Carl Cortez

CIS 628

Chapter 6 Applied Cryptography

Lab 1

Lab Exercise 6.01: Apple vs. FBI

As a consumer of Apple products and a former applicant to work at the FBI, I was fascinated at the quarrel between the two powerhouses. Both sides seemed to have gotten their hands dirty in this event. Apple, aware that there is potential evidence within their devices. The FBI, deciding to beg for forgiveness after they had asked for permission to view Farook's iPhone. Both parties are at fault for at least one thing.

I'm split between which party I side with. I applaud Apple for advocating user privacy even if the contents on Farook's iPhone were not revealing or helpful in the case. I commend the FBI for problem solving their way through a situation that they needed outside help for. From a business perspective, it's nice to know that the phones listening to us have some core privacy policies established. The FBI looks a bit outdated to me if they're asking for permission to snoop around on a format they don't have control over.

Although I may be split on which side is in the right, I know that this is a big case to learn from. As I upload more to my iCloud, I ponder how this information may be accessed by outside parties that I don't know about. The FBI has punctured a hole in Apple's security which I'm optimistic about. If more data and text are stored on phones, the FBI may have an opportunity to close cases quicker than before. I look forward to seeing more problem solving like this from the FBI and improvements in security from Apple.

Lab Exercise 6.02: Australia's Assistance and Access Bill

In 2022, I think that Australia's Assistance and Access Bill is a luxury for all parties to have. With digital information floating around everywhere, it's nice to know that malicious & critical information/data can be retrieved easier. As a life-long learner, I think it's great that technology companies are being asked to rethink their product and create intentional holes in their systems for the government. As we saw in the first exercise, some brands are apprehensive on assisting law enforcement with their investigations. For Australia to say that they need these access controls for data/information is a brave and progressive stance for governments.

I believe that the law is reasonable to protect people. If the government is seen as intrusive and manipulative to citizens' data & information, it would be a chaotic circumstance for both parties. The leaders we choose should be professional with the information that we need to share with others. If we give governments a bit more flexibility to protect us with the help of technology companies, I can only hope that they will use this power for good.

This law positions companies to hold firm or work cohesively with governments. Companies may have to ask themselves if they value free speech and privacy more than the safety of their citizens.

This law may push countries to be more controlling with the applications that they allow for use. China to me is an example of too much control over applications and technology for their citizens. That being said, if these laws can be implemented gradually, with general agreement amongst citizens, and in a safe manner, I feel as if citizens will feel safer sharing information online.

Lab Exercise 6.03: To Serve Man

This episode is a great example of what cryptography can accomplish. The investigation of unknown text in an effort to understand what is being said or intended. Despite the alien passing the lie detector test on their intents for Earth, the texts say something else about their hidden agenda. Decrypting the book is similar to how the FBI wanted to open Farook's iPhone; there's a hidden agenda and we want in!

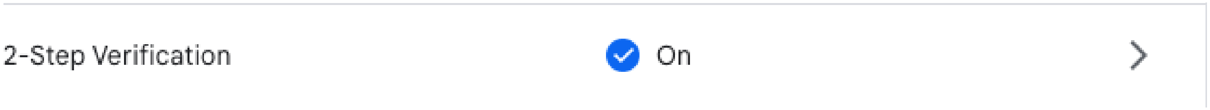
The Simpsons clip that stuck out to me was Lisa Simpson's deciphering of the book title. I related this back to how certain keys are needed to decrypt messages that are being sent. With Lisa's dust blowing as the decryption, she was able to see what was really happening to her family. Although it took effort on Lisa's part to decrypt, she was able to see an alternative message. In the technology world, intercepting messages and decrypting them seems almost as simple as Lisa's efforts.

I also tied this back to the FBI vs. Apple story in Task 1. I viewed the aliens from The Twilight Zone and The Simpsons as the Apple company. With information and data at their fingertips, the aliens and Apple have a certain agenda they would *prefer* to follow; user security for Apple and eating good for the aliens. On the flip side, I see Lisa as the FBI; needing answers/information and willing to do whatever is needed to see it through. Both parties oppose each other and you can debate which side is right or wrong.

