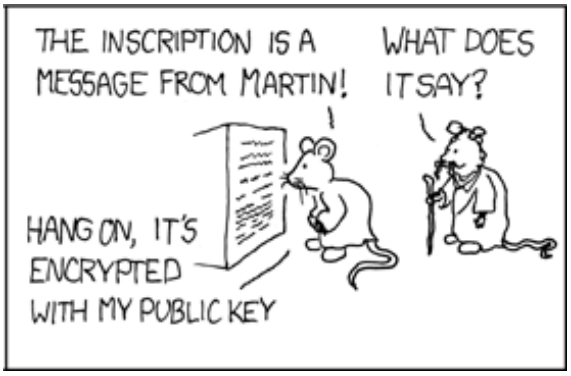
Taller 2: Criptografía Asimétrica con GPG

Para el desarrollo de este taller debe crear un informe en formato `.doc` o formato `.odt` en el cual debe colocar las respuestas a todas las preguntas **resaltadas en negritas** que encuentre en las siguientes Secciones. Al finalizar el taller envíe su respectivo informe al profesor. El informe debe incluir su nombre y número de cédula al principio.

1. Cifrado Asimétrico



1. Genere un par de claves pública y privada usando el comando "`gpg --full-generate-key`". Cuando el comando lo solicite coloque 4096 bits como el tamaño de clave y especifique una fecha de vencimiento de 1 año; use su nombre real y correo institucional de la Facultad de Ciencas como nombre y correo para la construcción de la identidad de clave. **Razone, ¿para que sirve el *passphrase* que solicita el comando?, ¿por que es necesario especificar una fecha de vencimiento?.**

2. Utilice el comando "`gpg --list-keys`" para visualizar las claves que tiene en su *keyring*. **Tome nota de cual es la identidad de la clave creada en el paso anterior**. Por defecto "`--list-keys`" muestra todas las claves en los *keyrings* público y privado. Para visualizar solo las claves públicas (el *keyring* público) use el comando "`gpg --list-public-keys`". El comando "`gpg --list-secret-keys`" muestra las claves privadas (el *keyring* privado).

3. Para cifrar archivos primero debe recibir la clave pública de algún compañero, a quien igualmente le debe haber compartido su propia clave pública. Para compartir las claves primero es necesario exportarlas. Exporte su clave pública con el comando "`gpg --export 'NOMBRE APELLIDO <CORREO>' > nombre.pub`", sustituyendo en el comando el bloque "`NOMBRE APELLIDO <CORREO>`" por la identidad de la clave que generó anteriormente y "`nombre.pub`" por un archivo que tenga su propio nombre con extensión `.pub`.

4. El archivo de clave generado es de formato binario. Para exportar la clave en un formato de texto utilice el comando "`gpg --enarmor < nombre.pub > nombre.pub.b64`", sustituyendo el nombre del archivo de clave por el que generó en el paso anterior. **Abra el archivo de clave en texto plano "`nombre.pub.b64`" y constate que es un archivo de texto. Investigue que es y para que sirve lo que se conoce como "armadura ASCII" en el contexto del protocolo OpenPGP.**. Para obtener una clave en formato binario dado un archivo de clave con armadura ASCII utilice el comando "`gpg --dearmor < nombre.pub.b64 > nombre.pub`".

5. Envíe su archivo de clave binario "`nombre.pub`" a algún compañero, quien debe enviarle su correspondiente archivo de clave pública. Luego importe la clave con el comando "`gpg --import compañero.pub`", utilizando el nombre correspondiente del archivo de clavé que recibió. **Examine el contenido de los *keyrings* para verificar que efectivamente se agregó la clave.**

6. Cifre un archivo cualquiera utilizando la clave pública de su compañero. Para esto use el comando "gpg -e -r 'IDENTIFICADOR DE CLAVE' archivo", sustituyendo el identificador de clave de su compañero y el archivo que quiera cifrar. **Indique que resultado produce este comando en el sistema de archivos de la computadora**. Envíe el archivo cifrado resultante a su compañero. Igualmente debe recibir de su compañero un archivo cifrado con la clave pública que usted le compartió.

7. Para descifrar el archivo que recibió de su compañero use el comando "gpg -d archivo.gpg > archivo". Si tiene una sola clave privada en su *keyring* entonces GPG utilizará esta por defecto. En caso de que tenga múltiples claves privadas puede especificar cual usar para descifrar con la opción "`-u 'ID DE CLAVE PRIVADA'`". **verifique que el archivo recibido se descifró correctamente.**

