Práctica 1 (PARTE 3) PGP

PGP (Pretty Good Privacy) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos mediante el uso de firmas digitales.

Es un criptosistema híbrido que combina técnicas de criptografía simétrica y criptografía asimétrica. Esta combinación permite aprovechar lo mejor de cada uno: El cifrado simétrico es más rápido que el asimétrico o de clave pública, mientras que este, a su vez, proporciona una solución al problema de la distribución de claves en forma segura y garantiza el no repudio de los datos y la no suplantación.

¿Para qué lo podríamos utilizar nosotros?
Podríamos generar un par de claves PGP para proveer a nuestro cliente de correo la posibilidad de enviar y recibir mensajes:

- Cifrados y firmados
- Cifrados solamente
- Firmados solamente

También lo podríamos utilizar para cifrar información personal como pueden ser archivos, carpetas o incluso particiones enteras de disco. Para esto, PGP nos permite utilizar tanto criptografía simétrica (utilizando algoritmos como AES) o criptografía asimétrica (utilizando la clave pública del destinatario).

Red de confianza en PGP
Tanto cuando ciframos mensajes como cuando verificando firmas digitales, es crucial que la clave pública enviada a alguien o alguna entidad realmente 'pertenezca' al destinatario intencionado. Existen repositorios públicos donde podemos subir nuestra clave pública PGP. El hecho de descargar una clave pública PGP de algún sitio no nos asegura que podamos confiar en dicha clave.

Para utilizar PGP adecuadamente necesitamos poder asegurarnos que la clave pública de un usuario es efectivamente la que dicho usuario dice ser. Para ello, luego de tener la certeza de que dicha clave pública es la de dicho usuario, deberíamos firmarla utilizando nuestra clave privada. De esta forma, nosotros certificamos ese documento que se corresponde con la clave PGP de otro usuario.

Ejercicio 19

a. Si no tiene una clave PGP, genere una utilizando el comando:

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

b. El siguiente, es un archivo firmado por alguien aparentemente de confianza. Use PGP para descifrarlo y siga las instrucciones para obtener la flag

```
-----BEGIN PGP MESSAGE-----

owHFWHtMFEcYB9Fa1phINDXVtmxbNWmpnPgqPqoiVSrBZ41Wg5plbw8v3ovb46Ge
eKe0giRqay3Q07CPAyEBRSA86uOqpC/bRtumSmyqdUxjWtv6R2ujWLUzszt3e3CH
h0U6DNwyOzPf7/t9v++bye0bHhNFRbd49xyfMmtQVHT9yLtZT1qsDibRUeDQd2Wd
pzVtg9qUR3WA0kzQ0eqwEz3SmbSTRh+UZvUcPArHlXe004kXbuiHRhEIuOlo5wZs
Bv6Fv7Bn9ocR1R0d/Hm8LRMbUqh6rA2aUA1NSpxIL+AdHM3Y2Y3GPCttyOVog9Fu
ZvRWmrVa6FwLQ7MmJo+jbR0fZZmMLENzFtrE0DlwIvyw2Y0WluMZOmPBohS0wtBR
z4Q0NWA+JUGfXud4lrFnd4g0Z6J5Y3aukbNovETgOd4BX2t9he6YjbxZdXhmBKZQ
2+hw2PiZOp3ebszjErOt1mwTl8hazTqD0cTp9Lok2wx9etLqpKU5NiZ5iSk1Z5p9
KpvHrHzzrWnzk5PNjhRdnpHLn5vL217jNzKQzuz/k7zJCnmchbUbbQ6FP8KaXiEV
0bWZZliW03fU0gyizWgxWCGPrLGjyYKodHAWo555mK0Bc2oKdCrVaraZOOQRxOtg
7BxCrYd6hjhtjJ2h7RwMu5mxo/cGE5P9cAMhLD3mphhChaLXekXjOqup2HSgkkfW
YLHDtbU3O7ieI6e1hT9QjSO1RIV31++0LtOJj43A6UGjU0VtD90BuqHLVI8HcjBk
OpFtigKCC0guIAtALgKyS+1CXzpa4gVyM5BbgHgKCL5Al1rRoFyNJ7iA2Mede3QK
SA1A9gGxEgge0o8TYz5szG/PqzojKhAhvlNAhDPh2lIglIQ3A19VoG3Rhq14t15h
SYS1bl10YXbhRhAx3EX0774fCC1AqlYpRyMlwc4oEN0ajr0B8iRBMy4EoylWoWuD
0FsnPEoIJKXZhYAOubsaVm/3gEqEb/RvBZqGntuAuAtjbQDCriDCQmtJINGDcmpB
TKH+HhB2BHyGkRQqqe7glHiFFlmx4iIQi/D6ZuzeUSDXA/kkjvI7eJo72B9sCc30
dxJGAqJ7oIKcwXOQVt1Yu6ExtSIZhF4P4ZapuOXDGKgfx2ENYX6syrQTQYiFMiDg
nBF2hs9ggeRGqSbVQs+uIHlW1IPpNmzDLx5NFxXzkMsqINZhTG2h5nhUeSDOwmmj
O9De4fpzzoP0LhPhol6EFBngvoR0t0ajpCyK3eb45a4opIrs6VVLkKiklydcnekd
brecK1E1gPLUX5JIxQ2qd0qvwzQ347wJrsdoB4+G9aNALAkr30eCS0ArWhSJA6on
bpw0niAWw4rSpaYpSrISILfjPXdFAqCPcFEc2wIJri1MkPhwh5bkL1UtGGWpGiIl
z+Rikn/9DlfJFagEhV2pHatNUcIJtdYGziSvevIppUoWyfGJfZNxcVWBenpm1X+H
W453h1VZKc/ViGl4CqAcJ6L0PwRAYEVC3BC0VkiSG6csnLY3cgx9FQNWAuKmGgfx
JGbxlBpWiRxmgQcsA3TvKVUvJ0EVrTJCUh8VLiRYvfr4NBcjUuoRbuIVgrsPM00A
qX5GKtN+gRtMMww0UkKzismPQ2pTrwpB3a2uGmi4kit0NP04kKbDOzngcBWrMFeC
x2UfubuEAiT1rWb1H1ykYE/EF9ael9e+pVcQXIoqiW4aHBVNRT371POD40/nCXf3
gKYFjuvvkq8HhwxCXwlGUbEjyAjTOez+uKv15xqSU8e9+GV99e7kHZtNGbO3x+3+
1PtV4+XLY3TpCUPvVK/Mj08bfuLvI4N4X9Hq9Bs3Fx56el3c4oNdU+fWdiY0ppxP
62wtOOLJKP+1/fP4umW28QWuwvhDD4aOAH/NKNy0Z17rpUOfLPmuefQ/g4ctHXUh
7lKXLWZ/TWHsvcs727YWcY2jpQlXvllRtr5xTXHtJnrZz1f33m75fWzttpG6jyet
Sf7h++kTrsdccrS+VMc33T+wLytmek357K4C08WXnyunDLvPdp6xzW9/IlUcL9ne
fn9i6SrDzY57v41Zfiu/atvXNfnpqxbHuYaMil1xcd0XbqducupaW8vWe82vGm/t
HM2Pub3y2mrHCw/mPHjl+htsY3PqVn7cjYSMEXO2XBi65Fhh1aqyK+Y/WkHahKIz
Lj52bX1hVGlGCvPZM0729AwfOz1uUUXO8Q/SmO0JuxcWLFtUvb4mk5l19ds/Y9Zd
adv/45bGiz4hsb0hLv7gh5UHXPLkeSPP/HRu/nLA/1J5rPwuFTv2zrWzTbPYfwE=
=sAUb
-----END PGP MESSAGE-----
```

Ejercicio 20

Utilice el diccionario indicado en el desafío publicado en la plataforma CTFd para crackear un archivo encriptado utilizando PGP con criptografía simétrica. Ver challenge **ej20 - symmetric pgp**

Ejercicio 21

Encriptar asimetrico: Encriptar con PGP el archivo "encriptar.txt" con la clave pública dada. En el CTFd, ver el ejercicio **ej21 - PGP encrypt asymmetric** y para obtener la flag, realizar el submit del archivo encriptado en formato armor en ic.catedras.linti.unlp.edu.ar 12003 de la siguiente manera:

```
cat encriptar.txt.asc | nc ic.catedras.linti.unlp.edu.ar 12003
```