Lab Exercise 6.04: E-mail Cryptography

Pre-Step 1

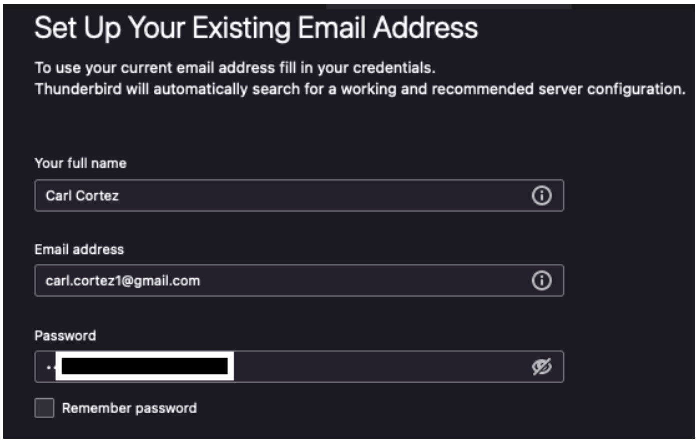
I turned on two step verification for my e-mail.



2-Step Verification ✓ On

Step 1 A-G

I've downloaded Thunderbird, am logging in with my gmail account, and have unchecked remember password.



Set Up Your Existing Email Address

To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.

Your full name: Carl Cortez

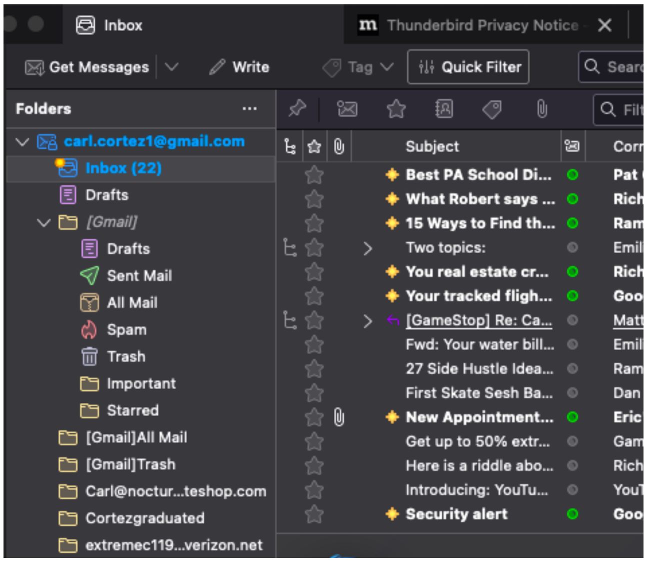
Email address: carl.cortez1@gmail.com

Password: [redacted]

□ Remember password

Step 1 H-J

I kept the default settings, clicked done, used 2-Step Verification, and have gotten to my inbox on Thunderbird.



