UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Práctica 02: Correo cifrado - Las Canijas Lagartijas

ALUMNOS

Gabriela López Diego - 318243485
Abraham Jiménez Reyes - 318230577
Javier Alejandro Rivera Zavala - 311288876
Juan Daniel San Martin Macias - 318181637

PROFESORA

Anayanzi Delia Martínez Hernández

AYUDANTES

Cecilia del Carmen Villatoro Ramos
Roberto Adrián Bonilla Ruíz
Ivan Daniel Galindo Perez
Roberto Adrián Bonilla Ruíz

ASIGNATURA

Criptografía y Seguridad

21 de Febrero del 2024

1. Introducción

En esta práctica exploraremos en el sistema de cifrado PGP, creado en 1991 y el cual se encarga de cifrar correos electrónicos, archivos y verificar la identidad de la persona que envia el mensaje para ofrecernos mayor privacidad y seguridad al momento de comunicarnos con otros usuarios. PGP funciona mediante el cifrado simétrico y asimétrico, es decir, usando llaves privadas y publicas. Las llaves publicas del destinatario se utilizan para cifrar el correo y las llaves privadas para descifrarlas. De este modo, nos aseguramos que la información contenida en el correo electrónico permanezca totalmente confidencial.
Ahora, para comenzar a dar uso de esta herramienta instalaremos la extensión llamada *FlowCrypt* en nuestros navegadores web (Chrome y Brave) y crearemos nuestras correspondientes llaves privadas y publicas.

2. Desarrollo

Para esta practica se utilizó de la extensión FlowCrypt en Chrome.

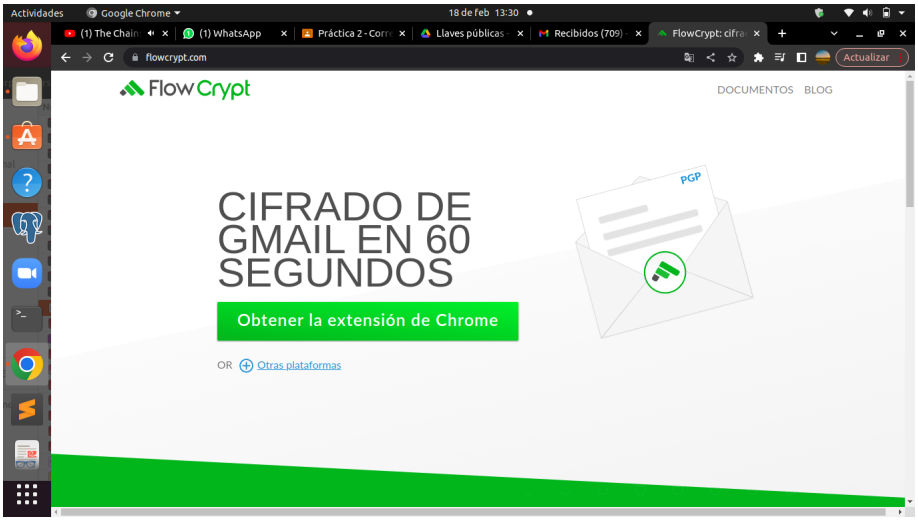

Figura 1: Evidencia 1

Ya que tenemos la extensión instalada procedemos a iniciar sesión con nuestra cuenta.

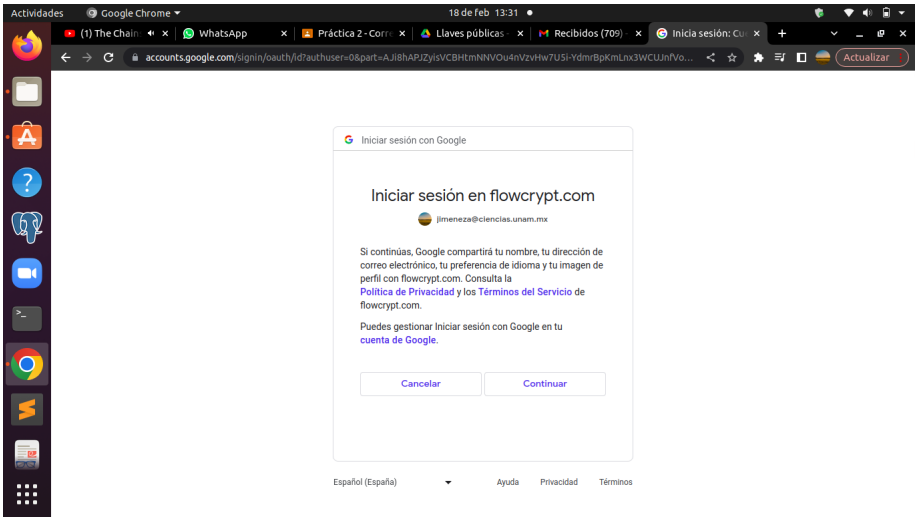

Figura 2: Evidencia 2

Al principio nos pedirá una frase secreta que será la que utilizaremos para nuestras encriptaciones e inicios de sesión. Esto nos genera nuestra llave de tipo RSA de 4096 bits. Ya que se realizó éste paso nos llegará un correo de Flowcript.

