Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Estado de México
Práctica de uso de PGP

Objetivo:

Familiarizar al estudiante con las principales funciones del programa PGP versión 8.1

Metodología

En el escritorio cree una carpeta, cuyo nombre este formado por su apellido y la primera letra de su nombre. Por ejemplo, en el caso de Antonio Becerra, sería abecerra. En ese archivo colocará todos los archivos, llaves y demás información que use. Al final tendrá que borrar esta carpeta y todo su contenido.

Llevar a cabo cada una de las siguientes acciones, es importante que respete el orden.

1. Escriba las direcciones electrónicas de dos de sus compañeros:
   Nombre:_____
   Dirección electrónica: _____
   Nombre: _____
   Dirección electrónica: _____

2. Cree sus llaves, siguiendo las recomendaciones del manual de PGP y/o las vistas en clase. Por favor **NO olvide la frase secreta de su llave**.
   - opción *New key* del menú *Keys* del cuadro de dialogo PGPKeys
3. Cree un archivo que contenga su llave pública, ponga su nombre y apellido al nombre de dicho archivo.
   - opción *Export* del menú de *Keys*
4. Envíe su llave pública a dos de sus compañeros. (si no cuenta con correo electrónico, se sugiere "depositar" la llave pública de su compañero en el directorio hogar de este vía FTP o a través de un dispositivo móvil de almacenamiento)
   - envíe una copia de su llave al profesor del curso (rogomez@itesm.mx), el correo debe contar con el subject: 01.LLAVE PUBLICA XXX YYY CURSO SEG INFORMATICA, donde XXX YYY es su primer nombre y apellido respectivamente.
5. En algunas ocasiones la frase asociada a su llave secreta permanece en cache. Con el objetivo de que todo el mundo este en las misma condiciones desactive esta opción
   - opción *Options* del menú *Edit*
   - en el recuadro *Single Sign-On* seleccione la opción *Do not cache passphrase*
6. Añada a su llavero de llaves públicas, las llaves de dos sus compañeros.
   - opción *Import* del menú de *Keys*
7. Elija la llave de uno de sus compañeros y verifique que la "huella" (fingerprint) de las llaves de sus compañeros sea la correcta.
   - opción *Properties* del menú *Keys*
8. Firme las llaves de sus compañeros y aumente el nivel de confianza de la llave (trust) uno a mediano y el otro a alto.
   - para firmar: opción *Sign* del menú *Keys* (verifique color del circulo del campo *Validity*, antes y después de firmar la llave)
   - para subir el nivel: mover la barra de *Untrusted* a *Trusted* de las propiedades de la llave
9. Tome un texto de internet y guárdelo en un archivo con su nombre y la primera letra de su apellido.

10. Cifre el archivo del paso anterior con la respectiva llave pública de sus compañeros y la del profesor[1], una vez encriptado envíelo a sus compañeros de curso y al profesor (igual que en el paso 3).
    - opción encripción de *PGPTools* o la opción *Encrypt* del menú *PGP* que aparece al presionar el botón derecho del ratón sobre el archivo
    - recuerde que para encriptar un archivo con la llave pública de alguien, esta debe estar dada de alta en su llavero.
    - al encriptar se desplegará un cuadro de dialogo dividido en dos partes, en la parte alta se despliegan los nombres de los dueños de las llaves públicas de su llavero; debe elegir los destinatarios y "depositarlos" en la parte baja del cuadro de dialogo.
    - Subject correo del profesor: 02.CIFRADO ARCHIVO
11. Con notepad (o wordpad si el archivo es muy grande) analice el contenido del archivo encriptado que le enviaron. ¿Puede entender algo?
12. Decripte el archivo enviado por su compañeros y verifique que es el que le enviaron.
    - opción decripción y verificación firma de *PGPTools* u opción *Decrypt/Verify* del menú *PGP* que aparece al presionar el botón derecho del ratón cuando el cursor se encuentra sobre el archivo
13. Modifique la contraseña de su clave privada.
    - opción *passphrase* de las propiedades de las llave
14. Elija a uno de sus compañeros y bórrelo de su llavero público.
    - opción *Delete* del menú *Edit*
15. Vaya al repositorio de llaves de Europa y traiga la llave de alguien llamado Pierre y delo de alta en su llavero.
    - opción *Search* del menú Server, elija el servidor *europe.keys.pgp.com*
    - *NOTA;* si después de quince segundos no obtiene respuesta del servidor, intente con otro servidor por el mismo tiempo; si tampoco le responde pase al siguiente punto. En algunas ocasiones los servidores se encuentran dados de baja.
16. Elija una imagen en internet de tipo jpg (no muy grande) bájela e incorpórela a su juego de llaves.
    - opción *Add* del menú *Keys*
17. Borre las llaves de sus compañeros de su llavero, intercambie su nueva llave (la que incluye la figura) con sus compañeros de nuevo y verifique la fotografía de las llaves que le lleguen
    - NOTA IMPORTANTE: al exportar de nuevo su llave asegúrese que la opción de *Include 6.0 Extensions* se encuentra activa.
    - NOTA 2: si aparece un signo de interrogación sobre la imagen de la llave de su compañero, debe firmar la llave para que este signo desaparezca
    - Envíe la llave con su foto a la cuenta del profesor con el subject 03.LLAVE CON FOTO
18. Escriba un correo electrónico y cífrelo con las llaves públicas de sus compañeros. El cuerpo del correo debe ser el mensaje encriptado. Envíe el correo a sus compañeros.
    - opción *Clipborad* del menú del icono de *PGP* en la barra de tareas (icono en forma de candado que aparece en la parte baja derecha de su pantalla)
    - también puede usar la opción *Current Window* del mismo icono
19. Decripte los correos que le lleguen.
20. Firme, solamente firme, el archivo que encriptó anteriormente (puntos 7,8) y envíeselo a sus compañeros.
    - opción firma de *PGPTools* o la opción *sign* del menú *PGP* que aparece al presionar el botón derecho del ratón cuando el cursor se encuentra sobre el archivo.
21. Verifique la firma de los archivos que le lleguen
    - opción *Decrypt & Verify* del menú *PGP* que aparece al presionar el botón derecho del ratón cuando el cursor se encuentra sobre el archivo
22. Escriba un correo electrónico y fírmelo, solamente fírmelo. El cuerpo del correo debe ser su mensaje firmado.
    - Envíe el correo firmado a sus compañeros
    - Envíe una copia al profesor con el subject 04.PRUEBA DE FIRMA CORREO

