

Previo a la realización de la práctica, es imprescindible:

- Tener instalado OpenSSL versión 3 o superior, con modo "Legacy" activado
- Conocer el manejo básico de OpenSSL en modo comando, especialmente
    - openssl-dgst
        - algoritmos de resumen (-sha1 -sha-256 -md5 etc.)
        - posibilidad de firmar resúmenes (mejor con openssl-pkeyutl)
    - openssl-enc
        - Algoritmos, modos de operación (openssl enc -list-ciphers)
        - Ficheros cifrados binarios y en BASE64
        - Cifrado con contraseña (y sal) o con clave/vector
        - Derivación de claves a partir de contraseña: -pbkdf1 y -pbkdf2 (**pbkdf2** será siempre **obligatorio**)
    - openssl-genpkey
        - generación de claves asimétricas
    - openssl-pkey
        - visualización de claves asimétricas, conversión de formatos
    - openssl-pkeyutl
        - cifrado, descifrado, firma, verificación y derivación con claves asimétricas
    - Otros comandos (openssl enc, etc.).

Documentación básica:

- Documentación de Openssl (https://www.openssl.org/docs/man3.2/index.html)
- Openssl Howto (https://openssl.cicei.com)
- Algoritmos de resumen MD5, SHA-1, SHA2 (256,384,512), SHA-3 (idem), Whirlpool, etc.
- Algoritmos de cifrado simétrico AES (128, 192, 256), DES, TDES, IDEA, CHACHA20, etc.
    - Wikipedia AES DES TDES IDEA CHACHA20 etc.
- Modos de operación de cifrado en bloque:
    - (https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)
- Algoritmos de cifrado y firma asimétricos (RSA)
- Algoritmos de firma asimétricos (DSA, ECDSA)
- Algoritmos de negociación de secretos asimétricos (DH, ECDH, X25519)
- Derivación de claves y vectores de cifrado simétrico a partir de secretos asimétricos
- Wikipedia (https://wikipedia.com)
- ChatGPT (https://openai.com/chat) , DeepSeek (https://chat.deepseek.com), etc.

Práctica 3: Algoritmos de cifrado asimétrico

3.1 Generación de claves asimétricas (pública-privada), firmado de resúmenes (RSA y DSA) y derivación de secretos con claves DH y ECDH (X25519)

- Generar un par de claves asimétricas RSA de 2048 bits en formato PEM con contraseña.
- Exportar la clave pública a otro fichero PEM.
- Exportar la clave privada a formato DER (binario) y de vuelta a PEM, con otro nombre de fichero. Comprobar que **la conversión a formato DER desprotege la clave privada** (elimina la contraseña).
- Con el par de claves asimétricas creadas, firmar y comprobar la firma del resumen (con SHA-256) de uno de los ficheros de texto de la práctica anterior.
- Repetir los **cuatro pasos anteriores** con claves DSA.
- Generar dos pares de claves DH estándar y demostrar que la combinación pública1-privada2 genera el mismo secreto que la combinación privada1-pública2.
- Generar dos pares de claves DH con curva elíptica X25519 (las utilizadas por Whatsapp) y demostrar que la combinación pública1-privada2 genera el mismo secreto que la combinación privada1-pública2.
- Comparar los tamaños de los dos secretos (DH y X25519) generados anteriormente.

3.2 Intercambio de información segura (cifrado asimétrico de clave simétrica y firma)

En este apartado vamos a reproducir en una secuencia de operaciones el intercambio de información segura entre dos agentes utilizando cifrado simétrico, cifrado asimétrico de las claves simétricas y firma digital (cifrado asimétrico de un resumen del documento original).

Para ello, generaremos dos parejas de claves RSA de 2048 bits que serán utilizadas por dos agentes (Ana y Berto) de forma que Ana construirá tres ficheros de texto a partir del fichero de texto original, el primero con el fichero cifrado, el segundo con las claves utilizadas y el tercero con la firma digital. Así, primero generaremos las dos claves:

- Generar una pareja de claves RSA de 2048 bits en ficheros anapub.pem y anapriv.pem y otra pareja de claves del mismo tipo bertopub.pem y bertopriv.pem.
- Proteger ambas claves privadas con contraseña “anak” y “bertok” respectivamente.

Se supone que Ana y Berto han intercambiado sus claves públicas. A continuación, realizaremos el trabajo de Ana:

- Cifrar un fichero de texto (texto.txt) de los apartados anteriores con AES-256 en modo CBC, con clave y vector escogidos por el estudiante y sin sal, con salida en formato BASE64 a un fichero llamado cifrado.txt.
- Crear un fichero de texto (hexadecimal) con la concatenación de la clave y el vector utilizados, de nombre claves.hex y cifrarlo con la clave pública bertopub.pem, con salida en formato binario a un fichero claves.bin
- Convertir claves.bin a claves.txt en formato BASE64 (mediante openssl enc -a …)
- Obtener un resumen sha256 en binario del fichero de texto original con nombre resumen.bin y firmarlo (es decir, cifrarlo con la clave privada anapriv.pem -clave anak-), con salida en formato BASE64 a un fichero llamado firma.txt.

En este momento, Ana enviaría los tres ficheros obtenidos cifrado.txt, claves.txt y firma.txt (junto a la meta-información relativa a los algoritmos utilizados, cómo se concatenan clave y vector…) a Berto… que seremos nosotros mismos. Actuando como Berto, procederemos a:

- Convertir el fichero claves.txt a fichero binario claves2.bin con openssl enc -a…
- Descifrar el fichero claves2.bin con la clave privada bertopriv.pem (contraseña bertok) y salida a un fichero claves2.hex (debería ser idéntico a claves.hex).
- Extraer de claves2.hex la clave y el vector en formato hexadecimal, siguiendo la meta-información que le envió Ana junto con los tres ficheros).
- Descifrar el fichero cifrado.txt con la clave y el vector obtenidos (de claves2.hex) y salida al fichero mensaje2.txt (que debería ser igual al fichero original mensaje.txt utilizado por Ana).
- Verificar que el fichero firma.txt, convertido a binario y descifrado con la clave pública de Ana (anapub.pem), coincide con un resumen sha256 del fichero mensaje2.txt. **Muy importante:** asegurarse de que utilizan la opción **-verifyrestore** para recuperar el resumen obtenido por Ana descifrando su firma y compararlo con un resumen obtenido por Berto.

Documentación y entrega de la práctica 3:

Se ha de preparar un **DOCUMENTO DE TEXTO** (en PDF) **documentando exhaustivamente los pasos realizados en cada una de las partes de esta práctica**. El número de páginas no será inferior a 6, y se incluirán listados de todos los ficheros obtenidos en formato texto, hexadecimal, base64, PEM o similar, según cada caso. con ejemplos de los resultados obtenidos (parte binaria en hexadecimal, base64 o PEM) y profusión de recortes de volcados de pantalla en los que se ha PERSONALIZADO el "prompt" de la consola con el nombre y apellido del estudiante (por ejemplo, en mi caso, usaría el comando **export PS1="Antonio Ocon> "). Este "prompt" personalizado se ha de mostrar en TODAS las restantes prácticas** que conlleven capturas de pantalla del sistema operativo.

Los estudiantes que **siguen la asignatura por curso defenderán personalmente cada práctica al profesor en el laboratorio**. Como máximo podrán entregar cada práctica dos semanas después del período de finalización de la misma.

Los estudiantes que **no siguen la asignatura por curso deberán subir el programa completo de prácticas a la plataforma en convocatoria extraordinaria o especial**, en las fechas indicadas en la página de la asignatura.