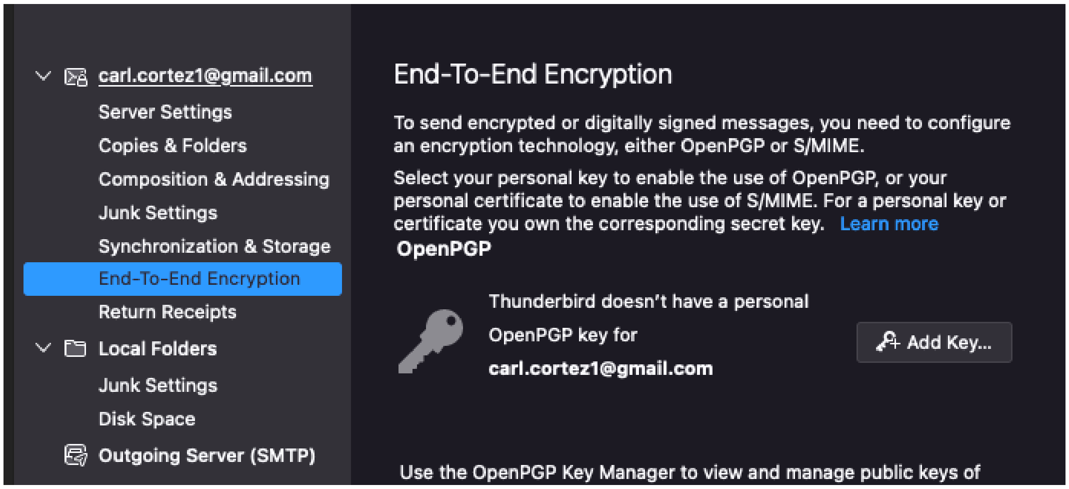
Folders

- carl.cortez1@gmail.com
  - Inbox (22)
  - Drafts
  - [Gmail]
    - Drafts
    - Sent Mail
    - All Mail
    - Spam
    - Trash
    - Important
    - Starred
  - [Gmail]All Mail
  - [Gmail]Trash
  - Carl@noctur...teshop.com
  - Cortezgraduated
  - extremec119...verizon.net

Subject	Corr
Best PA School Di...	Pat
What Robert says ...	Rich
15 Ways to Find th...	Ram
Two topics:	Emil
You real estate cr...	Rich
Your tracked fligh...	Goo
[GameStop] Re: Ca...	Matt
Fwd: Your water bill...	Emil
27 Side Hustle Idea...	Ram
First Skate Sesh Ba...	Dan
New Appointment...	Eric
Get up to 50% extr...	Gam
Here is a riddle abo...	Rich
Introducing: YouTu...	YouT
Security alert	Goo

Step 2 A-D

From the Settings tab, I clicked on end-to-end encryption



End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

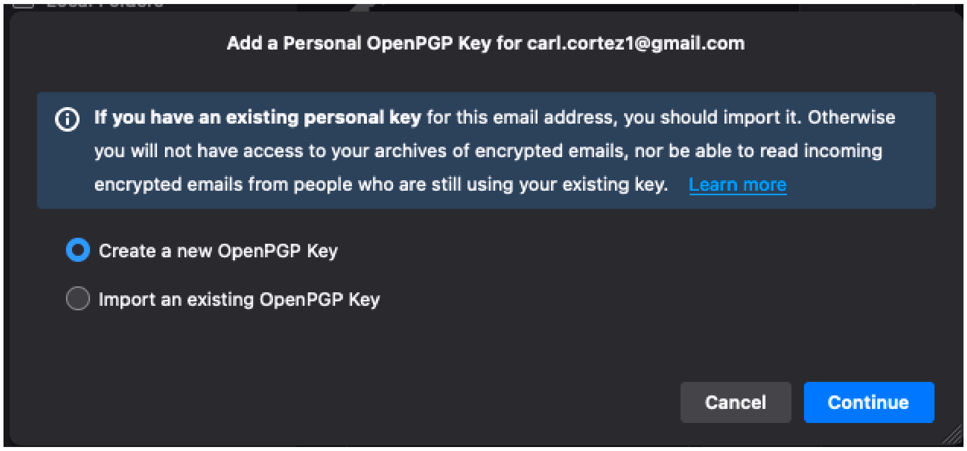
Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more

OpenPGP

Thunderbird doesn't have a personal OpenPGP key for **carl.cortez1@gmail.com**

Use the OpenPGP Key Manager to view and manage public keys of

Preparing to create a new OpenPGP Key with default button selection.