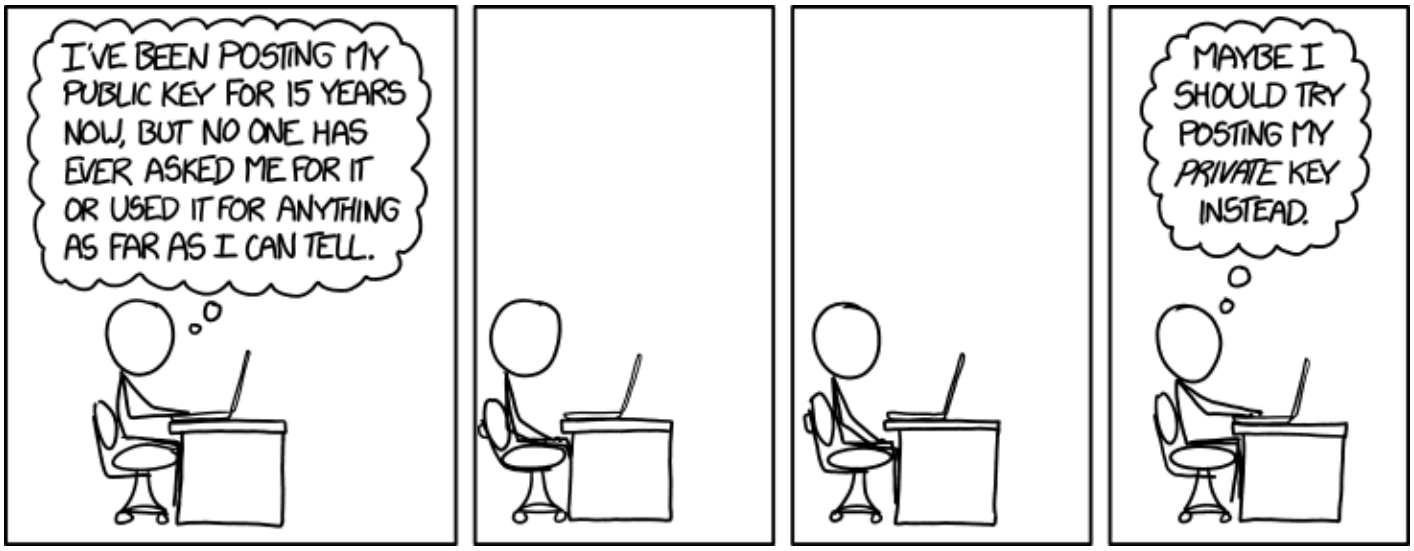
2. Firmas Digitales

1. Escoga un archivo para firmar con su clave privada, luego ejecute el comando "`gpg -u 'ID DE CLAVE PRIVADA'` –sign archivo". Esto produce como salida un archivo llamado "`archivo.gpg`", el cual contiene el archivo a firmar comprimido (más no cifrado) junto a una firma digital generada para dicho archivo. Envíe este archivo firmado a algún compañero con quien haya compartido su clave pública. Su compañero igualmente debe enviarle un archivo firmado de la misma manera. También se puede utilizar la opción "`--clearsign`" en lugar de "`--sign`" para obtener el archivo firmado sin comprimir.

2. Verifique el archivo enviado por su compañero con el comando "`gpg --verify archivo.gpg`". **Verifique que GPG indique que la firma del archivo es correcta**. Esta verificación se realiza de la misma manera independientemente de si el archivo fue firmado con "`--clearsign`" o "`--sign`".

3. También es posible obtener la firma separada del archivo a firmar usando la opción "–detach-sig". Ejecute el comando "`gpg --detach-sig -u 'ID DE CLAVE PRIVADA' archivo`". **Verifique que se creó un archivo llamado "`archivo.sign`" junto al archivo original. Luego ejecute el comando "`gpg --enarmor < archivo.sig`" y copie su salida en su informe.** Para verificar un archivo firmado de esta manera se debe colocar el archivo original junto al archivo de firma en el mismo directorio, y luego ejecutar el comando "`gpg --verify archivo.sig`".

3. Red de Confianza



1. Ejecute el comando "`gpg --list-sigs`" para listar las firmas de cada clave guardada en los *keyrings*. **Verifique cuales firmas tiene la clave pública de su compañero.**

2. Ejecute el comando "`gpg --sign-key 'ID DE CLAVE PÚBLICA'`" para firmar la clave de su compañero. **Luego ejecute el comando "`gpg --list-sigs`" nuevamente para verificar que efectivamente se ha firmado la clave pública.**

3. Ejecute el comando "`gpg --edit-key 'ID DE CLAVE PÚBLICA'`" usando la clave pública de su compañero para entrar a una sesión interactiva de GPG en la cual se pueden editar las propiedades de una clave. Dentro de la sesión interactiva ejecute el comando "`trust`" para editar el nivel de confianza que le tiene a la clave de su compañero. Puede utilizar cualquiera de los 5 niveles de confianza indicados por GPG. Para salir de la sesión interactiva use el comando "`quit`" o presione CTRL+D. **Luego ejecute el comando "`gpg --list-keys`" para verificar que se ha modificado el nivel de confianza de la clave.**

4. Post-Taller

Investigue las siguientes cuestiones y coloque sus respuestas en su informe.

1. Investigue que es y para que sirven lo que se conoce como servidores de distribución de claves OpenPGP.

2. Indique cuales comandos de GPG se utilizan para publicar claves públicas y firmas de claves para Red de Confianza en un servidor de claves.

3. ¿En que situaciones se podría necesitar revocar una clave?

4. Indique cual es el procedimiento para generar un certificado de revocación de clave con GPG y como publicarlo en un servidor de distribución de claves.