

Práctica 2 - Llaves públicas

Equipo Caifanes

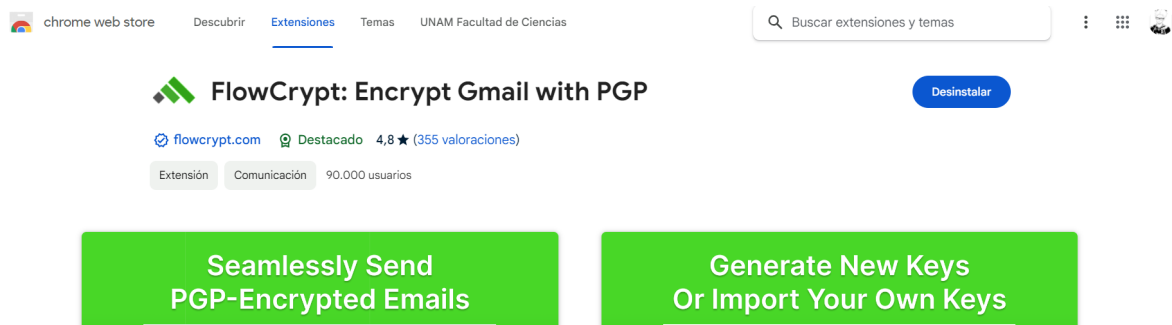
Integrantes

- Díaz Tinoco Gisel Maite (317020326)
- Vázquez González Melissa (317209468)
- Hernández Rojas Saúl Alejandro (315304433)
- Palma López Rossana (312047890)

Desarrollo

Instalación de Flowcrypt

La extensión en sí es muy fácil de instalar, lo único que se hizo fue buscar flowcrypt desde el navegador de Chrome e instalar:



Creación de la llave pública

Se nos pide una frase para poder proteger nuestros correos encriptados, escogimos una larga para que sea más segura.



Set Up FlowCrypt



Choose pass phrase to protect your encrypted emails. [choosing secure pass phrases](#)

..... show

GREAT (time to crack: centuries)

..... show

☐ Remember the pass phrase after closing the browser

☒ Back up encrypted private key in inbox (recommended)

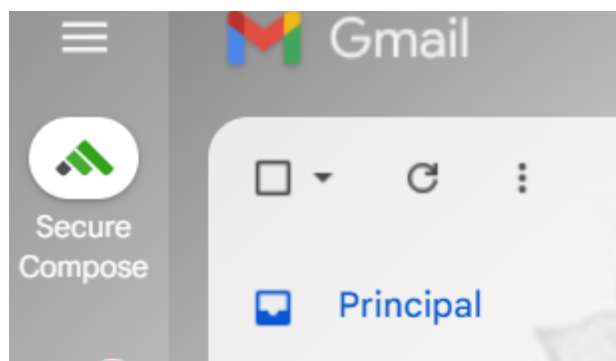
☒ Submit corresponding pubkey to FlowCrypt Attester (recommended)

