Práctica 2 - Criptografía y sus aplicaciones

Conceptos básicos

1. Dados los siguientes casos, determine cuál de los sistemas de cifrado resulta más adecuado (simétrico y asimétrico). Si decide utilizar el sistema de cifrado asimétrico, determine qué clave usaría para realizar el proceso de encriptado. Justifique brevemente su elección:

    a. Juan quiere mandarle un mensaje a Julio. A Julio no le importa asegurarse que el mensaje fue enviado por Juan, sin embargo Juan quiere estar seguro de que el mensaje no podrá ser leído ni alterado por un tercero. Juan trabaja en una empresa en Argentina y Julio es empleado de una empresa ubicada en España.

    b. Adriana y Leandro quieren comunicarse en forma segura. Para ellos resulta fácil conseguir un medio seguro para intercambiar información que luego necesiten para realizar esta comunicación segura. En este caso lo que importa es que nadie pueda espiar los datos involucrados en dicha comunicación.

    c. Analía usará el correo electrónico para enviar la aceptación de un contrato al Estudio en el cual trabaja. Para la persona que lo reciba es importante tener la garantía de que el mismo fue enviado efectivamente por Analía.

2. Para cada afirmación determine si es verdadera o falsa:

    En los criptosistemas simétricos no puede garantizarse el no repudio porque ambas partes de la transacción conocen la clave utilizada.

    Si únicamente me importara la eficiencia del método que uso para encriptar, debería optar por un algoritmo de cifrado asimétrico.

    Con ambos tipos de criptosistemas necesito contar con un mecanismo seguro para transmitir la clave.

Aplicaciones de criptografía

Herramientas necesarias: Iceweasel, Icedove, GnuPG, Enigmail y Steghide

Es importante que verifique el dia y la hora de su PC. Proceda a ajustar el mismo en caso de ser necesario, puesto que sino no será acertada la información sobre fecha y hora de generación de claves PGP y demás.

3. Configure el cliente de correo Icedove para acceder a su correo personal.

Primera parte: PKI

4. Diríjase al Sitio https://syper.linti.unlp.edu.ar/ y logre entrar sin que el navegador le advierta que el sitio no es seguro o confiable. Tenga en cuenta que para lograr esto, deberá realizar las siguientes tareas:
    a. **Instale el certificado de dicha Autoridad de Certificación** en su navegador, realizando los siguientes pasos. (A través de la opción CAs Info → Get CA Certificate y eligiendo la primer opción de la lista "CA-certificate in format CRT")
        i. Establezca que se confiará en esa Autoridad para verificar otros sitios y para certificar otros usuarios de correo.
        ii. Antes de instalarlo efectivamente, vea el certificado de la Autoridad de Certificación y mencione el algoritmo de firma que utiliza y el período de validez del mismo.

    b. **Verifique** que el certificado de la CA fue instalado correctamente en su navegador.

    c. **Solicite un certificado** de correo electrónico para ud. Para ello ingrese sus datos y siga las instrucciones que se le indiquen en el Sitio. (A través de la opción "Request a Certificate").
    Nota: la dirección de email que especifique en el certificado, deberá ser la que esté configurada en el cliente de correo Icedove.

    d. Una vez que el Operador de la RA y el Operador de la CA hayan emitido los certificados, proceda a obtener el mismo (A través de la opción "Get Requested Certificate") y luego verifique que dicho certificado haya sido correctamente instalado en su Navegador.

    e. Busque el certificado de otro usuario y procesa a instalar el mismo en su navegador. Verifique que el mismo haya sido correctamente.

5. Exporte su certificado personal y el certificado de la autoridad de certificación en una carpeta de su PC y luego impórtelos en su cliente de mail Icedove, a través de las siguientes opciones:
    a. El certificado de la CA impórtelo desde la opción: Editar → Preferencias → Avanzadas → Certificados → Ver Certificados → Autoridades
    b. Su certificado impórtelo desde la opción: Editar → Preferencias → Avanzadas → Certificados → Ver Certificados → Sus certificados

6. Envíe un mail firmado a un compañero y analice cómo llega el mismo a la cuenta personal de dicho usuario. Nota: deberá usar la opción Firmar Mensaje (S/MIME)). ¿Qué información es necesaria en el destino para verificar la firma?

7. Envíe un mail encriptado a un compañero y analice cómo llega el mismo a la cuenta personal de dicho usuario. Nota: deberá usar la opción Cifrar Mensaje (S/MIME)). ¿Qué información es necesaria en el destino para abrir el correo?

8. Envíe un mail encriptado y firmado a un compañero. ¿Qué información es necesaria en el destino para abrir el correo y verificar la firma?

9. Evalúe las siguientes situaciones en el marco de una infraestructura de PKI:
    a. Su clave privada fue comprometida
        i. ¿Qué consecuencias sufro respecto de la información firmada con la clave privada asociada a mi certificado?

ii. ¿Qué consecuencias sufro respecto de la información encriptada para que solo usted pueda ver?
iii. ¿Qué acciones se pueden llevar a cabo? ¿cómo?

b. Su clave privada fue comprometida y además usted perdió acceso a la misma, puesto que la misma fue borrada de su sistema.
i. ¿Qué consecuencias sufro respecto de la información firmada con la clave privada asociada a mi certificado?
ii. ¿Qué consecuencias sufro respecto de la información encriptada para que solo usted pueda ver?
iii. ¿Qué acciones se pueden llevar a cabo? ¿cómo?

