**Juan Carlos Navidad García**

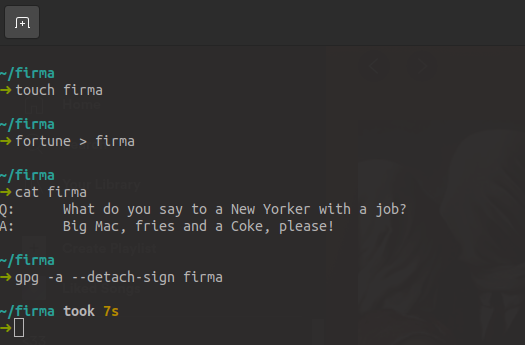
**Seguridad Informática**

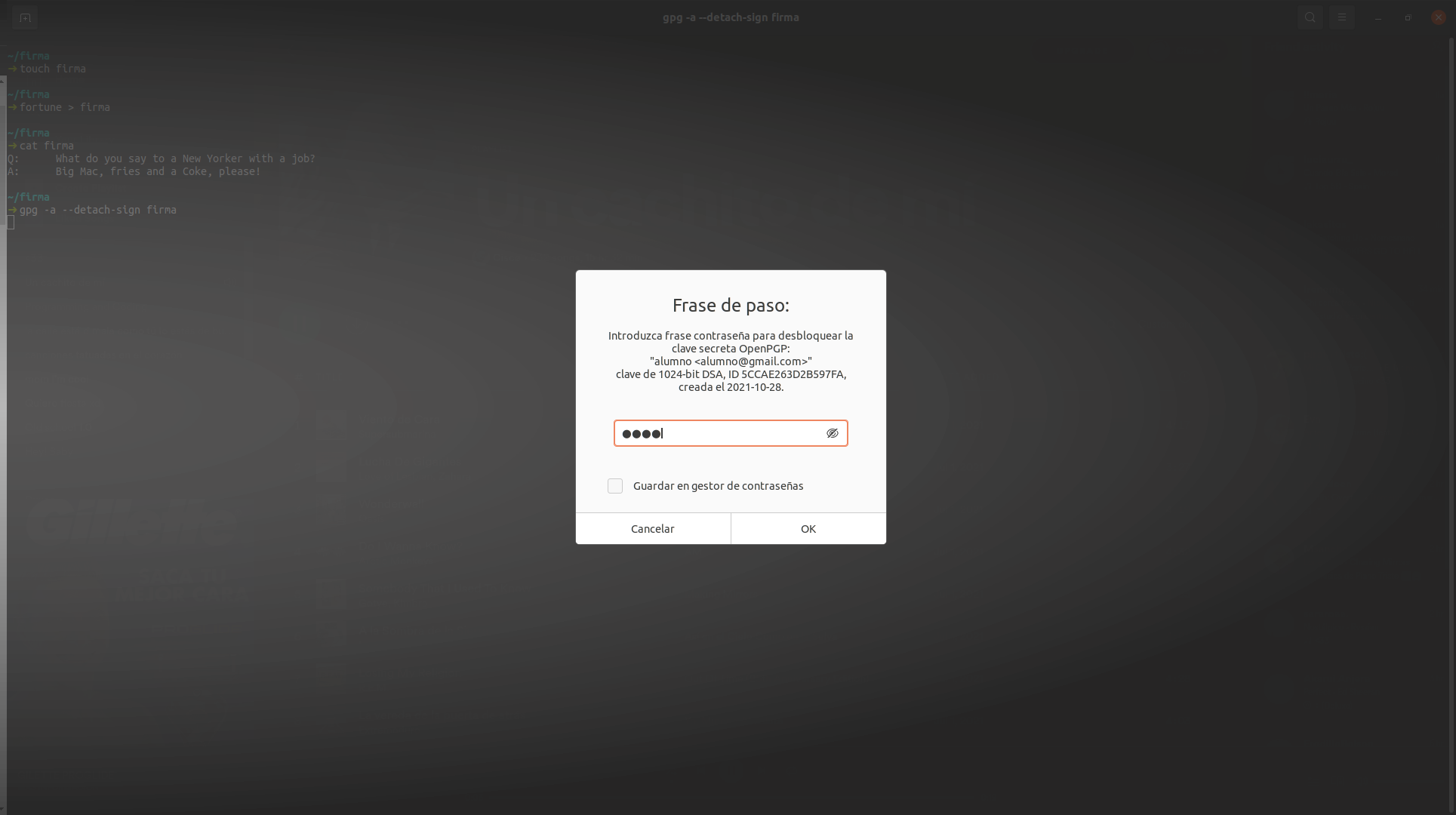
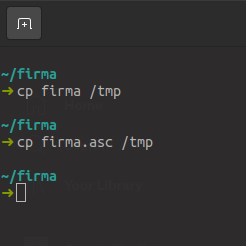
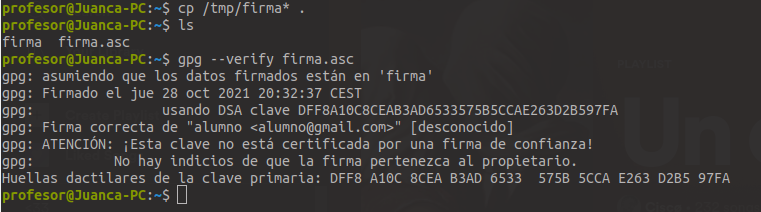
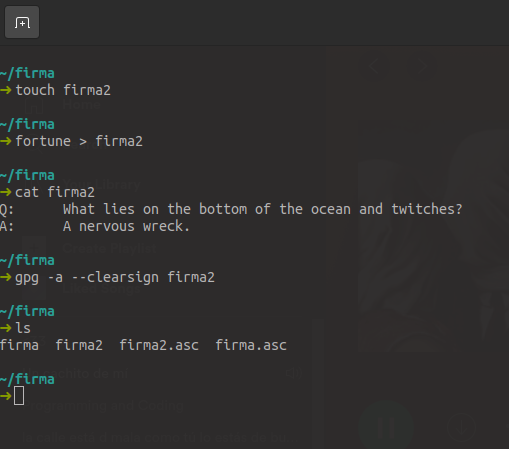
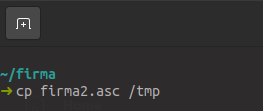


