

Ejercicio 5: Firma digital de un documento

1. Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.
2. Verifica que la firma recibida del documento es correcta.
3. Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.

```
http@http-VirtualBox:~/Escritorio$ gpg -sb -a FirmaDigital
Necesita una contraseña para desbloquear la clave secreta
del usuario: "AlejandroAnton <alejandro@gmail.com>"
clave RSA de 2048 bits, ID B133FF81, creada el 2017-03-13

http@http-VirtualBox:~/Escritorio$ gpg FirmaDigital.asc
gpg: asumiendo que hay datos firmados en «FirmaDigital»
gpg: Firmado el lun 13 mar 2017 22:30:36 CET usando clave RSA ID B133FF81
gpg: Firma correcta de «AlejandroAnton <alejandro@gmail.com>»
http@http-VirtualBox:~/Escritorio$ gpg --verify FirmaDigital.asc
gpg: asumiendo que hay datos firmados en «FirmaDigital»
gpg: Firmado el lun 13 mar 2017 22:30:36 CET usando clave RSA ID B133FF81
gpg: Firma correcta de «AlejandroAnton <alejandro@gmail.com>»
http@http-VirtualBox:~/Escritorio$ gpg -a --sign FirmaDigital
Necesita una contraseña para desbloquear la clave secreta
del usuario: "AlejandroAnton <alejandro@gmail.com>"
clave RSA de 2048 bits, ID B133FF81, creada el 2017-03-13

El archivo «FirmaDigital.asc» ya existe. ¿Sobreescribir? (s/N) s
http@http-VirtualBox:~/Escritorio$ gpg --verify FirmaDigital.asc
gpg: Firmado el lun 13 mar 2017 22:31:22 CET usando clave RSA ID B133FF81
gpg: Firma correcta de «AlejandroAnton <alejandro@gmail.com>»
```