# EJERCICIOS DE CRIPTOGRAFIA

Antonio Soler Amorós 2ºG SMR

## 1.Ejercicio cifrado simetrico

1º creamos el documento que queramos cifrar, en este caso ejercicio1
2º **gpg -c ejercicio1** para cifrar y nos pide una contraseña
3º para descifrar ponemos **gpg ejercicio1.gpg** y ponemos la contraseña

## 2.Ejercicio creación de nuestro par de claves publica-privadas

1º **gpg –gen-key**
2º ponemos un 1 para indicar RSA y RSA
3º tamaño requerido 2048 bits
4º ponemos un 0 para indicar que nunca caduca ca contraseña y confirmamos
5º ponemos nombre y apellidos, correo y un comentario
6º hay que hacer cosas en el pc para acumular bytes

## 3.Ejercicio exportar e importar claves publicas

1º ponemos **gpg -a –export antonio soler** (ID de la clave)
2º **gpg -a –export -o 1234.asc** (nombre del fichero que se creara) antonio soler
3º **gpg –import 1234.asc** (para ver el contenido)

## 4.Ejercicio cifrado y descifrado de un documento

1º pones **-aer antonio**(contraseña) **–encrypt 1234.asc**(documento)
2º **gpg 1234.asc.asc** para descifrar y nos pide la contraseña, ponemos antonio(contraseña) y ya veriamos el contenido

## 5º Ejercicio firma digital de un documento

1º creo el documento docuementoparafirmar y pongo la contraseña
2º pongo **gpg –verify documentoparafirmar.asc** para verificar que nadie lo ha modificado
3º modifico el fichero
4º pongo **gpg –verify documentoparafirmar.asc** para verificar, pero me dice que la firma no se pudo verificar, que no se ha encontrado ninguna firma y que hay un error en la suma de comprobacion