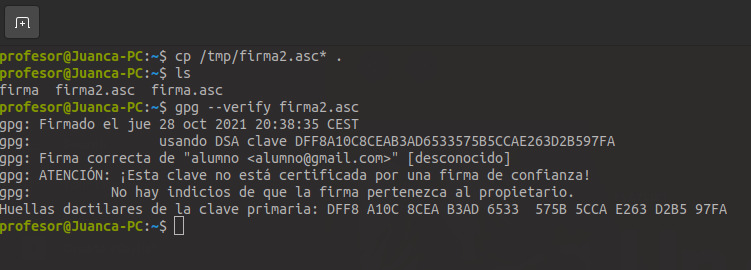
**FIRMA DIGITAL LINUX**

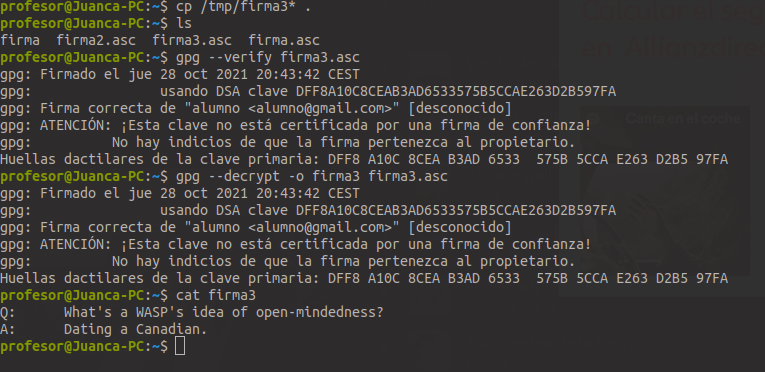
1. **Firma digital en Linux:**

* Recordemos que habíamos generado dos parejas de claves, una pareja **DSA** y una pareja **Elgamal**. En el cifrado del fichero habíamos utilizado la clave **Elgamal**.
* En la sesión de alumno creamos un fichero mensaje y lo firmamos con nuestra clave privada para que cualquiera pueda confirmar que es nuestro. Usaremos el parámetro **detach-sign**, que crea un fichero nuevo solo con la firma (el cifrado del resultado de aplicar el hash al fichero original). Utilizaremos también el parámetro a para observar ese fichero. Los comandos son:
  + ***alumno$ fortune > firma***
  + ***alumno$ gpg –a -–detach-sign firma***