Encryption key type: RSA 4096bit

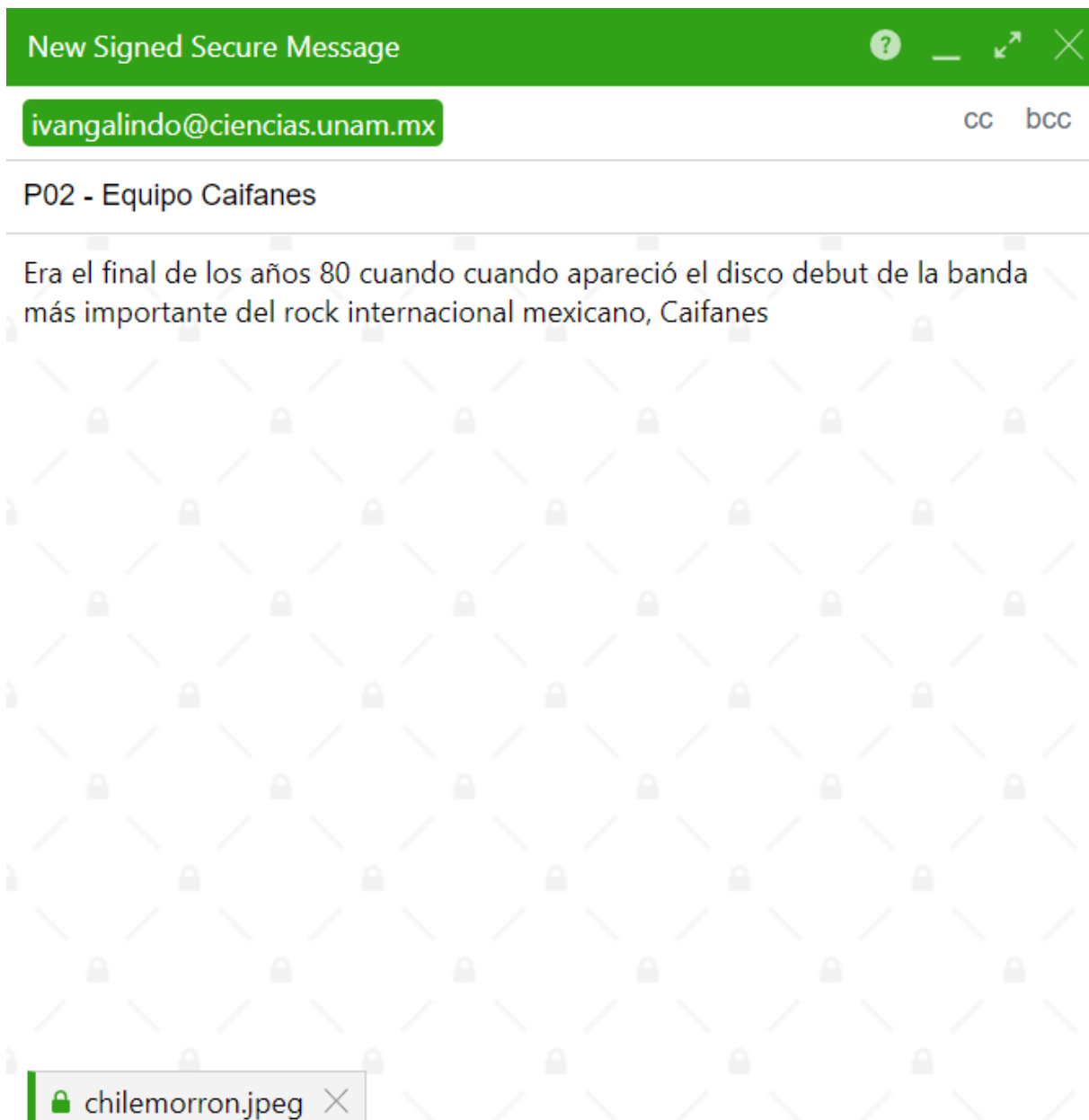
CREATE AND SAVE

Después de crearla, se nos muestra la frase por si queremos anotarla para no olvidarla más adelante.

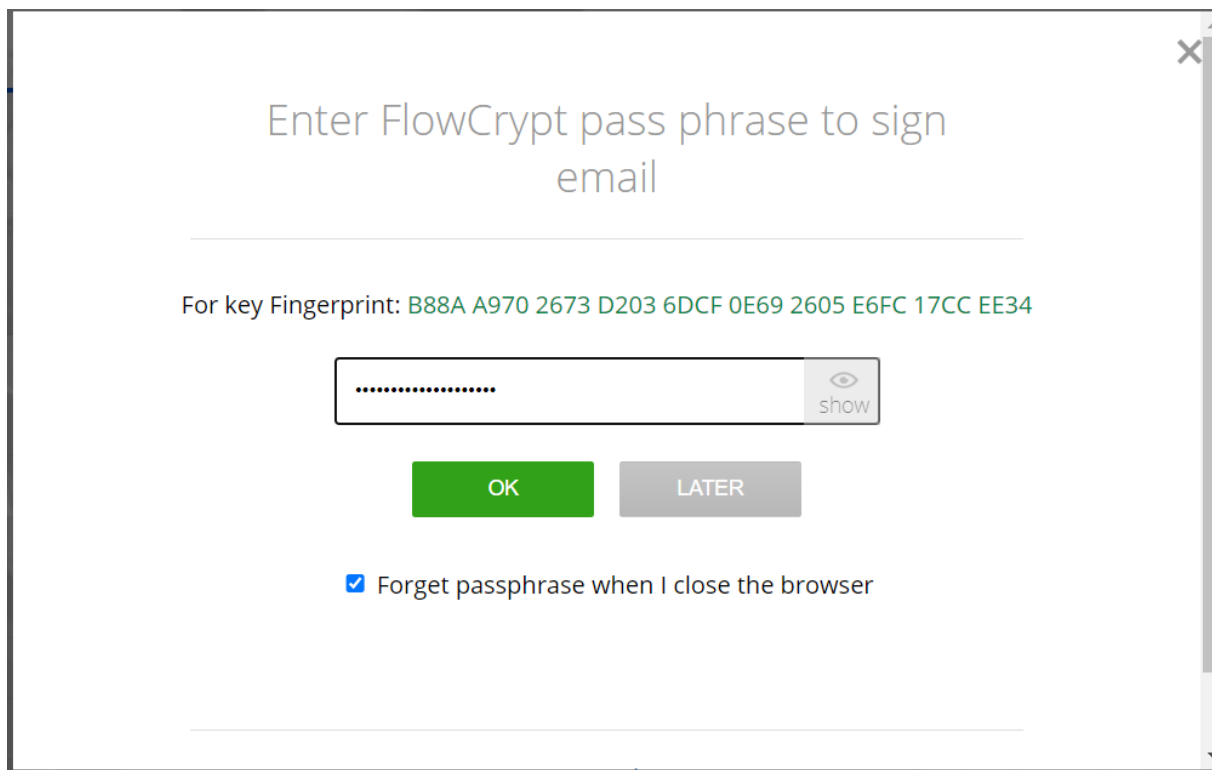
Notamos que a partir de aquí, en gmail nos aparece el siguiente símbolo que se usa para cuando queramos enviar correos encriptados:



Al inicio no sabíamos cómo agregar a Ivan al correo o cómo usar su llave, pero gracias a una ayuda rápida brindada por el siguiente artículo, lo añadimos como contacto desde los *Additional Settings* de FlowCrypt, esto se logra pasándole el archivo de su llave que descargamos desde la carpeta de drive que estamos usando de repositorio. De esta manera, cuando ya en Gmail ponemos en *Secure Compose* nos sugiere su correo y podemos comenzar a redactar el correo y adjuntamos una imagen como se nos especificó en las instrucciones:



Al terminar de redactar, se nos pide ingresar la frase que establecimos al inicio para poder encriptar el correo y mandarlo:

A screenshot of a web browser window showing a dialog box for entering a FlowCrypt pass phrase. The dialog has a title bar with a close button (X) in the top right corner. The main text reads "Enter FlowCrypt pass phrase to sign email". Below this is a horizontal line. Then, it says "For key Fingerprint: B88A A970 2673 D203 6DCF 0E69 2605 E6FC 17CC EE34". There is a text input field with a masked password "....." and a "show" button with an eye icon. Below the input field are two buttons: a green "OK" button and a grey "LATER" button. At the bottom, there is a checkbox labeled "Forget passphrase when I close the browser" which is checked.

Enter FlowCrypt pass phrase to sign email

For key Fingerprint: B88A A970 2673 D203 6DCF 0E69 2605 E6FC 17CC EE34

..... show

OK LATER

☒ Forget passphrase when I close the browser

A los pocos minutos recibimos respuesta de Ivan (muy eficiente, por cierto) con las siguientes preguntas:

¡Hola Caifanes! ¿Cuál es su canción favorita del grupo? Les dejo las preguntas que tienen que pensar, investigar y contestar, cualquier duda estoy al pendiente. ¡Saludos!

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

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

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

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

Preguntas y respuestas:

1. ¿Cuál es su canción favorita del grupo?

Saúl: "No dejes que..." Porque sale en la peli La vida inmoral de la pareja ideal y me gusta mucho.

Maite: "Maténme porque me muero", no hay mucho razonamiento tras de ello, nada más me gusta jaja

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

Si alguien tiene acceso a una llave privada ajena, también tiene acceso a los mensajes que se encriptaron con su respectiva llave pública.

Se tiene que revocar el certificado asociado a las llaves, de ese modo las personas que conocían la llave pública son notificadas que esta ha sido revocada y la llave privada ha sido comprometida.

Finalmente se genera un nuevo par de llaves. [1] [2]

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

En un ambiente donde es posible compartir libremente las llaves a través de servidores públicos. Ya que alguien puede pretender ser el destinatario usando su nombre o ID, y proporcionando la llave del impostor. El mensaje encriptado llegaría a la persona equivocada.

Para prevenir ser interceptados, se debe asegurar que la llave pública del destinatario es en realidad suya. Es recomendable usar llaves solo de personas con las que se realizó el intercambio en persona. Si se obtuvo la llave digitalmente, se verifica su autenticidad con certificados. [1]

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

Respuesta Pregunta 3 (Rossana)

Cuando haces una búsqueda en Google con lo siguiente ¿Outlook cifra los emails? al parecer encuentras una entrada de la propia Microsoft Support donde te muestran como realizar la configuración manualmente del cifrado de los correos electrónicos a continuación cito cuales son los pasos a seguir:

Requerimientos especiales:

- Suscripción a Microsoft 365
- Certificado de firma

Configuración del certificado para Microsoft 365:

Vamos al menú de Archivo

seleccionamos lo siguiente conforme vaya apareciendo, primero Opciones, de este menú Centro de Confianza y de este Configuración del Centro de Confianza

dirigirse a la opción Email Seguridad y

en el menú Correo Electrónico Cifrado seleccionar Configuración,

Seleccionar Certificados y algoritmos

Del menú Elegir seleccionamos el certificado S/MIME

Finalizamos la configuración dando clic en Aceptar

Cifrado de mensajes de correo

Para Office Insider

Elegimos Opciones y damos clic en Cifrar y seleccionamos la opción Cifrar con S/MIME