[1] La llave del profesor se encuentra en la página *homepage.cem.itesm.mx/rogomez*

23. Verifique la firma de los correos que le lleguen.
    - Seleccione el texto y cópielo al portapapeles (clipboard).
    - A través de opción *Clipborad* del menú del icono de *PGP* en la barra de tareas (icono en forma de candado que aparece en la parte baja derecha de su pantalla),
24. Tome el mismo cuerpo de correo del punto 18 y modifique una letra del mensaje y vuelva a enviarlo.
25. Vuelva a verificar la firma de los correos que le lleguen.
26. Envíe un correo al profesor indicando lo observado en los tres puntos anteriores (23-25). El subject del correo debe ser: 05.FIRMA COMPAÑEROS.
27. De la sección material de apoyo de la página homepage.cem.itesm.mx/rogomez/cripto.html baje el archivo TextoFirmado.txt
    28. Verifique que la firma es correcta, es necesario utilizar la llave pública del profesor para verificar lo anterior. Tome un screenshot y almacenelo en un archivo de nombre toto.jpg, a notar que el archivo es de tipo jpg.
    29. Cambie la primera palabra, Esto, por mayúsculas, ESTO y vuelva a verificar la firma. Tome un screenshot y almacénelo en un archivo de nombre cachafas.jpg, a notar que el archivo es de tipo jpg.
    30. Envíe ambos archivos en un correo al profesor con el subject: 06.VERIFICACION FIRMA
31. En un correo escriba su nombre completo, su(s) direccion(es) de correo electrónico, el semestre y la carrera que estudia. Cifre el archivo con la llave que se encuentra en la página: http://homepage.cem.itesm.mx/rogomez
    - Firme el correo y envíelo a la dirección rogomez@itesm.mx, el subject del correo debe ser 07.DATOS DE XXX YYY donde XXX YYY es su primer nombre y primer apellido (en mayúsculas).
32. Vuelva a crear otro archivo y explique las diferencias entre las cuatro opciones de encripción (parte baja izquierda del cuadro de encripción)
    - Text Output
    - Wipe Original
    - Conventional Encryption
    - Self Decrypting Archive
33. Envíe una de las diferencias al profesor en un correo con el subject 08.TIPOS CIFRADO PGP
34. Firme el archivo que uso en el punto del punto anterior y diga las diferencias entre:
    - Detached Signature
    - Text Output
    - La combinación de las dos
35. Envíe una de las diferencias al profesor en un correo con el subject 09.TIPOS FIRMA PGP
36. Verifique las opciones del punto anterior pero con un correo electrónico que tenga como cuerpo el mensaje firmado.
37. Acceda a la opción *Options* del menú *Edit*. Una ahí vaya a la sección de *File Wiping* y:
    - Cambie opción *Number of passes* a 1.
    - Borre uno de los archives que creó, y tome el tiempo de borrado.
    - Una vez borrado recupérelo de la carpeta de Basura
    - Vuelva al archivo y seleccione la opción *Wipe* del menú *PGP* que aparece al presionar el botón derecho del ratón cuando el cursor se encuentra sobre el archivo, y tome el tiempo de borrado.
    - Intente recuperar el archivo de la carpeta de Basura.
    - Modifique la opción de *Number de passes* a 30.
    - Elimine otro archivo con la opción de *Wipe* del menú PGP y tome el tiempo de borrado.
    - Envíe sus conclusions de lo anterior a su professor con el subject: 10.EJERCICIO WIPE
38. Borre la carpeta que creó al principio de la práctica.
    - Use la opción de borrado seguro de PGP