Trabajo Práctico 3
Administración de Redes y Seguridad
Profesor: Lic. Bruno Damián Zappellini

2018 - UNPSJB

Índice general

Guía de Trabajos Prácticos 3

Criptografía y sus aplicaciones

3.1. 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:

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

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

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

3.2. Aplicaciones de criptografía

Herramientas necesarias: Un Navegador (Chrome, firefox, Iceweasel, etc.), Cliente de correo (Thanderbird, Icedove, etc.), GnuPG, Enigmail y Steghide

Nota: 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.

3.2.1. Primera parte: PKI

3. ¿Que información es necesaria para que quien recibe un mail firmado, pueda verificar la firma del mismo?
4. ¿Que información necesito para poder enviar un mail encriptado?
5. ¿Que información es necesaria para que quien recibe un mail encriptado, pueda abrirlo?
6. Realice la siguiente práctica, efectuando los pasos en el orden que se proponen.
   - *a*) Configure el cliente de correo Thunderbird para acceder a su correo personal. Estos programas permite envio/recepción de mails cifrados/firmados.
     Nota: Verificar que esté seteada la opción de mantener correo en el servidor
   - *b*) Diríjase al Sitio `https://www.cacert.org/` e instale el certificado de la Autoridad de certificación en su navegador.
     1) A través de la opción Certificado raíz, descargar el Certificado Raíz (Formato PEM) su disco local.
     2) Antes de instalarlo, vea el certificado de la Autoridad de Certificación y mencione:
     3) El algoritmo de firma que utiliza.
     4) La cantidad de bits de cifrado.
     5) El período de validez del mismo.
     6) Otras observaciones que le parezcan importantes.
     7) Instale el certificado y establezca que se confiará en esa Autoridad para verificar otros sitios y para certificar otros usuarios de correo.
     8) Verifique que el certificado de la CA fue instalado correctamente en su navegador.
   - *c*) Una vez instalado, debería entrar sin que el navegador le advierta que el sitio no es seguro o confiable en el sitio de la CA `https://www.cacert.org/`
   - *d*) Ingrese nuevamente al sitio mencionado (con el certificado instalado, según el paso anterior), 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: Darse de alta, luego “Iniciar sesión con contraseña” y usar la opción “Certificado de cliente”.
     La dirección de email que especifique en el certificado, deberá ser la que esté configurada en el cliente de correo.
7. Instale y verifique que su certificado haya sido correctamente instalado en su Navegador.
   - *a*) Enviar el certificado al foro de consultas del aula así todos tienen los certificados de sus compañeros para hacer esta practica (o enviarlo por email al profesor asi los publica)

b) procesa a instalar el mismo en su navegador. Verifique que el mismo haya sido instalado correctamente.

c) 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, en el caso de Thunderbird a través de las siguientes opciones:

1) El certificado de la CA impórtelo desde la opción: Editar → Preferencias → Avanzadas → Certificados → Ver Certificados → Autoridades → Importar...
2) Su certificado impórtelo desde la opción: Editar → Preferencias → Avanzadas → Certificados → Ver Certificados → Sus certificados → Importar...

8. 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?

9. 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?
Nota: puede ser necesario que tenga que instalar el certificado de la persona a la que le desea enviar mails cifrado

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

11. Evalúe las siguientes situaciones en el marco de una infraestructura de PKI:

a) Su clave privada fue robada

b) Su clave privada fue robada y además usted perdió acceso a la misma, puesto que la misma fue borrada de su sistema.

En cada una de las situaciones presentadas, evalúe:

1) ¿Qué acciones se pueden llevar a cabo en cada una de las situaciones? ¿De qué manera se procede en cada caso?
2) ¿Qué consecuencias existen para con la información encriptada que solo usted debería poder ver?
   - ¿Hay alguna contramedida para esto?
3) ¿Qué consecuencias existen para con la información firmada con la clave privada asociada a su certificado?
   - ¿Hay alguna contramedida para esto?

3.2.2. Segunda parte: PGP

Creando anillos de claves y cifrando/firmando correo electrónico:

12. Cree su par de claves PGP, si usan Thinderbir, instalen el complemento Enigmail.

13. Dentro del administrador de claves, publique su clave en el Servidor de claves

a) Utilice la opción “Servidor de Clave” → “Subir Claves Públicas”

b) Compruébelo utilizando la opción Servidor de claves → buscar claves

14. 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) Importe la misma a su anillo de claves.

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

15. Utilizando el cliente de mail intercambie mails firmados y encriptados con su compañero usando las opciones:

    - "OpenPGP" → "Firmar Mensaje" y
    - "OpenPGP" → "Cifrar Mensaje"

16. 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:

        1) bruno.zappellini@gmail.com
        2) bzappellini@juschubut.gov.ar, la cual está firmada por bruno.zappellini@gmail.com (indicando que este último usuario confía en que la clave pública de bzappellini@juschubut.gov.ar es de quien dice ser)

    b) Dentro del administrador de claves busque e incorpore ambas claves.

        - Ahora confíe en el usuario bruno.zappellini@gmail.com, dándole el mayor nivel de confianza posible.

    c) ¿Qué ocurre con respecto a la validez de la otra cuenta bzappellini@juschubut.gov.ar? Para comprenderlo seleccione dicha clave e elija la opción "Ver Firmas"

17. 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").

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

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

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

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

22. Evalúe las siguientes situaciones:

    a) Alguien le ha robado la clave privada. Usted no había generado un certificado de revocación para su clave. Sin embargo, usted dispone de la clave privada actualmente, del mismo modo que la persona que se la robó

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.
En cada una de las situaciones presentadas, evalúe:

1) ¿Qué consecuencias sufro respecto de la información que se firma con esa clave?
2) ¿Qué consecuencias sufro respecto de la información encriptada para que solo esa clave pueda abrir?
3) ¿Qué acciones se pueden llevar a cabo en cada caso? y ¿cómo debo proceder?

3.2.3. Tercera parte: Criptografía Simétrica y esteganografía

Cifrando archivos con gpg(GnuPG) en forma simétrica:

23. Cree un archivo y encríptelo:

a) Genere un archivo cualquiera, por ejemplo con:
`echo ''Mensaje secreto para Alberto'' >archivo.txt`

b) Para encriptar el archivo, desde una terminal y parado en el mismo directorio, ejecutar:
`gpg -c archivo.txt`

c) Introduzca una clave 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

24. Oculte un archivo de texto en una imagen a través del siguiente comando:
`steghide embed -cf[nombre_imagen ]-ef [nombre_archivo_a_ocultar ]`

25. Visualice la imagen que contiene el archivo oculto

26. Extraiga el archivo oculto de la imagen a través del siguiente comando:
`steghide extract -sf [imagen_con_steganografia ]`