Para Outlook 2019 y 2016

Del menú Opciones elegir Permisos

Redactamos nuestro correo electrónico y enviamos

Si lo que deseamos es solo cifrar un mensaje hacemos lo siguiente

Vamos a la opción Propiedades del menú Archivo cuando estemos redactando el correo que queremos cifrar, seleccionamos Configuración de seguridad y de este menú marcamos la casilla Cifrar contenido del mensaje y datos adjuntos, continuamos con la redacción y enviamos

Para cifrar todos los mensajes salientes de nuestra cuenta tendremos que ir al menú de Archivo y buscar el sub-menu de Opciones, después Centro de confianza y elegir Configuración del centro de confianza, en este ultimo ir a

Seguridad de Email dirigírnos a la opción Correo electrónico cifrado y marcar la casilla que dice Cifrar contenido datos adjuntos para los mensajes salientes

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

No, Outlook por defecto utiliza el cifrado de mensajes de Microsoft Purview, las extensiones seguras multipropósito al correo de Internet (S/MIME) e Information Rights Management (IRM). [3]

Gmail también usa S/MIME por defecto, sin embargo, puedes usar la encriptación de cliente (CSE), que es la manera que tiene de llamarle a E2EE. [4]

Analizar con pgpdump una de sus llaves públicas e investigar y redactar qué significan los diferentes campos.

New: Public Key Packet(tag 6)(525 bytes)

Ver 4 - new

Public key creation time - Sun Feb 18 21:54:00 CST 2024

Pub alg - RSA Encrypt or Sign(pub 1)

RSA n(4096 bits) - ...

RSA e(17 bits) - ...

New: User ID Packet(tag 13)(49 bytes)

User ID - Gisel Maite Díaz Tinoco

digit@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 21:54:00 CST 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 - 0x2605E6FC17CCEE34
 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: issuer fingerprint(sub 33)(21 bytes)
 v4 - Fingerprint - b8 8a a9 70 26 73 d2 03 6d cf 0e 69 26 05 e6 fc 17 cc ee 34
 Hash left 2 bytes - 6b cd
 RSA $m^d \bmod n$ (4093 bits) - ...
 → PKCS-1
 New: Public Subkey Packet(tag 14)(525 bytes)
 Ver 4 - new
 Public key creation time - Sun Feb 18 21:54:00 CST 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 21:54:00 CST 2024
 Hashed Sub: issuer key ID(sub 16)(critical)(8 bytes)
 Key ID - 0x2605E6FC17CCEE34
 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: issuer fingerprint(sub 33)(21 bytes)

v4 - Fingerprint - b8 8a a9 70 26 73 d2 03 6d cf 0e 69 26 05 e6 fc 17 cc ee 34

Hash left 2 bytes - 92 a5

RSA $m^d \bmod n$ (4096 bits) - ...

→ PKCS-1

- **Public Key**

- **Ver 4 - new** indica que la versión del paquete de la clave pública es 4
- **New: Public Key Packet(tag 6)(525 bytes)** indica el tamaño del paquete
- **Public key creation time:** fecha y hora en que se creó la llave pública.
- **Pub alg - RSA Encrypt or Sign(pub 1):** Es el algoritmo utilizado (RSA) para cifrado o firma.

- **User ID:** El nombre y correo asociados a la llave pública.

- **Signature**

- **Hash alg - SHA256(hash 8):** Es el algoritmo que se utilizó para generar la firma
- **Signature creation time:** Fecha y hora en que se creó la firma.
- **Flags:** Indica los permisos asociados

- **Public Subkey:** similar a la llave pública

Referencias

[1] How PGP works. <https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html#p10>

[2] Lenovo Docs. Compromised private keys. https://pubs.lenovo.com/imm2/nn1jo_c_compromisedprivatekeys.html#:~:text=A private key is compromised,the sender of the data.

[3] Cifrado de correo electrónico. <https://learn.microsoft.com/es-es/purview/email-encryption>

[4] Más información sobre la encriptación del cliente de Google. <https://support.google.com/mail/answer/13317990?hl=es-419&sjid=16031715688073961026-NC>

Email Encryption in Transit. <https://support.google.com/mail/answer/6330403?hl=en#zippy=%2Csmime-enhanced-encryption>

Cifrar mensajes de correo. https://support.microsoft.com/es-es/office/cifrar-mensajes-de-correo-373339cb-bf1a-4509-b296-802a39d801dc#ID0EBBD=Newer_versions