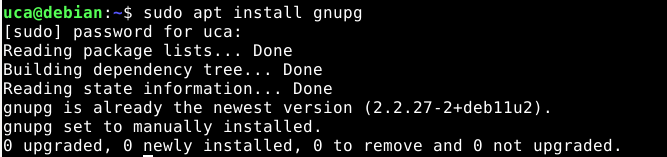
Laboratorio 1:

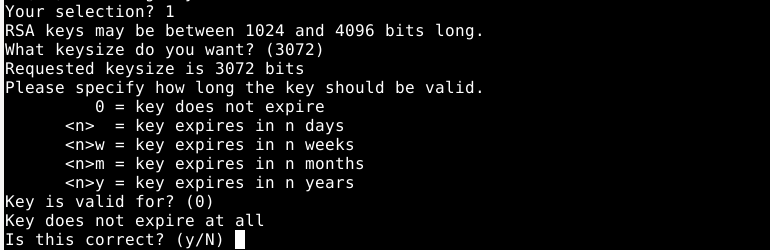
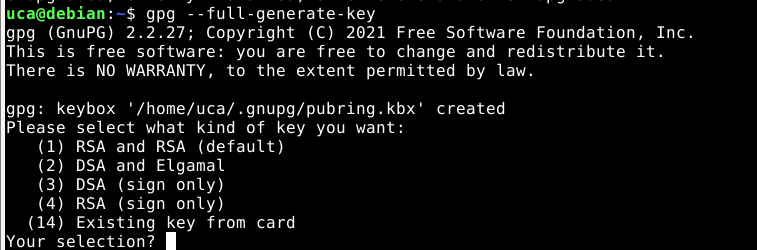
Victor Rafael Valenzuela Cortez

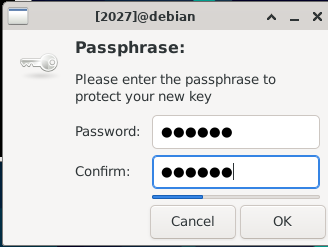
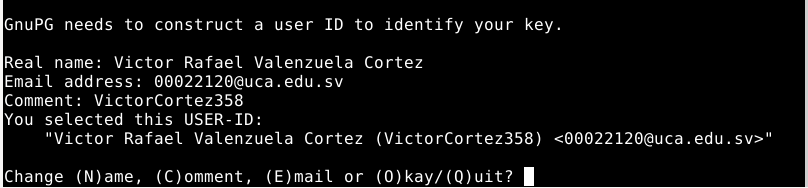
00022120