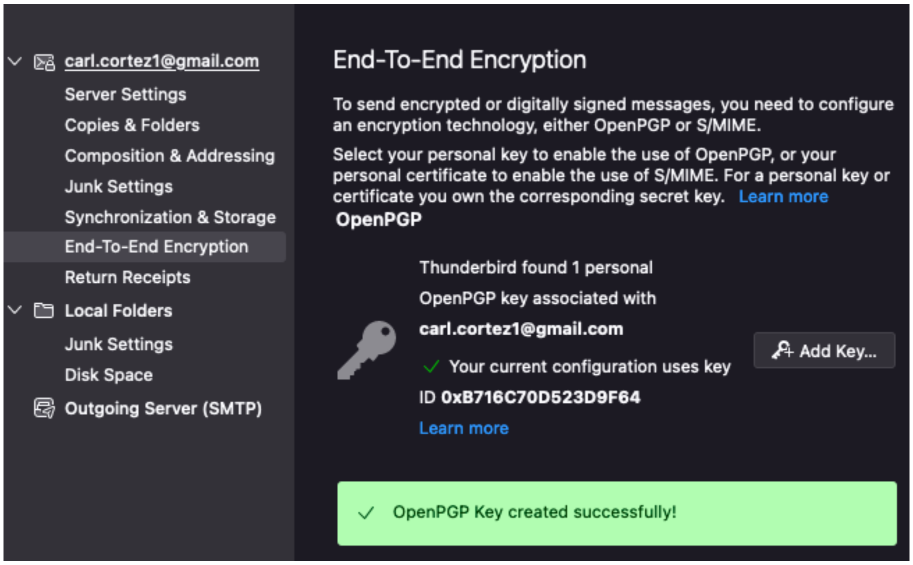
Add a Personal OpenPGP Key for carl.cortez1@gmail.com

If you have an existing personal key for this email address, you should import it. Otherwise you will not have access to your archives of encrypted emails, nor be able to read incoming encrypted emails from people who are still using your existing key. Learn more

● Create a new OpenPGP Key

○ Import an existing OpenPGP Key

I've created the OpenPGP Key!



End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with **carl.cortez1@gmail.com**

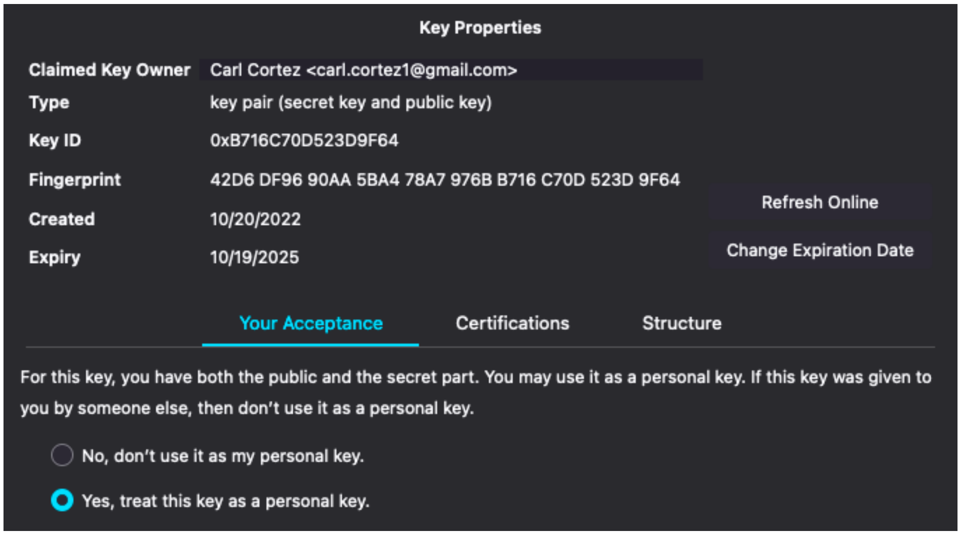
✓ Your current configuration uses key ID **0xB716C70D523D9F64**

Learn more

✓ OpenPGP Key created successfully!

Step 2 E:

Browsing around the Key Properties, exploring the Acceptance, Certifications, and Structure tabs.



