1:

Per utilitzar l'encriptació GPG es genera primer un par de claus que es la següent:

- Clau Pública: serveix per encriptar o cifrar dades per a que no es pot accedir o utilitzar el arxiu sense la clau privada.
- Clau Privada: es la clau per descifrar el arxiu cifrat per clau Publica.

Per posar una escena ideal del seu ús posaré un exemple:

Manolo genera un par de clau una pública i altre privada, la pública el comparteix amb el Pepe, el Pepe utilitza la clau publica per cifrar un missatge que ho vol passar només el Manolo. I el Manolo utilitza la clau privada que ve de la parella amb la clau pública per descifrar el missatge, i el llegeix.

En resum Si vols que algun et passi un missatge que només el llegeixes tu, primer li has de passar una clau publica per a que ell encripti aquell missatge, només tu que té la clau privada corresponent pot descifrar i mirar el missatge, la clau pública es com el cadenat que pot posar a qualsevol caixa, però només la persona que té la clau que es la privada pot obrir.