EJERCICIO EXPLORACIÓN CRIPTO 21-Nov-2015

Prof. Jorge Gana L.

Objetivo: Uso de GPG (OpenPGP)

Descripción: Instale una versión de GPG para su propio uso. Trabajaremos con Key Rings (anillos de claves) en forma local, salvo para la pregunta a).

a) Encuentre (al menos) una clave pública del Presidente Barack Obama de los EE.UU. en un servidor de claves GPG y también una clave pública a mi nombre y otra de Kevin Bacon. Entregará las claves públicas encontradas (*fingerprints* es suficiente) como parte de este ejercicio. Argumente si las claves encontradas son de quien corresponde. Basándose en sus experiencias, explique un aspecto positivo y otro negativo de los servidores de claves GPG. (máximo dos párrafos)

b) Genere un par público/privado de clave RSA de 2048 bits (default). **Use su nombre y dirección emai**l para etiquetarla. Por ejemplo en mi caso:

Jorge Gana jcganal51@gmail.com

Elija un buen “passphrase” y firme su propia Clave.

Extraiga su Clave pública y envíela a mi correo: jcganal51@gmail.com

Posteriormente yo enviaré mi clave pública a su email para que la agreguen a su anillo de claves. Seguidamente les enviaré un correo con mi “fingerprint” o huella digital para que la validen.

c) use gpg para verificar la firma de esta tarea. Copy/Paste la

salida de su sesión de verificación en un archivo. También incluya el

"fingerprint" de su clave en el archivo. Agregue la respuesta que tenga a la pregunta a)

Firme el archivo y encríptelo con mi clave pública en **modo ascii** y

envíe el resultado a mi correo: jcganal51@gmail.com

d) después de recibir su email, le enviaré un mensaje encriptado con su llave pública. Use su clave pgp para desencriptar el mensaje, y envíeme el resultado a mi correo electrónico.-

NOTA: SEGUIR LAS INSTRUCCIONES AL PIE DE LA LETRA PARA NO TENER QUE REPETIR LOS PASOS DEL EJERCICIO