Key Properties

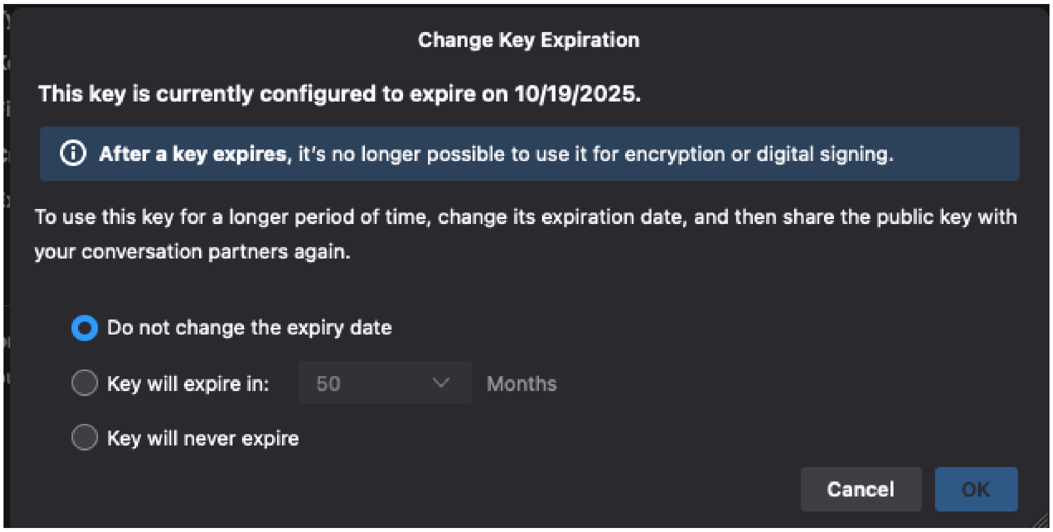
Claimed Key Owner	Carl Cortez <carl.cortez1@gmail.com>
Type	key pair (secret key and public key)
Key ID	0xB716C70D523D9F64
Fingerprint	42D6 DF96 90AA 5BA4 78A7 976B B716 C70D 523D 9F64
Created	10/20/2022
Expiry	10/19/2025

For this key, you have both the public and the secret part. You may use it as a personal key. If this key was given to you by someone else, then don't use it as a personal key.

○ No, don't use it as my personal key.

● Yes, treat this key as a personal key.

Now, taking a peek at the Change Expiration Date choices before exiting.



Change Key Expiration

This key is currently configured to expire on 10/19/2025.

ⓘ **After a key expires,** it's no longer possible to use it for encryption or digital signing.

To use this key for a longer period of time, change its expiration date, and then share the public key with your conversation partners again.

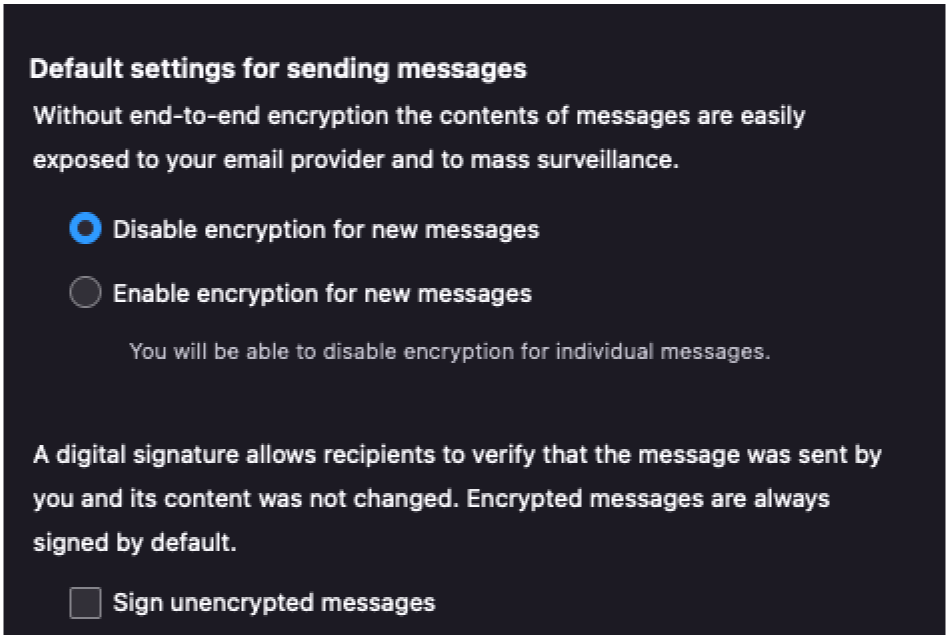
● Do not change the expiry date

○ Key will expire in: 50 Months

○ Key will never expire

Step 2 F:

Back on the End-To-End Encryption page, I've scrolled down to ensure that I've disabled encryption and adding my digital signature by default.



Default settings for sending messages

Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.

