Introducción a la criptografía con GPG

Cómo mandar tu correo navideño con privacidad

Bienvenidos

- Angel Pablo Hinojosa
- @psicobyte_
- www.psicobyte.com

Mitos de la criptografía

- Criptografía “de categoría militar”
- Decodificar "paso a paso"
- Siempre hay un hacker lo bastante bueno
- ...pero hay que teclear como un poseso
- El algoritmo es secreto

Realidades:

- Sí existe la criptografía perfecta, pero no es práctica.
- El punto flaco son las personas.
- Recuerda siempre: "La seguridad es un estado mental".

Encriptar (cifrar)

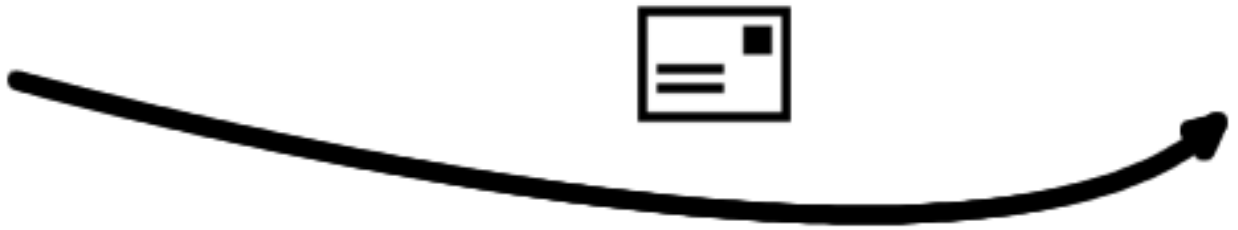
Archivo en claro

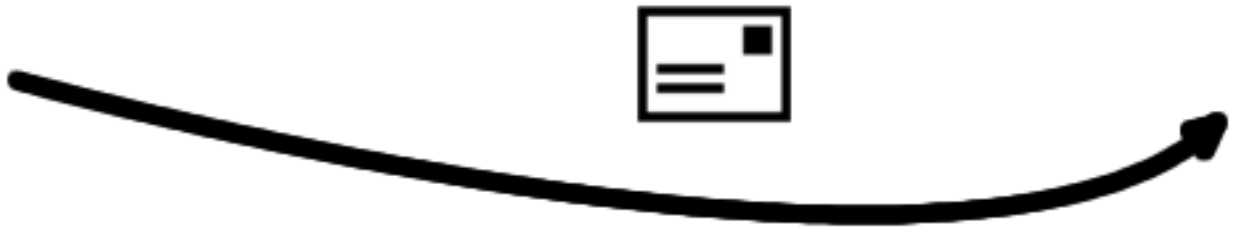
▼

Clave + Algoritmo de cifrado

▼

Archivo encriptado





Clave simétrica

Interludio matemático

¿Cuales son los dos factores primos del número 808567?

Es un problema difícil.

(Bueno: es fácil porque son pequeños, pero...)

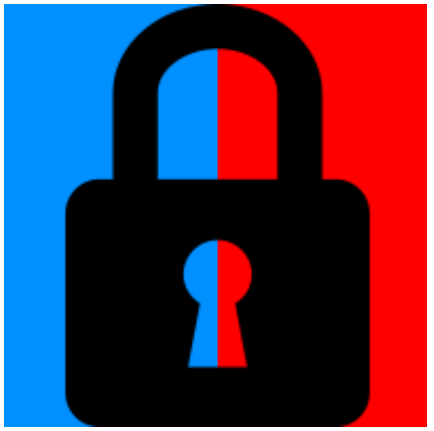
Interludio matemático

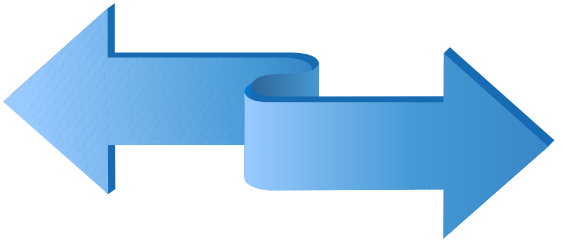
¿Cuánto es 811 X 997?

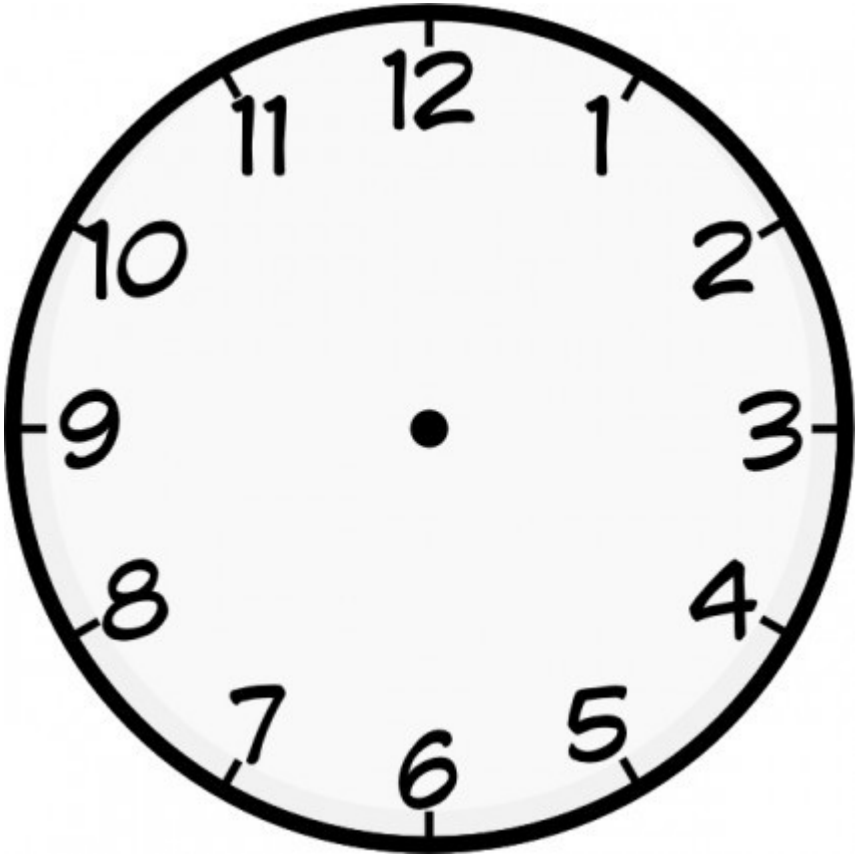
Es un problema fácil.