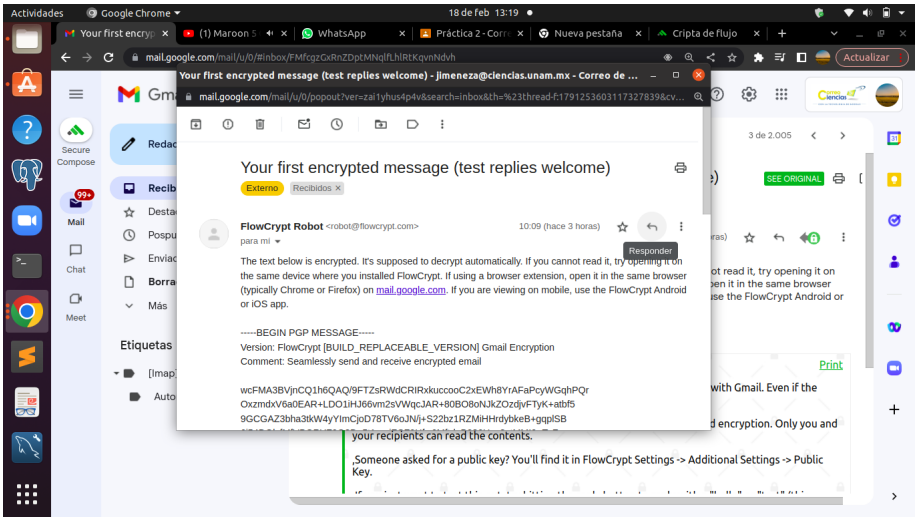

Figura 3: Evidencia 3

Podemos encontrar nuestra llave pública en la parte de configuraciones adicionales.

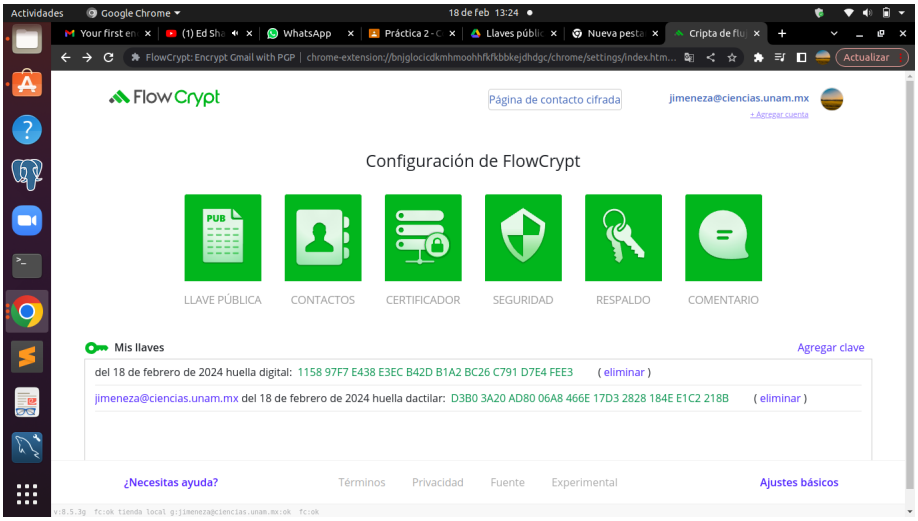

Figura 4: Evidencia 4

Procedemos a enviar el correo al ayudante.

