Práctica 2. Criptografía asimétrica y aplicaciones prácticas (2 puntos)

Esta práctica se realiza en grupo (mismos integrantes que para el trabajo tutelado).

El objetivo de esta práctica es que refuerce los conceptos de criptografía asimétrica vistos en clase de teoría y que pruebe herramientas relacionadas.

NOTAS:

1) Todos los ejercicios deben ser realizados por todos los integrantes del grupo, aunque en la memoria, bastará con que se incluyan las evidencias de uno de ellos.
2) No se debe entregar, ni publicar en la memoria ninguna de las claves privadas.
3) En la nomenclatura de los archivos, *GN* hace referencia a su grupo de prácticas (p.ej: 1.1.1)
4) Todos los integrantes del grupo deben conservar los mensajes de prueba utilizados en la práctica, de cara para la defensa. Asimismo, los mensajes deben tener "asuntos" suficientemente descriptivos de la prueba realizada (P. ej: "Prueba de correo electrónico firmado con la clave 0x1234" en lugar de "Prueba 3" o "sin asunto")

1) Utilizando Cryptool 1, generen un par de claves RSA de 2048 bits.
   a) Documenten el proceso.
   b) ¿Qué números conforman la clave pública?
   c) Realicen pruebas de cifrado y descifrado sobre el archivo `secreto.txt` disponible en el Campus Virtual. Comenten los resultados obtenidos.

2) Utilizando Cryptool 1, generen una clave D&H con 1000 < p < 2000.
   a) ¿Qué utilidad puede tener la clave obtenida?
   b) ¿Qué problemas de seguridad pueden darse con este método? ¿Cuál sería la solución?

3) Instalen la herramienta QuickHash y prueben las opciones básicas.
   a) Si se modifican los atributos de un archivo (p.ej. sólo lectura), ¿varía el hash?
   b) Busquen, prueben y documenten herramientas o comandos para calcular hashes, que estén disponibles de forma nativa en sistemas recientes de Windows, Linux y Mac OS.
   c) Seleccionen una cadena de texto de 6 letras (sólo minúsculas y sin ñ) y calculen su hash md5, al que nos referiremos como h1.
   d) Seleccionen una cadena de texto de 16 letras (sólo minúsculas y sin ñ) y calculen su hash md5 (h2).
   e) Seleccionen una cadena de texto de 6 letras (con minúsculas, mayúsculas, letra ñ/Ñ y números) y calculen su hash md5 (h3).

4) Instalen la herramienta John the Ripper y prueben las opciones básicas.
   a) Utilicen JtR para crackear el hash calculado en el apartado c del ejercicio 3. Describan las características de la máquina en la que ejecuta JtR, el comando JtR utilizado y el número de hashes por segundo que puede probar. ¿Cuánto tarda en crakear el hash?
   b) Calculen cuanto tardaría en crackear los hashes de los apartados d y e en la misma máquina.

5) Instalen la herramienta hashcat y prueben las opciones básicas.
   a) En la misma máquina que el ejercicio 4, utilicen hashcat para crackear el hash calculado en el apartado c del ejercicio 3.
   b) Comenten las diferencias observadas entre hashcat y JtR.

6) Utilizando 7-Zip generen un archivo comprimido protegido con contraseña, teniendo en cuenta lo siguiente:
   - El algoritmo de compresión debe ser .zip
   - La contraseña debe ser de 6 letras (sólo minúsculas y sin ñ)
   - El algoritmo de cifrado debe ser AES.
   - Tome como base el archivo `secreto.txt`.

   a) Documenten el proceso.
   b) Utilicen JtR para intentar obtener la contraseña. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados obtenidos.

7) En una máquina Linux de la que dispongan, revisen los archivos `/etc/passwd` y `/etc/shadow` y realicen lo siguiente:
   a) Indiquen cuál es el objetivo de esos archivos y expliquen el formato de los mismos (los campos que contienen y qué significa cada campo).
   b) Averigüen qué algoritmo de hash se está utilizando.
   c) ¿Cuál es el propósito del campo "*salt*"?
   d) Intenten calcular manualmente el hash de la contraseña de uno de los usuarios y comprueben si coincide con el que figura en el archivo.
   e) Utilicen JtR para intentar obtener la contraseña de algún usuario. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados obtenidos.

8) Seleccionen un sitio web que utilice https y cuyo certificado digital contenga una clave pública RSA.
   a) Descarguen el certificado y analícenlo con la herramienta OpenSSL.
   b) ¿Qué números conforman la clave pública? Indíquelos en hexadecimal y decimal.
   c) ¿Cuál es el tamaño de la clave en bits? En caso de que no lo indicase de manera explícita el certificado, ¿de qué forma se podría saber?
   d) ¿Cuál es el contenido del campo Common Name? ¿Por qué es importante este campo?