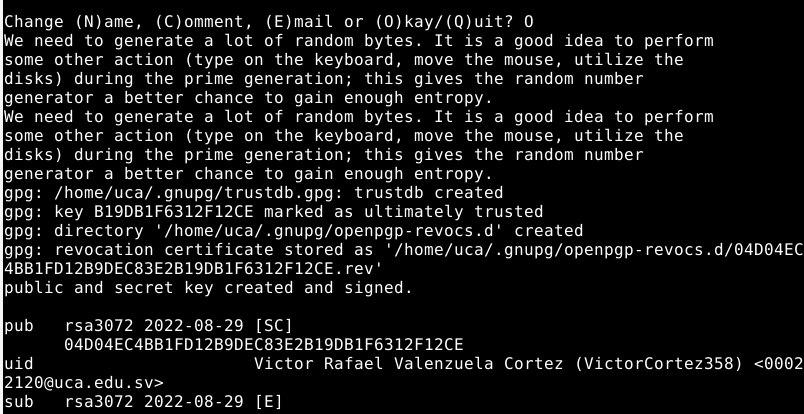
Instalar GPG

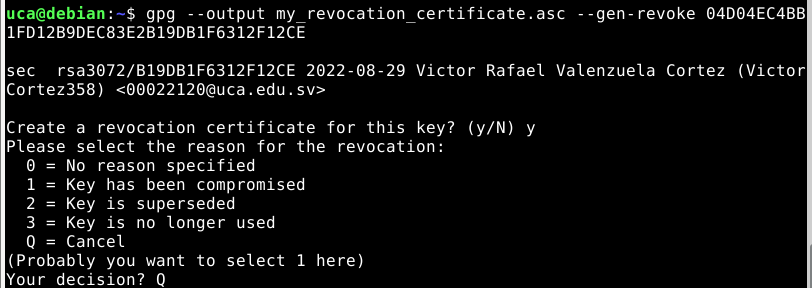


Generando llave

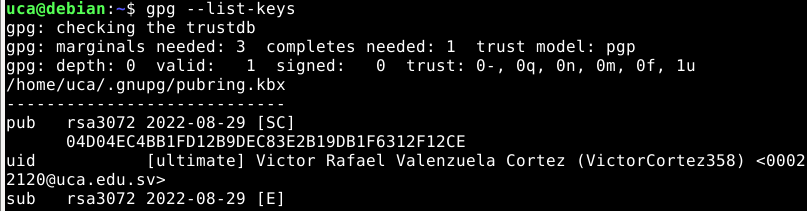






Remover el certificado a la llave

Lista de claves que hay



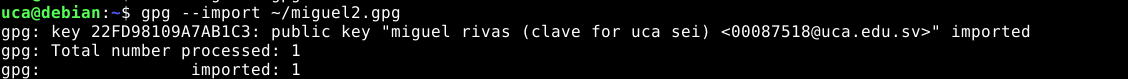
