CURSO EXPLORACIÓN - 09/06/2015
Trabajo final Criptografía
Profesor: Jorge Gana L.

Objetivo: Uso de GPG4 (PGP)

Descripción: Instale una versión de GPG4 (aka PGP) para su propio uso. Trabajaremos con Key Rings (anillos de claves) en forma local.

a) **Reflexiones sobre la Confianza**. GPG4 se basa en un modelo de "red de confianza", permite a los usuarios "firmar" las claves públicas entre unos y otros ". Supongamos que Alicia firma la clave pública de Bob; ¿qué está Alicia, en efecto, declarando cuando ella hace esto?
¿Por qué es útil que las personas firmen sus claves entre unos y otros? ¿Qué precauciones se deben tomar antes de firmar la clave de otra persona, y porqué son estas medidas apropiadas?

b) Encuentre (al menos) una clave pública de Kevin Bacon, otra bajo president@whitehouse.gov en un servidor de claves OpenPGP y también una clave pública a mi nombre. Posteriormente me enviarán las claves públicas encontradas (*fingerprints* es suficiente). Basado en sus hallazgos, explique un aspecto positivo y otro negativo de los servidores de claves GPG4. (máximo dos párrafos).

c) Genere un par público/privado de clave RSA de 2048 bits. **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 agregue a su anillo de claves. Seguidamente le enviaré un correo con mi "fingerprint" o huella digital para que la valide.

d) use GPG4 para verificar la firma de esta tarea. Copy/Paste la salida de la sesión de verificación en un archivo. También incluir el "fingerprint" de su clave en el archivo. Agregue las respuestas que tenga a las preguntas a) y b)
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, yo le enviaré un mensaje encriptado con su clave pública. Use su clave pgp para decodificar el mensaje.

ASEGURARSE DE HACERLO BIEN LA PRIMERA VEZ.