9) Utilizando OpenSSL:
   a) Indique el comando necesario para cifrar el archivo `secreto.txt` con el algoritmo AES con una clave de 256 bits.
   b) ¿Cómo es el tiempo, comparado con RSA?

10) Utilizando OpenSSL, genere una clave RSA de 2048 bits.
   a) Indique el comando utilizado y la clave pública obtenida.
   b) ¿Cuál es el número e de la clave pública?
   c) Indique el comando necesario para cifrar el archivo `secreto.txt` usando la clave pública generada.

11) Utilizando GnuPGP versión 2.X[1], generen un par de claves PGP asociadas a su cuenta de la UDC.
    a) Documenten los pasos seguidos.
    b) Exporten la clave pública en formato texto de cada uno y guárdenla con la siguiente sintaxis: *GN*_Apellido1_Apellido2,_Nombre.asc.

12) Descarguen el gestor de contraseñas KeepassXC (https://keepassxc.org/download). Antes de instalarlo, hagan lo siguiente:
    a) Verifiquen el archivo descargado con el hash sha-256 y la firma PGP que se facilitan en la web. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados.
    b) ¿Qué método de verificación es más seguro? ¿Cuál es la diferencia?
    c) En el caso de PGP, ¿cómo se puede verificar la autenticidad de la clave?
    d) Una vez verificado el archivo, instalen la herramienta y prueben las opciones básicas.
    e) Además de la usabilidad, ¿qué diferencia importante, en términos de seguridad, encuentran entre usar un gestor de contraseñas o un archivo de texto cifrado con AES, por ejemplo?

13) Búsqueda de claves.
    a) Utilizando un servidor de claves PGP, mediante línea de comandos, buscar claves PGP de personal de la UDC. Indiquen los comandos y opciones utilizadas. Indiquen si se obtienen los mismos resultados consultando servidores diferentes.
    a) Además de la búsqueda mediante línea de comandos, indiquen otros métodos de búsqueda. Indiquen si se obtienen los mismos resultados que en el apartado anterior.
    b) Seleccionar una de las claves descargada en los apartados anteriores y revisar sus principales parámetros (tipo de clave, longitud de la misma, firmas, …)

14) Exporten la clave pública generada en el ejercicio 11) en un formato adecuado para enviar por correo electrónico o publicar en un foro.
    a) Indiquen los comandos utilizados.
    b) Súbanla a la carpeta P2_PGP_Public_keys en Teams, siguiendo la nomenclatura *GN*_Apellido1_Apellido2,_Nombre.asc (p. ej.: Vazquez_Naya,_Jose.asc).

15) Realicen una copia de la clave privada generada en el ejercicio 11).
    a) Indiquen los comandos utilizados.

16) Eliminen de los anillos las claves generadas en el ejercicio 11) e instálenlas de nuevo a partir de la copia generada.
    a) Indiquen los comandos utilizados.

[1] Todos los ejercicios relativos a PGP deben realizarse utilizando GnuPGP versión 2.X o superior, pero puede utilizar el SO de su preferencia.

17) Seleccionen y descarguen una clave pública del directorio P2_PGP_Public_keys en Teams.
    a) Asegúrense de que dicha clave es auténtica. Y, en caso afirmativo, indíquenselo a su sistema PGP. Indiquen los comandos utilizados.
    b) Después de este paso, prueben a exportar de nuevo la clave y compararla con la original. ¿Son iguales? Indiquen los comandos utilizados.
    c) Indiquen también a su sistema PGP su confianza en el dueño de la clave. Indiquen los comandos utilizados.

18) Utilizando GPG en línea de comandos generen mensajes en un formato adecuado para enviar por correo electrónico. A continuación, envíen dichos mensajes utilizando la herramienta de correo electrónico de su elección, pero que no tenga activada la funcionalidad de PGP. Es decir, deben utilizar la herramienta de correo electrónico sólo para el envío del correo, no para la firma (ni otra operación relacionada con GPG). Concretamente, deben generar y enviar:
    a) Un mensaje firmado
    b) Un mensaje cifrado
    c) Un mensaje firmado y cifrado

    NOTA: Recuerden enviar directamente los mensajes en el cuerpo del correo, no como archivos adjuntos.

19) Utilizando GPG en línea de comandos, prueben a descifrar y/o verificar correos recibidos cifrados y/o firmados con GPG.
    a) Indiquen los comandos utilizados.

20) En caso de querer enviar un mensaje cifrado por correo electrónico a varios destinatarios. ¿cuál sería el procedimiento?

21) Editen su clave y añadan una nueva dirección de correo electrónico. ¿Ha cambiado el fingerprint?