Segunda parte: PGP

Creando anillos de claves y cifrando/firmando correo electrónico:

10. Cree su par de claves
    a. Ingrese al cliente de mail Icedove, elija la opción "OpenPGP" → "Administración de Claves".

    b. Dentro del administrador de claves elija "Generar"→ "Nuevo Par de Claves"

    c. Seleccione la cuenta para la cual creará el par de claves PGP.

    d. Ingrese la "frase clave" con la cual se protegerá su clave privada. Luego de este paso el asistente generará las claves.

    e. Al ser interrogado respecto a generar el certificado de revocación de su clave, responda que si y guarde el archivo generado en un lugar seguro. (A los fines prácticos de realizar estos ejercicios, guardelo en el Desktop de su PC)

11. Dentro del administrador de claves, publique su clave en el Servidor de claves
    a. Utilice la opción "Servidor de Clave" → "Subir Claves Públicas"

    b. Compruebelo utilizando la opción Servidor de claves → buscar claves

    [En lugar de exportarla a un servidor podría ser exportada a un archivo, utilizando la opción "Archivo → Exportar claves a un fichero" (seleccionando que se exporte con o sin la clave privada)

12. Dentro del administrador de claves, incorpore la clave de su compañero a su anillo de claves, para ello:
    a. "Servidor de Claves" → "Buscar Claves" e ingresando la dirección de mail que corresponda a su compañero.

    b. Impórtela a su anillo de claves.

    c. Firme la clave de su compañero, a través de la opción "Firmar".

    Nota: En lugar de buscarla en el servidor la pueden importar de un archivo: "Archivo → Importar clave desde un fichero", y luego eligiendo el archivo correspondiente a la clave, la cual se la puede enviar un compañero.

13. Utilizando el cliente de mail Icedove intercambie mails firmados y encriptados con su compañero usando las opciones:
    - "OpenPGP" → "Firmar Mensaje" y
    - "OpenPGP" → "Cifrar Mensaje"

14. Trabajando con relaciones de confianza. Para ello se plantearán distintos casos a probar, teniendo en cuenta que:
    a. En el Servidor de claves se encuentran publicadas las claves de:
        i. paula.venosa@gmail.com
        ii. pvenosa@mail.linti.unlp.edu.ar, la cual está firmada por paula.venosa@gmail.com (indicando que este último usuario confía en que la clave pública de pvenosa@mail.linti.unlp.edu.ar es de quien dice ser)

    b. Dentro del administrador de claves busque e incorpore ambas claves.
        i. Ahora confíe en el usuario paula.venosa@gmail.com, dándole el mayor nivel de confianza posible.

    c. ¿Qué ocurre con respecto a la validez de la otra cuenta pvenosa@mail.linti.unlp.edu.ar? Para comprenderlo seleccione dicha clave e elija la opción "Ver Firmar"

15. Analice distintos resultados que se obtienen al cambiar la confianza que ha establecido respecto a la clave de algún compañero (haga las pruebas usando la opción "Establecer confianza del propietario").

16. ¿Qué información es necesaria para que quien recibe un mail firmado, pueda verificar la firma del mismo?

17. ¿Qué información necesito para poder enviar un mail encriptado?

18. ¿Que información es necesaria para que quien recibe un mail encriptado, pueda abrirlo?

19. Para que mi cliente de correo tenga confianza en una clave determinada, ¿Qué circunstancias pueden haberse dado? Enumere las distintas posibilidades.

20. Evalúe las siguientes situaciones:
    a. Alguien le ha robado la clave privada. Usted no había generado un certificado de revocación de su clave. Sin embargo, usted dispone de la clave actualmente, del mismo modo que la persona que se la robó:
        i. ¿Qué consecuencias sufro respecto de la información firmada con esa clave?
        ii. ¿Qué consecuencias sufro respecto de la información encriptada para que solo esa clave pueda recibir?
        iii. ¿Qué acciones se pueden llevar a cabo? ¿cómo?

    b. Alguien le ha robado la clave privada y además borró la misma de su almacén de claves. Usted no había generado una revocación de su clave.
        i. ¿Qué consecuencias sufro respecto de la información firmada con esa clave?

ii. ¿Qué consecuencias sufro respecto de la información encriptada para que solo esa clave pueda recibir?

iii. ¿Qué acciones se pueden llevar a cabo? ¿cómo?

Tercera parte: Criptografía Simétrica y esteganografía

Cifrando archivos con gpg en forma simétrica:

21. Cree un archivo y encríptelo:
    a. Genere un archivo cualquiera, por ejemplo con

    ```
    echo "Mensaje secreto para Alice" > archivo.txt
    ```

    b. Para encriptar el archivo, desde una terminal y parado en el mismo directorio, ejecutar

    ```
    gpg -c archivo.txt
    ```

    c. Intruduzca una frase para cifrar el archivo y la confirmación de la clave.
    d. Ahora archivo.txt esta en texto claro y archivo.txt.gpg esta cifrado.
    e. Haga las pruebas que considere necesarias. Lea las páginas del manual para obtener información acerca del algoritmo de cifrado.
    f. Intercambie archivos cifrados con sus compañeros.
    g. Para desencriptar pruebe

    ```
    gpg -d archivo.txt.gpg
    ```

Esteganografía

22. Oculte un archivo de texto en una imágen a través del siguiente comando: steghide embed –cf [nombre de la imagen a usar] –ef [nombre del archivo a ocultar]
23. Visualice la imagen que contiene el archivo oculto en un navegador
24. Extracte el archivo oculto en la imagen a través del siguiente comando: steghide extract –sf [imagen a usar]