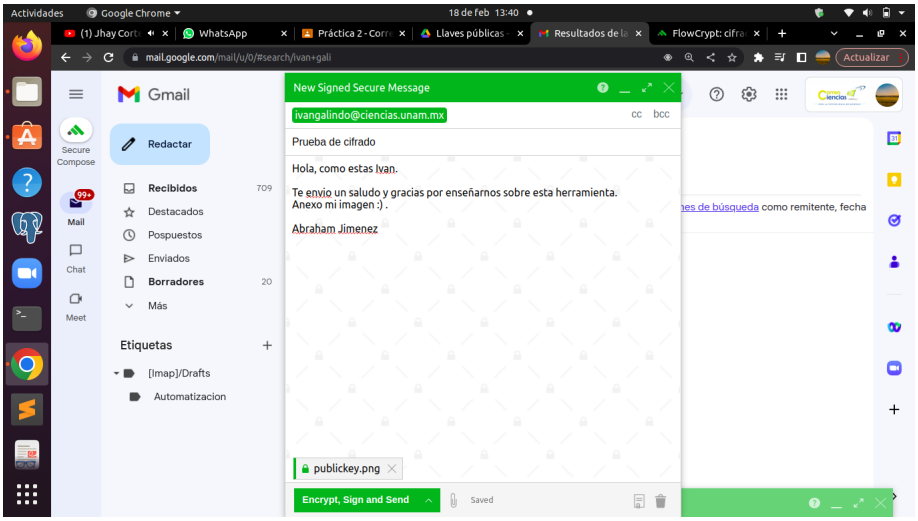

Figura 5: Evidencia 5

3. Preguntas

1. ¿Qué pasa si comprometen mi llave privada? ¿Qué opciones tengo?

   En caso de que terceras personas llegasen a tener acceso a nuestra llave privada, puede que sean capaces de leer correos electrónicos encriptados que habíamos recibido con anterioridad o estén por mandarnos. También conseguirían firmar correos electrónicos a nuestro nombre sin nuestro consentimiento.
   Ante esta situación, podemos actualizar nuestra llave privada o bien, revocarla en su totalidad.

2. ¿Bajo qué escenario el sistema PGP puede ser vulnerable a un ataque de MitM y cómo mitigarlo?

   Cuando dos personas desean intercambiar correos electrónicos usando PGP, primero es necesario que intercambien sus llaves públicas . En este proceso, el atacante buscará interceptar la comunicación entre ambos y modificar las llave publica del destinatario por una suya y así obtener el o los correos encriptados que estaban destinados originalmente a otra persona. Podemos mitigar este tipos de ataques buscando una forma de intercambio de claves mucho más segura, ya sea por un medio de un sistema de seguridad más fuerte, o en su defecto, organizar una reunión presencial.

3. ¿La comunicación por correo electrónico en servicios como Outlook o Gmail está cifrada por defecto?

   Sí, los servicios de correo electrónico como Outlook y Gmail cuentan con un sistema de cifrado durante el transporte de los mensajes. Este tipo de cifrado, conocido como TLS (Transport layer security), se encuentra activado tanto en Outlook como en Gmail por defecto, aunque no asegura la privacidad de la información de los mensajes, mientras que estos se encuentran almacenados en los servidores de Microsoft o de Alphabet.

4. ¿La comunicación por correo electrónico en servicios como Outlook o Gmail está cifrada de extremo a extremo (E2EE) por defecto?

   Ninguno de los 2 servicios cifra los correos de extremo a extremo por defecto, pero ambos ofrecen opciones para así lograrlo. Outlook cuenta con la opción de activar ese tipo cifrado a través de S/MIME (Secure/-Multipurpose Internet Mail Extensions) con cifrado asimétrico, por otro lado, Gmail tampoco cifra sus correos en el servidor de forma predeterminada, por ende los mismos serán visibles para el destinatario,

el remitente y para Google. En el caso de Gmail, tal servicio sólo está disponible para usuarios de una cuenta Google workspace, el cifrado se realiza a través de S/MIME y comenzó a estar disponible a fines del año pasado.