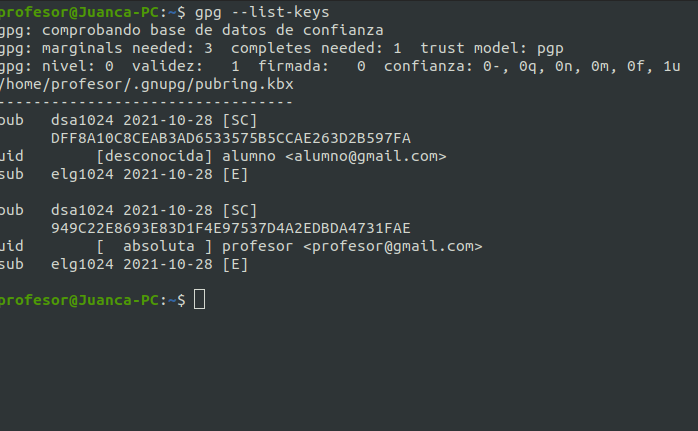


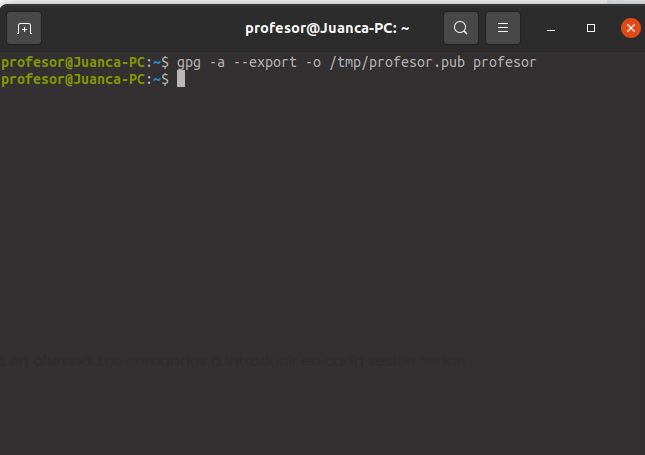
* Vemos que la herramienta nos pide la contraseña de nuestra clave secreta:
* Ahora realizamos el envío al usuario profesor (por ejemplo, podríamos estar entregando un trabajo). En este caso simplemente lo copiaremos en **/tmp**. Hay que copiar los dos ficheros: **firma**, que no lleva la firma, y **firma.asc**, que solo es una firma. Los comandos serían:
  + ***alumno$ cp firma /tmp***
  + ***alumno$ cp firma.asc /tmp***
* Iniciamos una sesión con el usuario **profesor**, copiamos los ficheros a nuestro directorio y comprobamos la firma. El parámetro es **verify** junto con el nombre del fichero que lleva la firma (en mi caso, **firma.asc**). Los comandos son:
  + ***profesor$ cp /tmp/firma\* .***
  + ***profesor$ gpg –-verify firma.asc***
* Para evitar enviar dos ficheros, podemos incluirlo todo en el mismo. Volvemos a la sesión del usuario **alumno** y ahora firmamos con el parámetro **clearsign**. El comando sería:
  + ***alumno$ gpg –a -–clearsign firma***
* De nuevo hay un fichero **firma2.asc**pero ahora contiene tanto la firma como el texto del mensaje
* Podemos copiarlo de nuevo a **/tmp** y tomarlo desde la sesión del **profesor**. El comando de verificación es el mismo que en el caso del fichero separado.

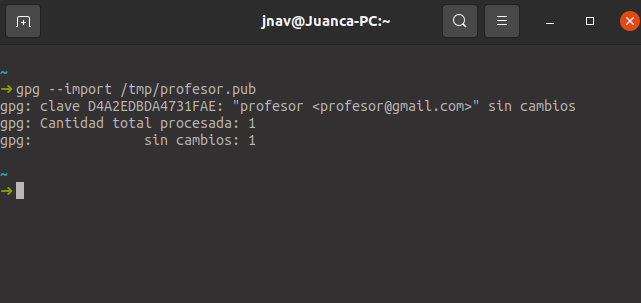


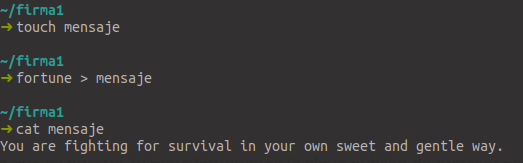
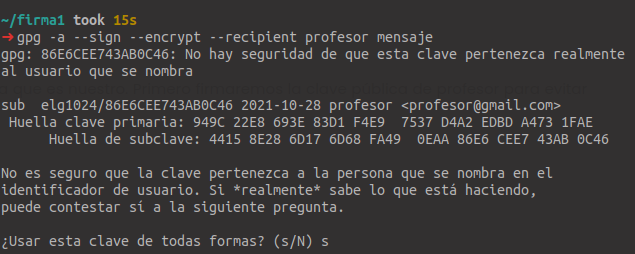
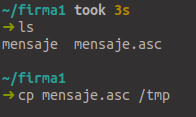
* De nuevo podemos llevarlo al directorio **/tmp**para que el usuario **profesor** haga una copia y lo verifique. Si además queremos extraer el fichero utilizaremos **decrypt**:
  + ***profesor$ cp /tmp/firma3.asc .***
  + ***profesor$ gpg –-verify firma3.asc***
  + ***profesor$ gpg –-decrypt –o firma3 firma3.asc***
* Aunque esta protección es bastante débil, porque cualquiera que tenga la clave pública de alumno tendrá acceso al contenido del fichero. Debemos utilizar el cifrado normal, lo que nos lleva a que el usuario profesor genere su par de claves (hasta ahora no ha sido necesario).
  + ***profesor$ gpg –-full-generate-key***



