Práctica 2. Criptografía asimétrica y aplicaciones (1,6 puntos)

NOTAS:

1) Esta práctica se realiza en grupos de 4 personas.
2) 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.
3) En la nomenclatura de los archivos, reemplacen *GN* por el código asignado a su grupo de prácticas (p.ej: 1.1).
4) No deben entregar, ni publicar en la memoria ninguna de sus claves privadas.
5) Todos los integrantes del grupo deben conservar los mensajes de prueba utilizados en la práctica, de cara a 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")

Cifrado asimétrico

1) Utilizando la opción "Demostración RSA" en Cryptool 1, recreen el ejemplo visto en clase de teoría y muestren un ejemplo de cifrado de un texto de su elección.
   a) Documenten el proceso.

2) Utilizando la opción "Demostración Diffie-Hellman" en 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) Utilizando la opción de "Generar/Importar Claves" de 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.

4) Utilizando OpenSSL, generen una clave RSA de 2048 bits.
   a) Indiquen el comando utilizado.
   b) ¿Qué números conforman la clave pública?
   c) Prueben a cifrar el archivo `secreto.txt` usando la clave pública generada. ¿Encuentran algún problema? Caso afirmativo, planteen una solución al mismo.

Funciones hash

5) Herramientas para cálculo de hashes
   a) 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.
   b) Instalen la herramienta QuickHash GUI[1]. Prueben las opciones básicas y muestren evidencia de ello.
   c) Al calcular el hash de un archivo con alguna de las anteriores herramientas, si se modifican los atributos del archivo (p.ej. sólo lectura), ¿varía el hash?

[1] https://quickhash-gui.org/

6) Utilizando la librería hashlib de Python, desarrollen una función que permita calcular el hash md5, sha-1 o sha-256 de un texto introducido por pantalla o de un archivo, a elección del usuario.
   a) El algoritmo debe poder ejecutarse desde una terminal, invocando al comando `hash.py` y pasándole los argumentos y parámetros necesarios.
      - El parámetro `--help` debe mostrar la sintaxis y las instrucciones de uso. Muestren en la memoria la salida del comando con este parámetro.
      - Guarden el código implementado para su posterior entrega en una carpeta denominada `hash`.
   b) Comprueben con la ayuda de QuickHash GUI o de Cryptool 1, que su implementación es correcta y muestren evidencia de ello.

7) Utilizando la herramienta de su elección, calculen el md5 de las siguientes cadenas de texto:
   - h1 = md5(`ajtxnk`)
   - h2 = md5(`casalibropezmar`)
   - h3 = md5(`C0ruñ4`)

   a) Si esas cadenas fuesen utilizadas como contraseña, ¿cuál diría que es la más segura?

8) Instalen la herramienta John the Ripper.
   a) Prueben las opciones básicas y muestren evidencia de ello.
   b) Utilicen JtR para crackear el hash h1.
      - Describan las características de la máquina en la que ejecuta JtR
      - Indiquen el comando JtR utilizado y el número de hashes por segundo que puede probar y el tiempo empleado en crackear el hash
   c) Calculen matemáticamente cuanto se tardaría en crackear los hashes h2 y h3 en la misma máquina.

9) Instalen la herramienta hashcat.
   a) Prueben las opciones básicas y muestren evidencia de ello.
   b) En la misma máquina que el ejercicio anterior, utilicen hashcat para crackear h1.
      - Indiquen el comando hashcat utilizado y el número de hashes por segundo que puede probar y el tiempo empleado en crackear el hash.

10) 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` disponible en el Campus Virtual.
    - Documenten el proceso.

    a) Utilicen JtR para intentar obtener la contraseña. Indiquen los comandos utilizados y muestren capturas de pantalla de los resultados obtenidos.
    b) Utilizando lo aprendido, intenten obtener la contraseña del archivo secreto.zip.

11) Revisen los archivos `passwd` y `shadow` disponibles en Campus Virtual y realicen lo siguiente:
    a) Indiquen cuál es el objetivo de esos archivos y expliquen el formato detallado de los mismos (los campos que contienen y qué significa cada campo).
    b) ¿Qué algoritmo de hash se está utilizando?
    c) ¿Cuál es el propósito del campo "*salt*"?
    d) Sabiendo que la contraseña del usuario pepe es "`España`" (sin comillas), indiquen los pasos para calcular el hash de la contraseña y comprueben si coincide con el que figura en el archivo.
    e) Utilicen JtR para intentar obtener la contraseña del usuario `root`. Documenten el proceso.

Certificados digitales y Autoridades de Certificación

12) Seleccionen 5 sitios web que utilicen https.
    a) Revisen los datos de los certificados e indiquen, para cada uno, qué algoritmo o algoritmos de cifrado se utilizan.
    b) Seleccionen 1 de los certificados anteriores, que utilicen cifrado RSA, descarguen dicho certificado y analícenlo más detalladamente con la herramienta OpenSSL.
        - ¿Qué números conforman la clave pública? Indíquelos en hexadecimal y decimal.
        - ¿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?
        - ¿Cuál es el contenido del campo *Common Name*? ¿Por qué es importante este campo?
        - ¿Qué Autoridad Certificadora emitió el certificado?