Exportar clave

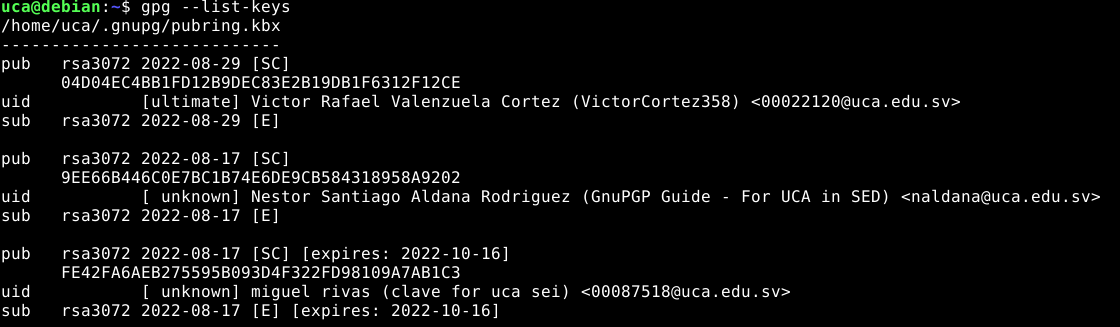


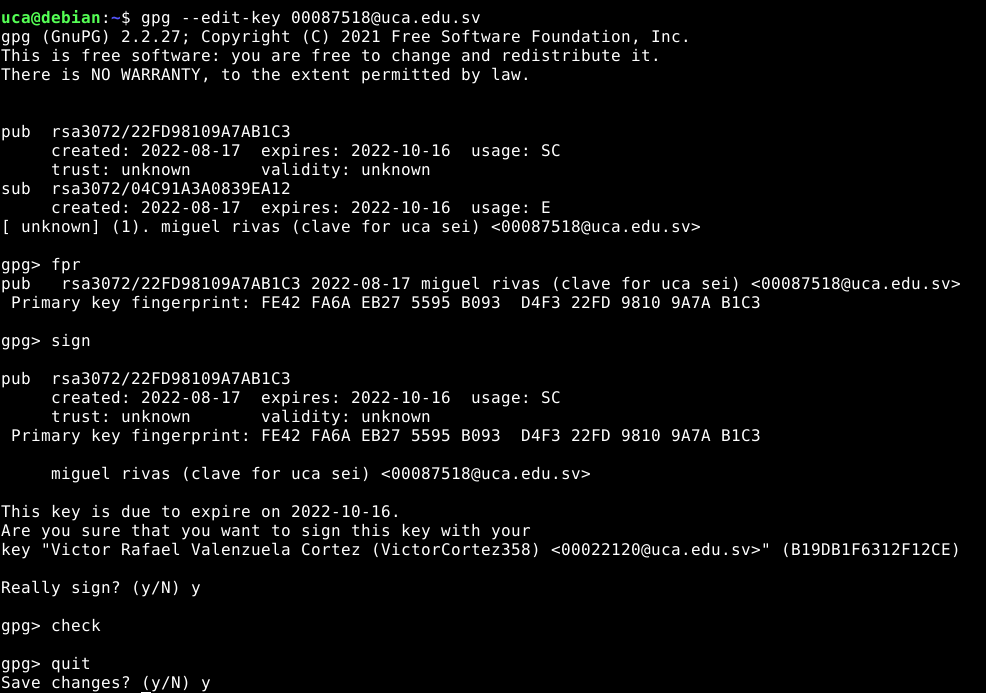
Importar claves

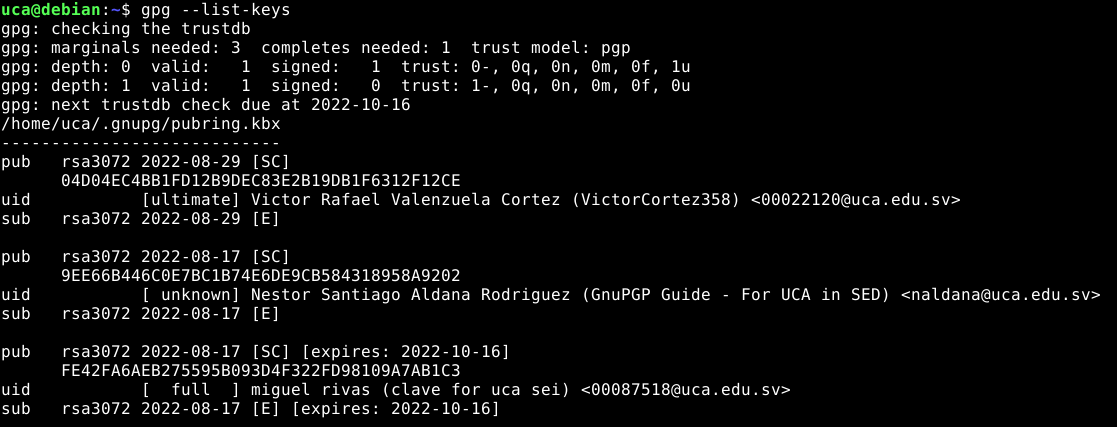




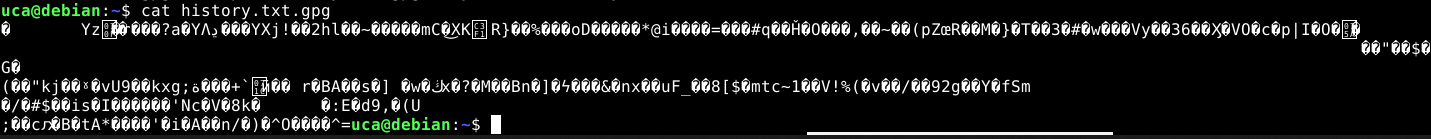
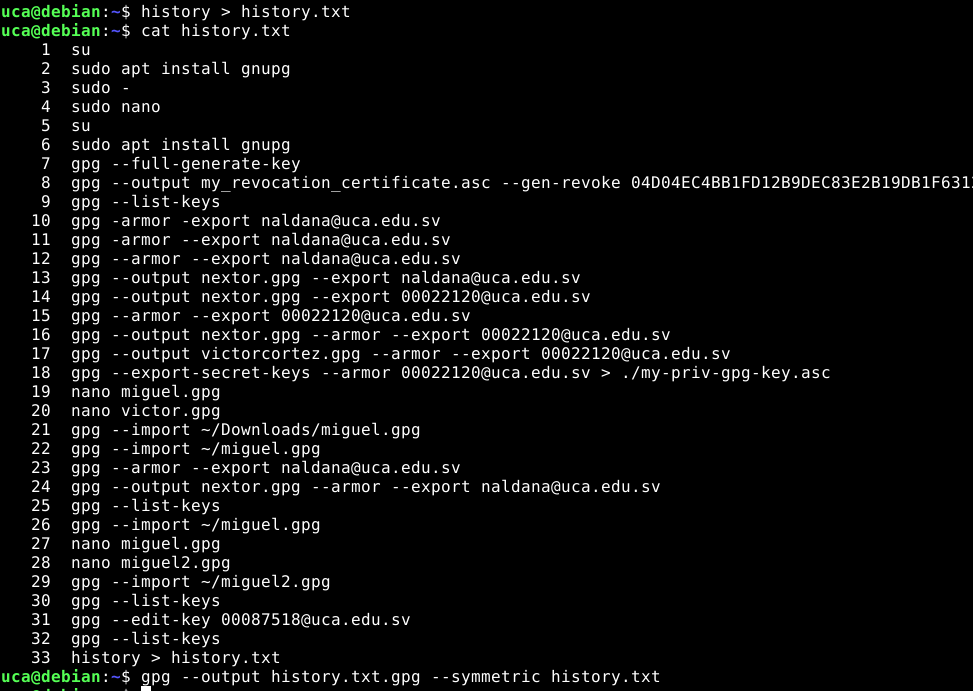




