Criptografía y Seguridad
Practica 1

Equipo Pingüicoders
Arrieta Mancera Luis Sebastian
Cruz Cruz Alan Josué
García Ponce José Camilo
Matute Cantón Sara Lorena

Desarrollo

- Diferencias entre entre texto claro y cifrado, imagen clara y cifrada
  - Texto
    texto cifrado

```
camilo@wowi:~$ cat mensaje.txt.pgp
-----BEGIN PGP MESSAGE-----

hF4Du3wTAQdmfrwSAQdAVp4ujb13aT+zd7tz83LeLW+gNOWxwg8qYdAouFdUpCEw
HeirEsSn26SiztdUGL/5VDJe9xkqU694PVaOwocwurPvUUpmaeghiOM6UBf8DegQ
0m4BDSEN8Oz1JFQpa+Iepqw9nzbxion1Hy/wpi7LTb0wxep3i7UDV9jiwY5wZo9k
69gZ3eKbWP2xXnm6o0sOrqLz2RKAZZgv9OzZbwwtHTKbypJBX+H5zUGwMWqk2CJC
/z7uuL1NPcZoVprGDL9/9Q==
=oCHA
-----END PGP MESSAGE-----
camilo@wowi:~$
```

    texto claro

```
camilo@wowi:~$ gpg -d mensaje.txt.pgp
gpg: encrypted with cv25519 key, ID BB7C130107667EBC, created 2024-01-20
      "Camilo (int1) <jcamilo@ciencias.unam.mx>"
Hola mucho gusto, soy Luis Sebastian :D
camilo@wowi:~$
```

    Las diferencias más claras, son que en el texto claro podemos leer fácilmente el mensaje, a diferencia del texto cifrado donde solo hay símbolos los cuales no podemos encontrarles un sentido

    Para descifrar usamos el comando gpg -d archivo

  - Imagen
    imagen cifrada

```
camilo@wowi:~$ cat imagen.jpeg.pgp
-----BEGIN PGP MESSAGE-----

hF4Du3wTAQdmfrwSAQdA33Oon4j+pxuek3Jmk+5hZS87Fn23Sm5peHtZis5AVxMw
/jvMez8bIaaUihNtR/sKRBxWkcqGawdY3OswWvXsUOBXYLoqYJjeUS/7yubagdKc
0u0BpcwrrywN3EdYDIwWzLG8CAuiKqBkSesTThiTjWrilV8M5krDtc4og+P2R1rx
BaoAN6KYoDjUsgGWuzteUrJx9DLSuYOvrNPIfC7MBDjWZpJVICKmzMVC5XncNpmQ
6sb4ZotW5434V8hmRoXM5UXPsqR1kGa8yc1KDYqLxLZVQGDHAvHeze/y0lyH2PoX
apj13bbBN9TA8ZS8POMZhcaTluOMfr/vpxCmWs3gpAy8Z1ASNlcvn+hPxkXkfWTT
O2XJ5Z5fHUn2XYrok6DhwjHihhS3PsCmEsRbTYeUw6V+lRgK1sNyMO4C6R6AW92F
QA2KDOuCpEyHmc9/+LaxMC75jJgU63iw0G6JMQner5RYW3ATzndlmdPfx1tUV1Q4
V+Gl7KdmL5gQJsrFbBM7HrfnDoh/zNzqnAsPIFl9g97RJMgfyqkF2hHDaoUrf1//
vauVXp/TeZ5cYj25s8/MsZSVyd2GTAiC6rySF6uzFBhptw8UFD1h5zwxqOks5j0c
```

imagen clara (es la obtenida luego de desencriptar)