(incluso con número grandes)

RSA






12
1
2
3
4
5
6
7
8
9
10
11

Caveat

- Nada garantiza que mañana el problema deje de ser “dificil”.
- Pero no parece probable.

Clave asimétrica

En la práctica

https://www.gnupg.org

En línea de comandos

Crear par de claves:

```
gpg --gen-key
```

listar claves:

```
gpg -k
```

Exportar clave pública a un archivo

```
gpg --output ARCHIVO --export IDCLAVE
```

Importar clave pública de un archivo

```
gpg --import ARCHIVO
```

En línea de comandos

Enviar clave a un servidor

```
gpg --keyserver SERVER --send-keys IDCLAVE
```

Recibir clave de un servidor

```
gpg --keyserver SERVER --recv-key IDCLAVE
```

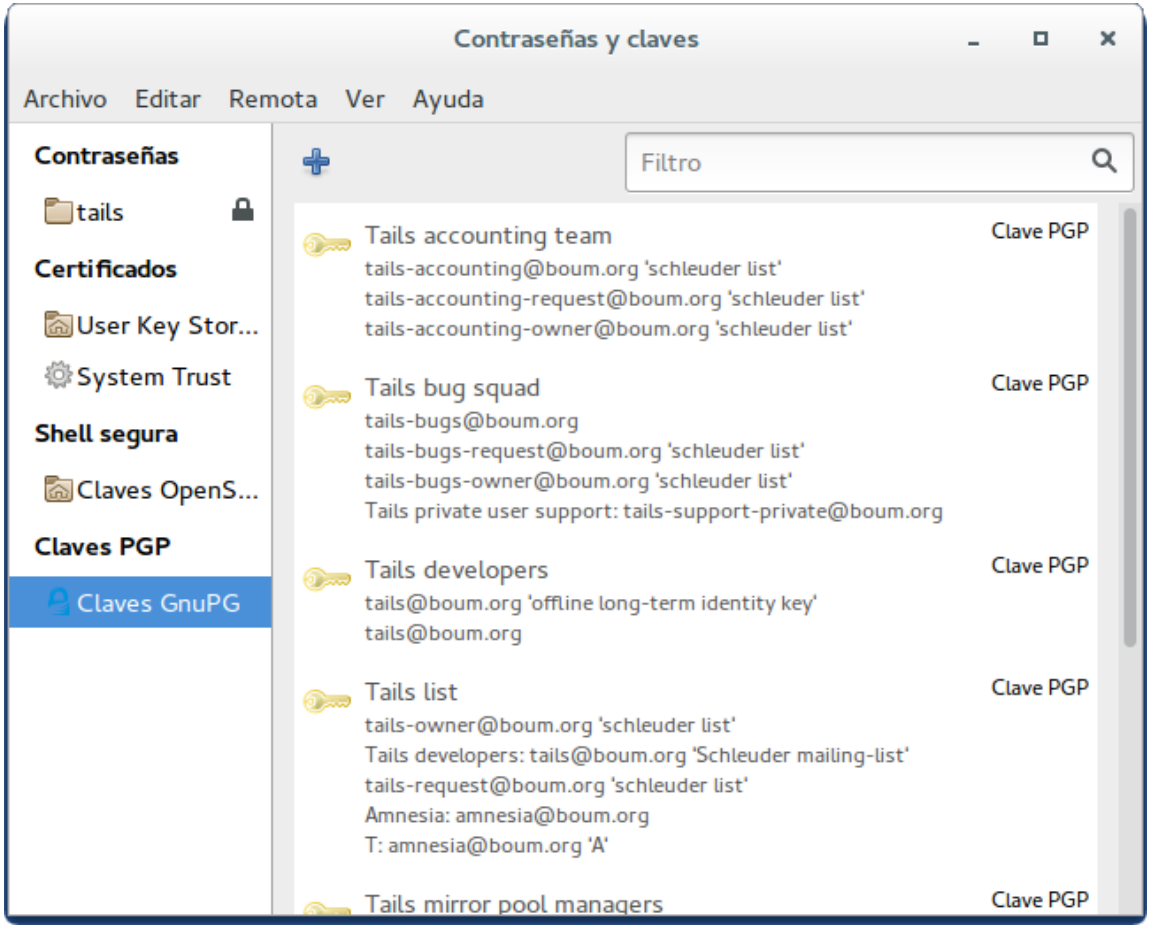
Encriptar archivo

```
gpg --encrypt --recipient IDCLAVE ARCHIVO
```

Desencriptar archivo

```
gpg -d ARCHIVO
```

Interfaz gráfico (seahorse)



Plugins

- Mozilla Thunderbird
- Evolution
- Nautilus
- ...

www.gnupg.org/related_software/frontends.html

Muchas Gracias

www.psicobyte.com/descargas/gpg.pdf