* Con **list-keys** podemos comprobar que tenemos dos claves: las nuestras y las de alumno.
  + ***profesor$ gpg –-list-keys***

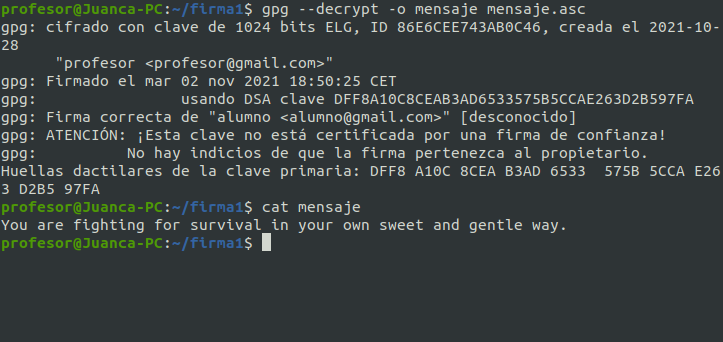
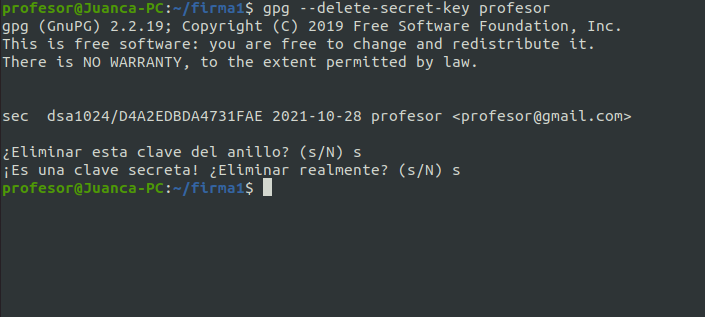
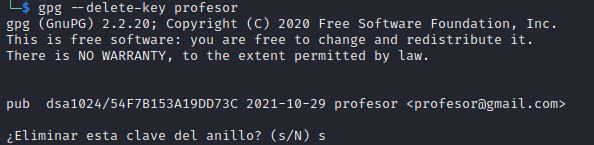
* Para que **alumno** nos pueda cifrar el fichero firmado, debemos seguir el procedimiento conocido: exportar la clave pública de **profesor** e importarla en **alumno**. Los comandos a introducir en cada sesión serían:
  + ***profesor$ gpg –a –-export -o /tmp/profesor.pub profesor***
  + ***alumno$ gpg –-import /tmp/profesor.pub***

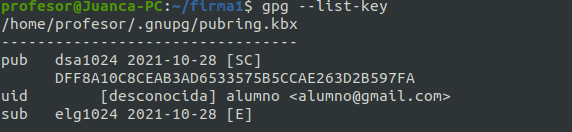


* En la sesión de **alumno** vamos a generar un nuevo fichero, lo cifraremos para que solo **profesor** pueda recuperarlo y lo firmaremos para que sepa que es nuestro.
  + ***alumno$ fortune > mensaje***
  + ***alumno$ gpg –a –-sign –-encrypt –-recipient profesor mensaje***
  + ***alumno$ cp mensaje.asc /tmp***

* El fichero **mensaje.asc**es ilegible y lleva dentro el contenido del fichero **mensaje**y la **firma**. Lo copiamos en **/tmp**para recuperarlo desde la sesión de **profesor**, descifrarlo, verificar la firma y recuperar el fichero **mensaje**. El parámetro será **decrypt**, porque también nos ofrece la confirmación de la firma. Nos pedirá la contraseña que protege la clave privada de **profesor**, necesaria para descifrar el fichero. Los comandos serían:
  + ***profesor$ cp /tmp/mensaje.asc .***



* + ***profesor$ gpg -–decrypt –o mensaje mensaje.asc***
  + ***profesor$ cat mensaje***
* Si no tenemos la clave privada de **profesor**, no podemos descifrar ni, por tanto, recuperar el fichero ni comprobar la firma. Por ejemplo, podemos borrar nuestras propias claves con los parámetros **delete-secretkey**y**delete-key**. Después ya no funcionará ni descifrar ni verificar. El mensaje de error indicará que el fichero fue cifrado con una clave que ya no tenemos. Los comandos son:
  + ***profesor$ gpg -–delete-secret-key profesor***
  + ***profesor$ gpg –-delete-key profesor***
  + ***profesor$ gpg –-list-key***



* + ***profesor$ gpg –-decrypt mensaje.asc***
  + ***profesor$ gpg –-verify mensaje.asc***