4. Diferencias entre texto claro y texto cifrado

Explicaremos en primer lugar, como funciona el mecanismo de cifrado empleado para este apartado: Flowcrypt utiliza pretty good privacy o PGP, los datos se encriptan para que solo puedan ser descifrados usando una clave pública, que está asociada a un nombre de usuario o una dirección de correo electrónico. Cuando PGP comprime la información, una clave privada aleatoria se genera automáticamente. Este par de claves pública y privada mantiene la información segura, ya que esta solo se puede descifrar usando la clave privada que corresponde a la clave pública. Ahora, al comparar los mensajes para ver que tanto cambiaba el mensaje cifrado respecto del mensaje normal, notamos que hay marcadas diferencias entre el texto del mensaje original y el texto cifrado. Obviamente el texto original es legible y goza de un significado claro de acuerdo a las normas sintácticas y semánticas del español, mientras que el resultado es un intrincado compendio de símbolos alfanuméricos junto con algunos operadores aritméticos. Contamos con letras tanto en minúsculas como en mayúsculas, todas ellas pertenecientes al alfabeto inglés, pues la ñ, cuando menos en nuestro caso, no aparece por ningún lado, esto a pesar de que nosotros enviamos nuestro mensaje en español. Tenemos además, dígitos en el rango de 0-9 y los operadores aritméticos o símbolos +, / y =.
Todo el mensaje cifrado se presenta en forma de texto ilegible y además, aunque hay partes del texto que se asemejan a palabras reconocibles (LEMUS, WEB, WORE, etc.), no podemos dar fe de que en efecto sean palabras con algún significado en concreto y no de que se trate de simples combinaciones de caracteres que coinciden con palabras reconocibles, sin su significado. Vemos que la estructura del cifrado tanto del mensaje recibido como del enviado, en ambos casos comienza con $wcFMAz$, por ende sospechamos que esto podría servir como una etiqueta importante dentro del código. Cuando enviamos un texto sin imagen, tiene la misma estructura el cifrado que al mandar texto junto con imagen, sólo cambia el hecho de que aparece el archivo adjunto como "*nombrepng.png*" con la etiqueta encrypted file y esta no es accesible si no se dispone de la clave adecuada. Los mensajes cifrados cuentan con las etiquetas BEGIN PGP MESSAGE y END PGP MESSAGE para señalar el inicio y fin del mensaje, además de ello, no hay espacios en el texto ilegible, se trata de una cadena continua donde sobre todo hay letras, seguidas en cantidad por números y en última instancia por los operadores ya mencionados. Por último, al inicio del mensaje se nos señala la versión del plugin con el cuál se genero el mensaje cifrado que enviamos/recibimos, esta información nos será útil para poder descifrar la información recibida en caso de no tener detalles mayores sobre su procedencia.

5. Campos dentro de una llave pública

Los campos comunes que se pueden encontrar al analizar una llave pública con pgpdump incluyen:

1. **Versión de la llave:** Indica la versión del estándar OpenPGP utilizado para crear la llave.
2. **ID de la llave:** Es un identificador único asociado a la llave pública.
3. **Algoritmo de cifrado:** El tipo de algoritmo utilizado para cifrar datos con la llave pública.
4. **Fecha de creación:** La fecha en la que se creó la llave.
5. **Fecha de expiración:** Si la llave tiene una fecha de expiración establecida.
6. **Usuario asociado:** El nombre o dirección de correo electrónico asociado a la llave.
7. **Firma digital:** Información sobre las firmas digitales asociadas a la llave.
8. **Subpaquetes:**Información adicional sobre subpaquetes de la llave, como subllaves o capacidades especiales.