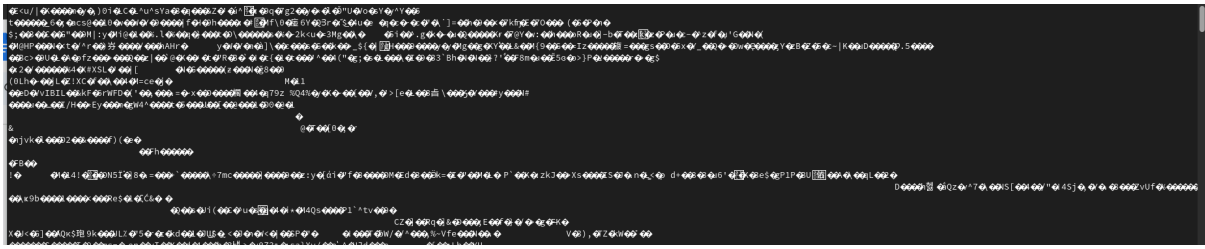
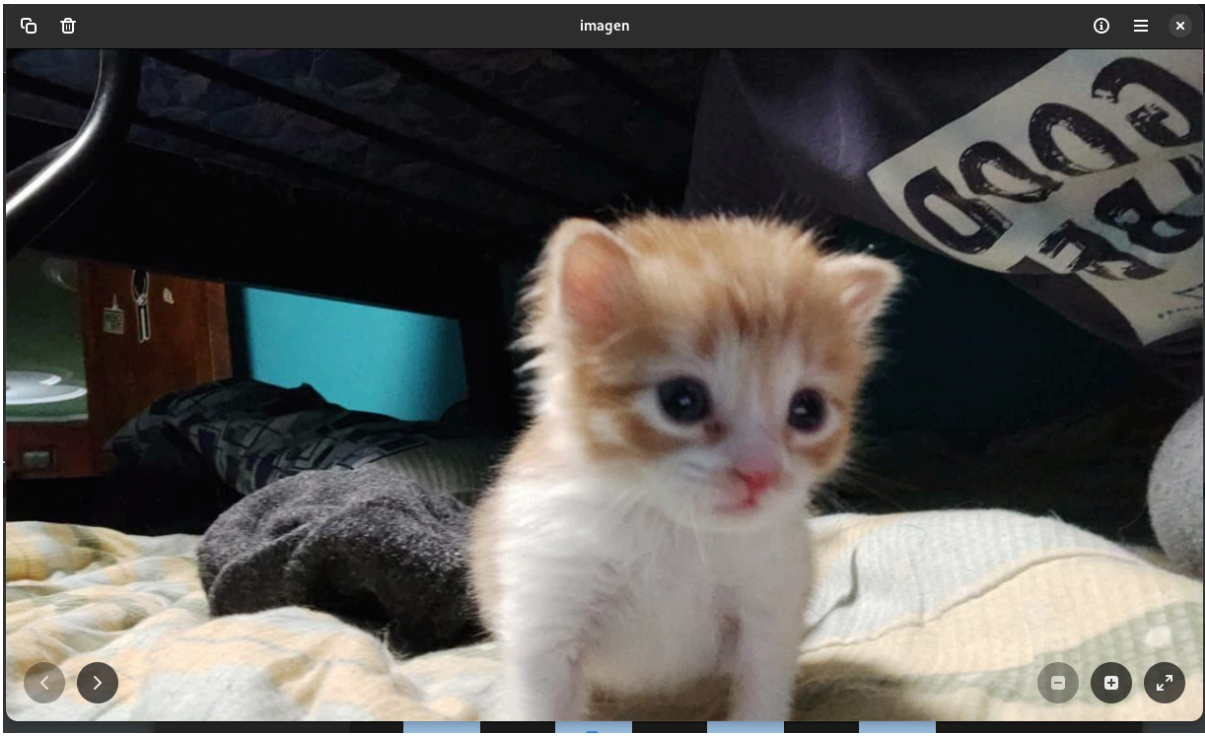


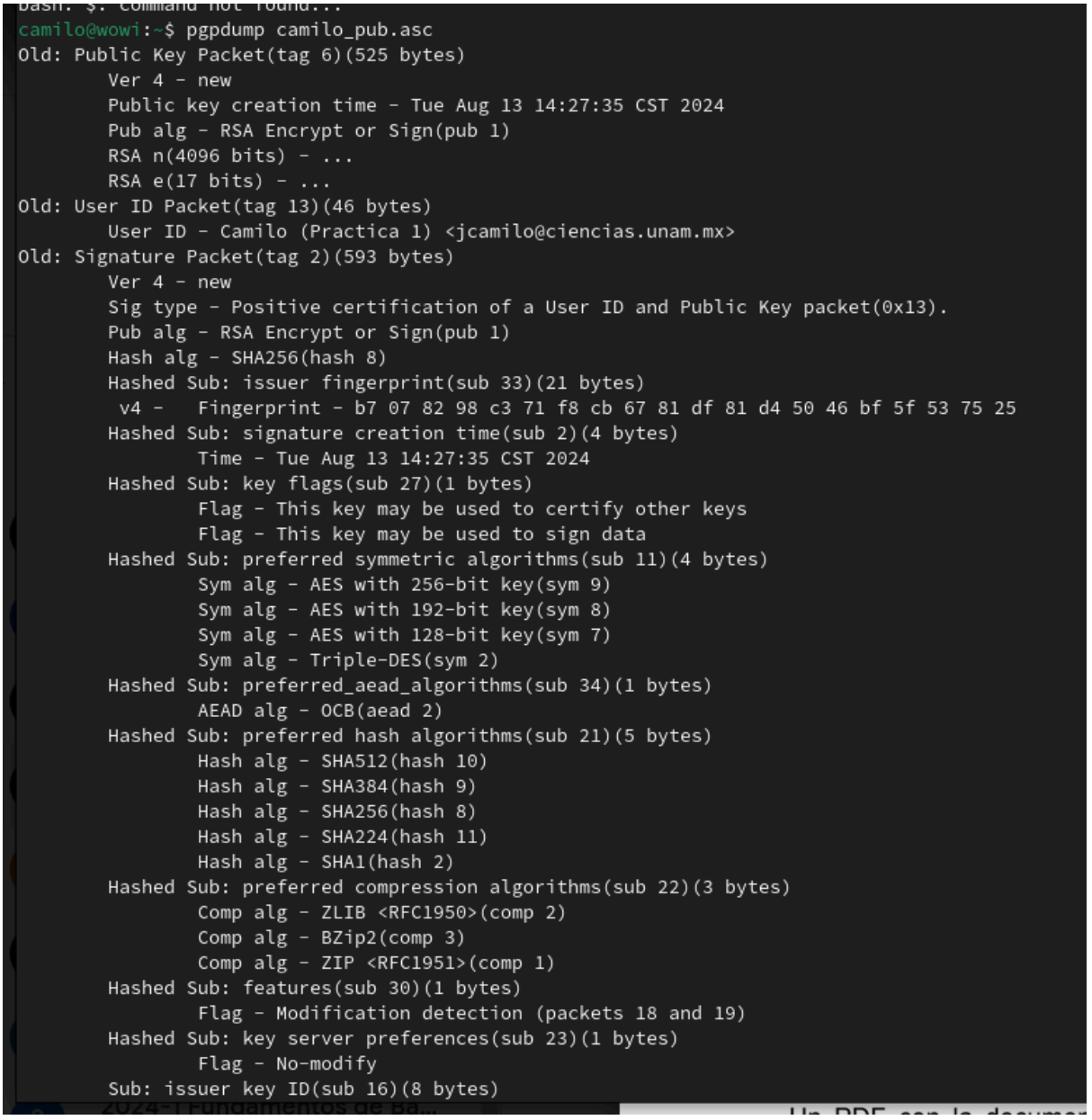
imagen clara (ahora visible)