13) Sigan los pasos vistos en clase para obtener un certificado digital de la FNMT.
    a) Documenten el proceso. ¿Dónde se generan las claves (¿en el navegador? ¿en la CA?). ¿En qué lugar se almacenan?
    b) 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`
    c) Usando OpenSSL, analicen los campos del certificado de clave pública. ¿Cuáles son los "usos" válidos para el certificado?

    NOTAS:
        - Si ya disponen previamente de un certificado de la FNMT, comuníquenselo al profesor de prácticas.
        - 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.

Seguridad en Correo Electrónico

14) Utilizando GnuPGP versión 2.X[2],
    a) Generen un par de claves PGP asociadas a su cuenta de la UDC. Documenten los pasos seguidos.
    b) Exporten la clave pública de cada uno en un formato adecuado para enviar por correo electrónico o publicar en un foro. Documenten los pasos seguidos.
    c) Súbanla a la carpeta `P2_PGP_Public_keys` en Teams, siguiendo la nomenclatura: `GN_Apellido1_Apellido2,_Nombre.asc`. (p. ej.: `1.1_Vazquez_Naya,_Jose.asc`).
    d) Indiquen en la memoria el *fingerprint* de las claves de todos los integrantes del equipo.
    e) Realicen copia de su clave privada y almacénenla en un lugar seguro (cada uno la suya). Documenten los pasos seguidos.

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

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

16) Edición de clave:
    a) Añadan una nueva dirección de correo electrónico. Documenten el proceso.
    b) Cambien la fecha de expiración de su clave al 04/05/2025. Documenten el proceso.
    c) Después de estos cambios, ¿ha cambiado el *fingerprint*?

17) Búsqueda de claves.
    a) Utilizando un servidor de claves PGP, mediante línea de comandos, busquen claves PGP de personal de la UDC y del MIT. Indiquen los comandos y opciones utilizadas. Indiquen si se obtienen los mismos resultados consultando servidores diferentes.
    b) 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.
    c) Seleccionen una de las claves descargada en los apartados anteriores y revisen sus parámetros principales (tipo de clave, longitud de la misma, firmas, …)

18) Seleccionen y descarguen una clave pública del directorio `P2_PGP_Public_keys` en Teams.
    a) Comprueben 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. Señalen las diferencias.
    c) Indiquen también a su sistema PGP su confianza en el dueño de la clave. Indiquen los comandos utilizados.

19) Utilizando GPG en línea de comandos generen mensajes en un formato adecuado para enviar por correo electrónico. A continuación, envíen dichos mensajes utilizando Outlook Web (sin hacer uso de ningún plugin o extensión para PGP). Concretamente, deben generar y enviar:
    a) Un mensaje firmado para el resto de integrantes del grupo
    b) Un mensaje cifrado para el resto de integrantes del grupo
    c) Un mensaje firmado y cifrado para el resto de integrantes del grupo

    NOTA: No envíen los mensajes como archivos adjuntos.

20) Instalen Thunderbird (versión 78 o superior)
    a) Configuren la cuenta de correo de la UDC e importen las claves PGP generadas en el ejercicio 14). Documenten el proceso.
    b) Comprueben que Thunderbird procesa correctamente los correos recibidos generados en el ejercicio 19)
    c) Realicen pruebas de envío y recepción de mensajes, utilizando las facilidades GPG de la propia herramienta. Documenten el proceso.

21) "Web of Trust"
    a) Diseñen, describan y ejecuten un caso de uso para comprobar el funcionamiento del modelo "Web of Trust".
    b) 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.).

22) Generen un nuevo par de claves PGP y 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.
    c) Hagan copia, elimínenlas y vuelvan a instalarlas en su sistema. Documenten el proceso. ¿Qué ocurre con los datos de confianza?

23) Busquen y prueben opciones disponibles actualmente para usar PGP desde Outlook Web. Documenten los resultados obtenidos.

24) 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.

25) Utilicen alguna herramienta de correo electrónico con soporte para S/MIME y prueben a enviar correos firmados, cifrados y firmados y cifrados[3]. Pueden utilizar sus certificados de la FNMT, si soportan esta opción, recurrir a alguna CA que permita obtener certificados digitales de forma gratuita, o bien generarlos ustedes mismos con la herramienta OpenSSL.

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

Modo y fecha de entrega

La memoria y resto de archivos, se entregarán vía Campus Virtual, no más tarde del **lunes 25 de noviembre a las 10:00**. Sólo una entrega por grupo. Un único archivo *GN*_P2.zip, que debe contener:

- Memoria, en formato .pdf:
    - No agrupen ni cambien el orden de ejercicios ni apartados. Mantengan la numeración de los ejercicios y apartados y respondan con claridad a lo que se pide en cada uno de ellos.
    - Aporten evidencias suficientes del trabajo realizado (capturas de pantalla, comandos concretos utilizados, explicaciones, etc.).
    - Se valorará positivamente el que la memoria esté firmada digitalmente por todos los integrantes del grupo, haciendo uso del certificado de la FNMT.
- Archivos indicados en el enunciado de la práctica, respetando la nomenclatura indicada.

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, cada uno con su ordenador y todo lo necesario para poder mostrar cualquier ejercicio de la práctica.

[3] 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.