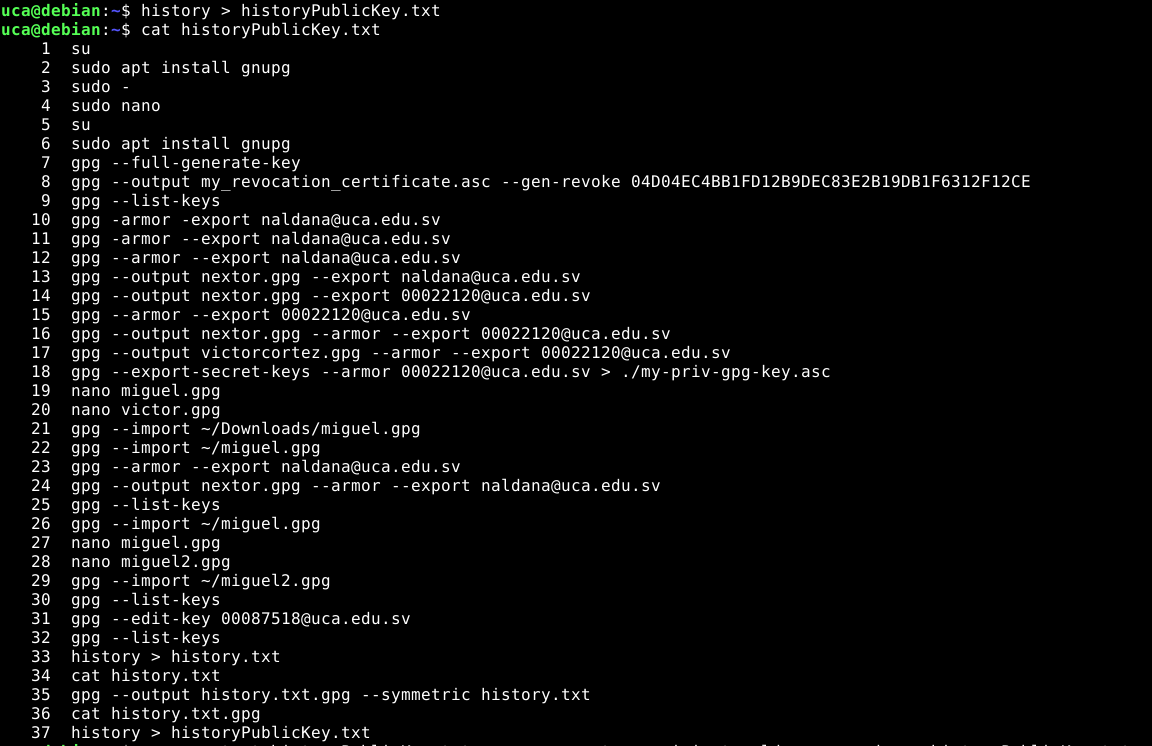


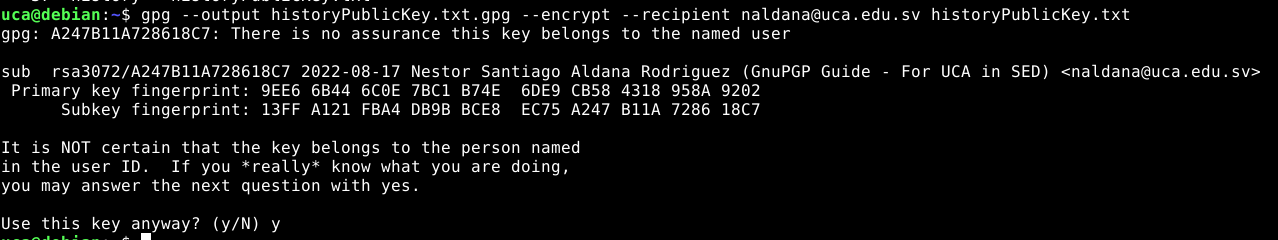


Cifrado simétrico



Cifrado

asimétrico:



* ¿Cuál es el punto más débil de PGP?

Phong Nguyen identifico un error grave en la manera en la que GnuPG creaba y usaba claves ElGamal para firmar. Éste es un fallo de seguridad significativo, ya que podria provocar un compromiso de casi todas las claves ElGamal que se usuaran para firmar.

* ¿Cuándo es conveniente utilizar solamente cifrado simétrico?

Por que se puede adivinar la clave de alguna manera.

## Creación y verificación de firmas digitales