La principal diferencia es que la imagen clara es muy muy larga, la versión cifrada también es larga pero sí se pudo ver toda en una terminal, también la versión cifrada son símbolos y la clara es una versión fácil de reconocer

Para descifrar usamos el comando gpg -d archivo pero la imagen solo se mostró en terminal como símbolos raros, entonces para obtener la imagen bonita usamos gpg -o imagen -d archivo

- Análisis de llave pública con pgpdump



En Old se indica el tipo de información que contiene el paquete. En Public Key Packet tenemos: Version (la versión del formato de la llave), Public key creation time (cuando se creó la llave), Pub alg (algoritmo usado para generar la llave), User ID (con el nombre y correo del propietario) y Signature Type (que indica el tipo de la llave), también aparecieron muchos datos más y creo que algunos se repetían (o al menos creo que se repiten). Y en New Version indica la versión del formato PGP utilizado.

- Preguntas
    - ¿Qué pasa si comprometen mi llave privada? ¿Qué opciones tengo?
      El que tenga mi llave privada podrá descifrar mensajes encriptados para mi o firmar archivos como si fuera yo.
      La opción que tenemos es revocar la llave (para esto necesitamos crear un certificado de revocación y luego distribuirlo), para que ya no pueda ser usada y avisar que fue comprometida, y luego generar una nueva llave.

    - ¿Bajo qué escenario el sistema PGP puede ser vulnerable a un ataque de MitM y cómo mitigarlo?
      Cuando un agente maligno convence a alguien de que su clave es la de otra persona, engañándolo y pasándose por otra persona.
      Esto lo podemos mitigar obteniendo la llave pública de la persona por un medio confiable o usando mensajes con firma.

    - ¿La comunicación por correo electrónico en servicios como Outlook o Gmail está cifrada por defecto?
      Por defecto Gmail no cifra sus correos, por lo cual son visibles para Google.
      En el caso de Outlook es algo similar.
      Pero existe la opción de cifrar los correos en ambos servicios.

    - ¿La comunicación por correo electrónico en servicios como Outlook o Gmail está cifrada de extremo a extremo (E2EE) por defecto?
      No, esto no pasa por defecto. Gmail y Outlook se cifran con Cifrado en Tránsito (se cifra entre el servidor, el que lo envía y el que lo recibe).
      En cambio E2EE solo es entre el que lo envía y lo recibe (dejando fuera al que provee servicios).

Bibliografía

El manual de pgp y pgpdump
https://support.google.com/mail/answer/6330403?hl=es-419
https://gist.github.com/johnfedoruk/7f156d844af54cc91324dff4f54b11ce
https://support.google.com/a/answer/10745596?hl=es-419#zippy=%2Cpuedes-hacer-que-el-clc-sea-el-ajuste-predeterminado-de-las-aplicaciones-de-los-usuarios