● Disable encryption for new messages

○ Enable encryption for new messages

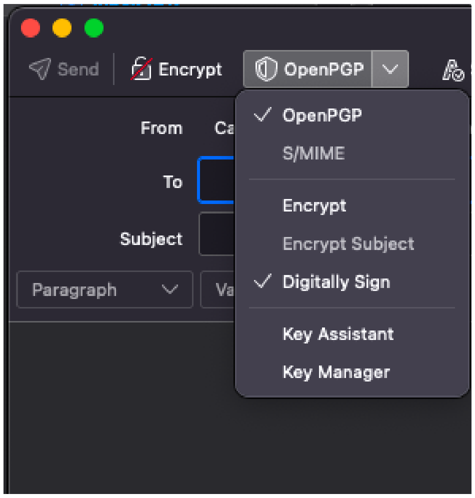
You will be able to disable encryption for individual messages.

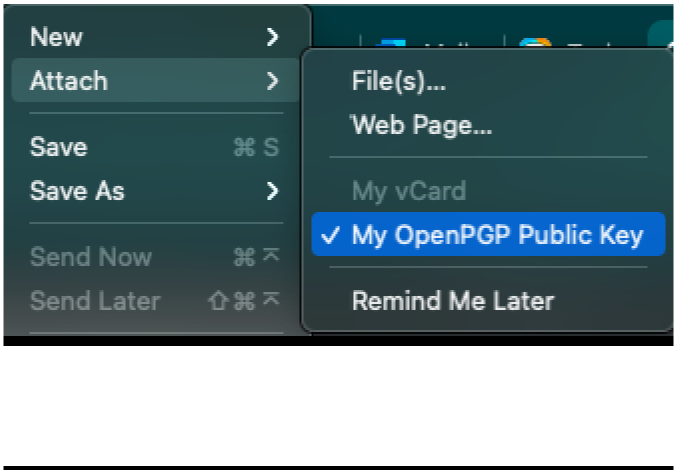
A digital signature allows recipients to verify that the message was sent by you and its content was not changed. Encrypted messages are always signed by default.

□ Sign unencrypted messages

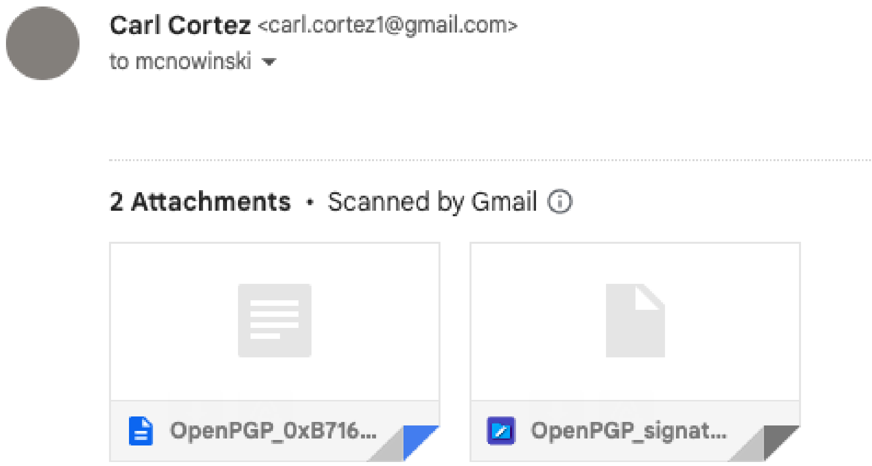
Step3A:

I've created a new email draft, enabled digitally signing and attached my public key. Upon emailing with Professor Weissman, I've been told that the interface has changed since the book's publishing. If there is an error with this work, please email me at cccortez@syr.edu.





Step3B:
I emailed my partner a message with the settings mentioned above.