Para analizar estos campos con pgpdump utilizamos la página web `https://www.lirnberger.com/tools/pgpdump/`, donde al analizar nuestra public key obtenemos éstos resultados:
Donde podemos describir brevemente cada sección que se muestra como:

```
New: Public Key Packet(tag 6)(525 bytes)
        Ver 4 - new
        Public key creation time - Sun Feb 18 17:09:08 CET 2024
        Pub alg - RSA Encrypt or Sign(pub 1)
        RSA n(4096 bits) - ...
        RSA e(17 bits) - ...
New: User ID Packet(tag 13)(50 bytes)
        User ID - Abraham Jiménez Reyes <jimeneza@ciencias.unam.mx>
New: Signature Packet(tag 2)(586 bytes)
        Ver 4 - new
        Sig type - Generic certification of a User ID and Public Key packet(0x10).
        Pub alg - RSA Encrypt or Sign(pub 1)
        Hash alg - SHA256(hash 8)
        Hashed Sub: signature creation time(sub 2)(critical)(4 bytes)
                Time - Sun Feb 18 17:09:08 CET 2024
        Hashed Sub: preferred symmetric algorithms(sub 11)(3 bytes)
                Sym alg - AES with 256-bit key(sym 9)
                Sym alg - AES with 128-bit key(sym 7)
                Sym alg - AES with 192-bit key(sym 8)
        Hashed Sub: issuer key ID(sub 16)(critical)(8 bytes)
                Key ID - 0x2828184EE1C2218B
        Hashed Sub: preferred hash algorithms(sub 21)(2 bytes)
                Hash alg - SHA256(hash 8)
                Hash alg - SHA512(hash 10)
        Hashed Sub: preferred compression algorithms(sub 22)(3 bytes)
                Comp alg - Uncompressed(comp 0)
                Comp alg - ZLIB <RFC1950>(comp 2)
                Comp alg - ZIP <RFC1951>(comp 1)
        Hashed Sub: primary User ID(sub 25)(1 bytes)
                Primary - Yes
        Hashed Sub: key flags(sub 27)(critical)(1 bytes)
                Flag - This key may be used to certify other keys
                Flag - This key may be used to sign data
        Hashed Sub: features(sub 30)(1 bytes)
                Flag - Modification detection (packets 18 and 19)
        Hashed Sub: unknown(sub 33)(21 bytes)
        Hash left 2 bytes - b7 fb
        RSA m^d mod n(4095 bits) - ...
                -> PKCS-1
New: Public Subkey Packet(tag 14)(525 bytes)
        Ver 4 - new
        Public key creation time - Sun Feb 18 17:09:08 CET 2024
        Pub alg - RSA Encrypt or Sign(pub 1)
        RSA n(4096 bits) - ...
        RSA e(17 bits) - ...
New: Signature Packet(tag 2)(566 bytes)
        Ver 4 - new
        Sig type - Subkey Binding Signature(0x18).
        Pub alg - RSA Encrypt or Sign(pub 1)
        Hash alg - SHA256(hash 8)
        Hashed Sub: signature creation time(sub 2)(critical)(4 bytes)
                Time - Sun Feb 18 17:09:08 CET 2024
        Hashed Sub: issuer key ID(sub 16)(critical)(8 bytes)
                Key ID - 0x2828184EE1C2218B
        Hashed Sub: key flags(sub 27)(critical)(1 bytes)
                Flag - This key may be used to encrypt communications
                Flag - This key may be used to encrypt storage
        Hashed Sub: unknown(sub 33)(21 bytes)
        Hash left 2 bytes - 1c 89
        RSA m^d mod n(4095 bits) - ...
                -> PKCS-1
```

- *Public Key Packet:* Se muestra la información de la clave pública RSA utilizada para cifrar o firmar.
- *User ID Packet:* Contiene la identificación del usuario asociado a la clave pública.
- *Signature Packet:* Detalles de la firma realizada sobre la clave pública y el ID de usuario. Incluye información sobre algoritmos preferidos, marcas de clave, funciones y más.
- *Public Subkey Packet:* Similar a la clave pública principal, pero esta es una subclave.
- *Signature Packet:* Firma asociada a la subclave, con detalles sobre el tipo de firma, algoritmos utilizados y más.

6. Conclusión

En conclusión, podemos afirmar de cuanta relevancia posee tener buenas prácticas de seguridad informática y saber como proteger mejor nuestros datos e información privada pues hemos explorado, investigado y aprendido todo lo relacionado con el sistema PGP (Pretty Good Privacy) desde su fecha de creación, instalación, uso, hasta las diferencias que hay entre texto claro y cifrado junto con los campos que conforman una llave pública. Esta herramienta es una de tantas que nos ofrece confidencialidad en internet cada que usamos nuestro correo electrónico, gracias al cifrado de mensajes. No obstante, siempre hay que considerar la existencia de vulnerabilidades que puede sufrir cualquier sistema de seguridad, por ejemplo ataques frecuentes como lo son MintM, así que se recomienda tomar precauciones y medidas adicionales pero necesarias para mitigar el daño y/o robo de datos personales, financieros o susceptible puesto que todo usuario en la red tiene derecho al resguardo de su información.

7. Referencias

- Freda, Anthony, (27 de enero de 2023). ¿Qué es el cifrado del correo electrónico?, AVG website `https://www.avg.com/es/signal/email-encryption`
- Publico, Ricky, (20 de marzo de 2017). ¿Qué es S/MIME y cómo funciona?, Global sign `https://www.globalsign.com/es/blog/what-is-s-mime`
- Carvajal, José Manuel, (20 de diciembre de 2022). Gmail mejora la seguridad en tus correos con cifrado de extremo a extremo, Computer hoy `https://computerhoy.com/google/gmail-mejora-seguridad-correos-cifrado-extremo-extremo-1172784`
- Lirnberger. (s.f.). PGPdump: A PGP packet visualizer. Recuperado de `https://www.lirnberger.com/tools/pgpdump/`
- Cloudflare. (s.f.). How does public key encryption work? Recuperado de `https://www.cloudflare.com/es-es/learning/ssl/how-does-public-key-encryption-work/`
- Buckbee, M. (2020, abril 6). What is PGP encryption and how does it work? Varonis.com. Recuperado de `https://www.varonis.com/blog/pgp-encryption`