

|  |  |
| --- | --- |
| **SEGURIDAD INFORMATICA** – 2º SMR | |
| UT5: Sistemas de identificación. Criptografía. | Práctica 1: Cifrado simétrico. |
| Nombre: Nuria Gutierrez Liaño | |
| Nota: | Observaciones: |

1. Busca información sobre el programa GPG:
   1. Significado de las siglas.

GNU Privacy Guard

* 1. Breve descripción.

Herramienta de cifrado y firmas digitales

* 1. ¿A qué herramienta supone una alternativa?

PGP

* 1. ¿Qué tipo de cifrado puede realizar?

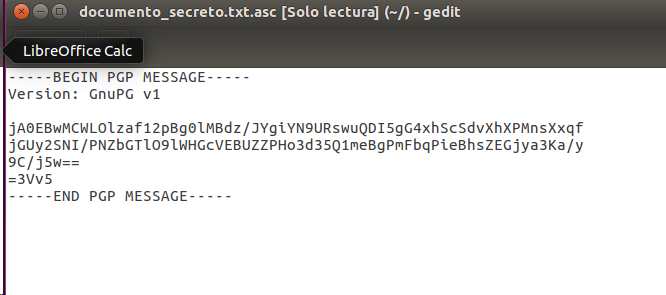
Asimétricos

1. Con la ayuda de las páginas man o internet averigua para qué sirven las siguientes opciones:
   1. –c 🡪 Cifrar
   2. –a 🡪 Cifra en formato ASCII
   3. –d 🡪 Descifrar
2. Ahora escribe un documento cualquier en texto plano, documento\_secreto.txt, y encríptalo usando GPG.





1. Abre el documento que acabas de encriptar editándolo con el editor que utilices normalmente. ¿Qué ocurre?



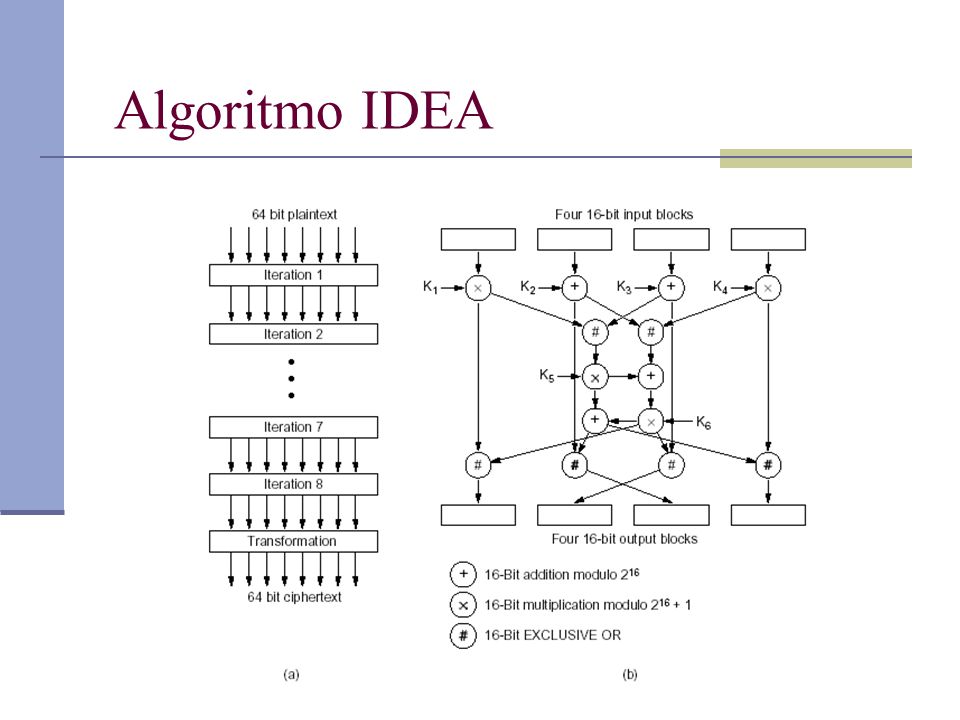
1. Cifra con GPG el texto que has escrito y envíalo junto con la práctica y la contraseña que has utilizado.

La contraseña es **password**

1. Investiga cuál es el algoritmo de cifrado simétrico utilizado.

Algoritmo de cifrado IDEA que está presente en PGP casi desde sus inicios. En su lugar usa una serie de algoritmos no patentados como [ElGamal](https://es.wikipedia.org/wiki/ElGamal" \o "ElGamal), CAST5, Triple DES (3DES), AES y [Blowfish](https://es.wikipedia.org/wiki/Blowfish" \o "Blowfish). También es posible usar IDEA en GPG descargando un plugin extra, sin embargo este puede requerir una licencia para usuarios de algunos países en donde esté patentada IDEA.

GPG es un software de cifrado híbrido que usa una combinación convencional de criptografía de claves simétricas para la rapidez y criptografía de claves públicas para el fácil compartimiento de claves seguras, típicamente usando recipientes de claves públicas para cifrar una clave de sesión que es usada una vez. Este modo de operación es parte del estándar [OpenPGP](https://es.wikipedia.org/wiki/OpenPGP" \o "OpenPGP) y ha sido parte del PGP desde su primera versión.



IDEA

1. ¿Cuántas claves necesitarías tú si quisieras enviar mensajes cifrados a 10 personas diferentes? 10 ¿Y si entre todos os quisierais enviar mensajes cifrados? 45 ¿Y si el grupo estuviera formado por 100 personas? 4950

Esto sirve para cifrado simétrico

**Formula:**

**= equivale a el numero de personas -1**