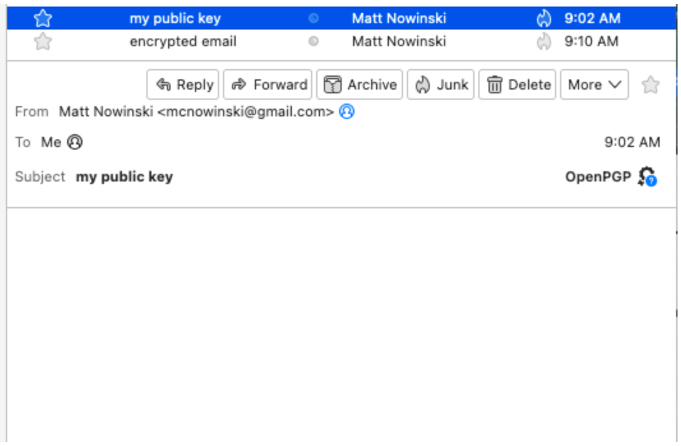
Carl Cortez <carl.cortez1@gmail.com>
to mcnowinski

2 Attachments • Scanned by Gmail

OpenPGP_0xB716...

OpenPGP_signat...

Step 4 A:
Clicking on the email I received, another email, and then back to my partner's email.



my public key	Matt Nowinski	9:02 AM
encrypted email	Matt Nowinski	9:10 AM

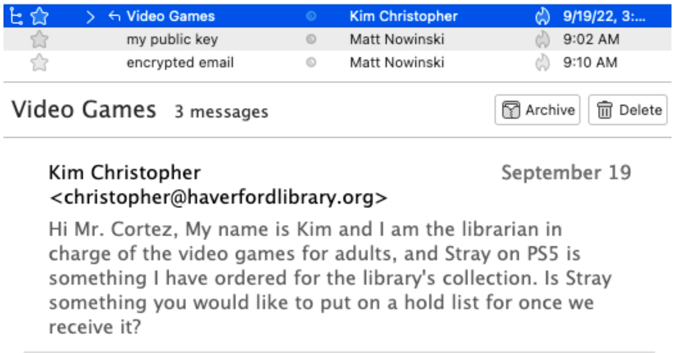
From Matt Nowinski <mcnowinski@gmail.com>

To Me

9:02 AM

Subject **my public key**

OpenPGP



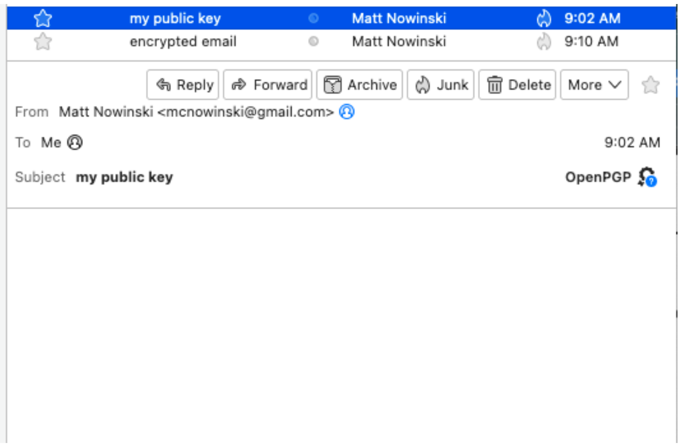
Video Games	Kim Christopher	9/19/22, 3:...
my public key	Matt Nowinski	9:02 AM
encrypted email	Matt Nowinski	9:10 AM

Video Games 3 messages

Kim Christopher <christopher@havefordlibrary.org>

September 19

Hi Mr. Cortez, My name is Kim and I am the librarian in charge of the video games for adults, and Stray on PS5 is something I have ordered for the library's collection. Is Stray something you would like to put on a hold list for once we receive it?