22) Indiquen el comando necesario para subir su clave a un servidor de claves. No es necesario que ejecuten dicho comando. Recuerden que una vez subida una clave, se puede revocar, pero no eliminar del servidor de claves.

23) "Web of Trust"
    a) Diseñen, describan y ejecuten un caso de uso para comprobar el funcionamiento del modelo "Web of Trust".
    a) Indiquen cómo se comporta GPG al importar una clave firmada por alguien de su total confianza.

    NOTA: Con el objetivo de facilitar la corrección de este apartado, es importante describir con precisión el caso de uso (claves concretas utilizadas, qué firmas tiene cada clave, etc.).

24) Generen un nuevo par de claves PGP. Realicen algunas pruebas con ellas (firmar un texto, cifrarlo, firmarlo y cifrarlo).
    a) A continuación, revoquen dichas claves. Indiquen los comandos utilizados.
    b) Indiquen si se pueden seguir utilizando para firmar, verificar una firma, cifrar o descifrar.

25) Instalen Thunderbird (versión 78 o superior), configuren la cuenta de correo de la UDC e importen las claves PGP generadas en el ejercicio 11). A continuación, utilizando las facilidades GPG de la propia herramienta, prueben a:
    a) Enviar un mensaje firmado al resto de integrantes de su grupo
    b) Enviar un mensaje cifrado al resto de integrantes de su grupo
    c) Enviar un mensaje firmado y cifrado al resto de integrantes del grupo
    d) Verificar un mensaje firmado
    e) Descifrar un mensaje cifrado
    f) Descifrar y verificar un mensaje firmado y cifrado

26) Prueben a verificar y descifrar con Thunderbird los correos recibidos previamente, generados vía comandos gpg. Indiquen si funciona correctamente o se encuentra algún problema.

27) Busquen opciones disponibles actualmente para usar PGP desde Outlook Web.

28) Busquen información y hagan un resumen sobre el formato clave PGP, indicando los principales campos.

29) En los ejercicios anteriores se han realizado operaciones de cifrado y firma orientadas al correo electrónico, pero PGP también se puede utilizar para cifrar y firmar archivos. Tomando como ejemplo el .pdf de este documento:
    a) Indique el comando necesario para cifrarlo, de manera que lo pueda descifrar usted mismo.
    b) Indique el comando necesario para firmarlo.

30) Sigan los pasos vistos en clase para obtener un certificado digital de la FNMT.
    c) Documenten el proceso. ¿Dónde se generan las claves (¿en el navegador? ¿en la CA?). ¿En qué lugar se almacenan?
    d) Exporten el certificado de clave pública (¡no incluyan la clave privada!) de cada uno en formato PKCS #7 y guárdenlo con la siguiente sintaxis:
    `GN_Apellido1_Apellido2,_Nombre.p7b`

    NOTA:
    - IMPORTANTE: Tengan en cuenta que este certificado permite autenticación y firma digital con validez legal. De modo que deben almacenarlo en un lugar seguro y nunca revelar la clave privada.

31) Utilicen alguna herramienta de correo electrónico con soporte para S/MIME y prueben a enviar correos firmados, cifrados y firmados y cifrados[2] utilizando el certificado de la FNMT obtenido en el ejercicio anterior.

32) Prueben a realizar alguno de los ataques a S/MIME comentados en clase.

33) Busquen y prueben opciones disponibles actualmente para usar S/MIME desde Outlook Web. Documenten los resultados obtenidos.

[2] Tenga en cuenta que si utiliza un certificado reconocido (por ejemplo, el de la FNMT) la firma tiene validez legal. Para el desarrollo de la práctica firme únicamente mensajes de prueba.

Modo de entrega
Se entregará vía Campus Virtual, sólo una entrega por grupo. Un único archivo *GN*.zip, que debe contener:

- Memoria, en formato .pdf.
    - Copien el enunciado de cada ejercicio tal cual, sin modificaciones, y respondan dentro de cada apartado (a), b), etc.)
    - Es importante responder con claridad a lo que se pide en cada ejercicio, y aportar evidencias suficientes de que han realizado los ejercicios (capturas de pantalla, comandos concretos utilizados, explicaciones, etc.).
    - Se valorará positivamente el que la memoria está firmada digitalmente por todos los integrantes del grupo.
- Archivos indicados en el enunciado de la práctica, directamente sobre el directorio raíz, sin subcarpetas, respetando la nomenclatura indicada.

Fecha de entrega
La **fecha límite** es el jueves **1 de diciembre de 2022 a las 13:30**.

Defensa
Posteriormente a la entrega, el profesor indicará una fecha para la defensa de la práctica. En la defensa deben estar presentes todos los integrantes del grupo.