my public key	Matt Nowinski	9:02 AM
encrypted email	Matt Nowinski	9:10 AM

From Matt Nowinski <mcnowinski@gmail.com>

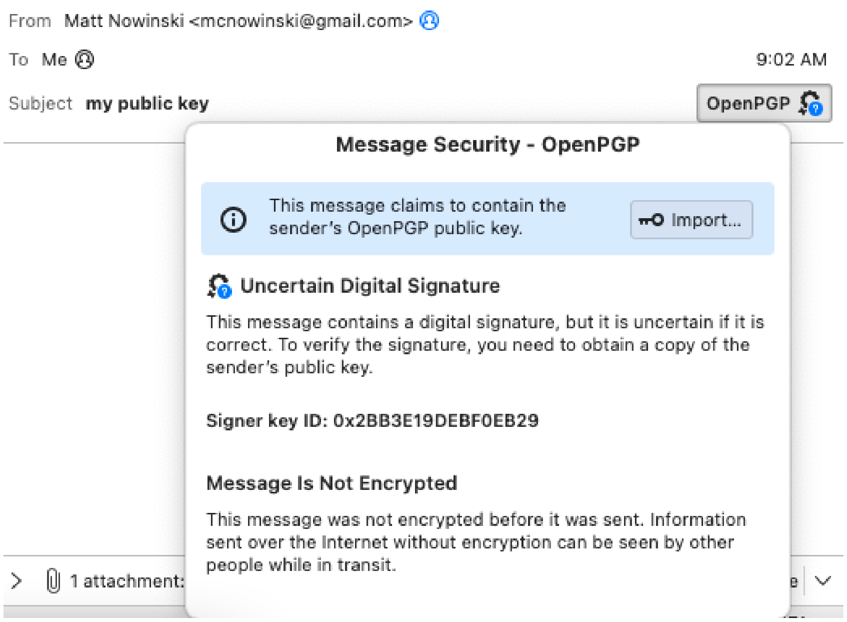
To Me

9:02 AM

Subject **my public key**

OpenPGP

Step4B:



From Matt Nowinski <mcnowinski@gmail.com>

To Me

9:02 AM

Subject **my public key**

Message Security - OpenPGP

This message claims to contain the sender's OpenPGP public key.

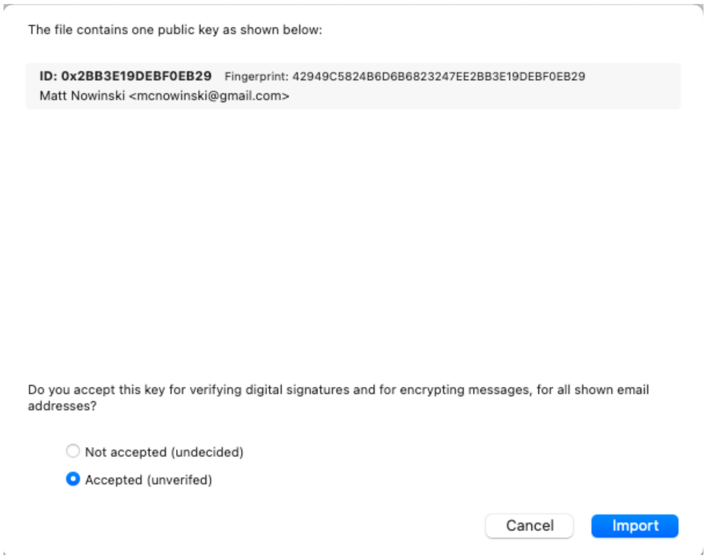
Uncertain Digital Signature

This message contains a digital signature, but it is uncertain if it is correct. To verify the signature, you need to obtain a copy of the sender's public key.

Signer key ID: 0x2BB3E19DEBF0EB29

Message Is Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.



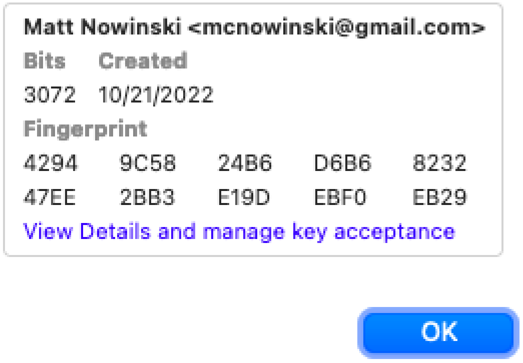
The file contains one public key as shown below:

ID: 0x2BB3E19DEBF0EB29 Fingerprint: 42949C5824B6D6B6823247EE2BB3E19DEBF0EB29
Matt Nowinski <mcnowinski@gmail.com>

Do you accept this key for verifying digital signatures and for encrypting messages, for all shown email addresses?

○ Not accepted (undecided)

● Accepted (unverifed)



Matt Nowinski <mcnowinski@gmail.com>

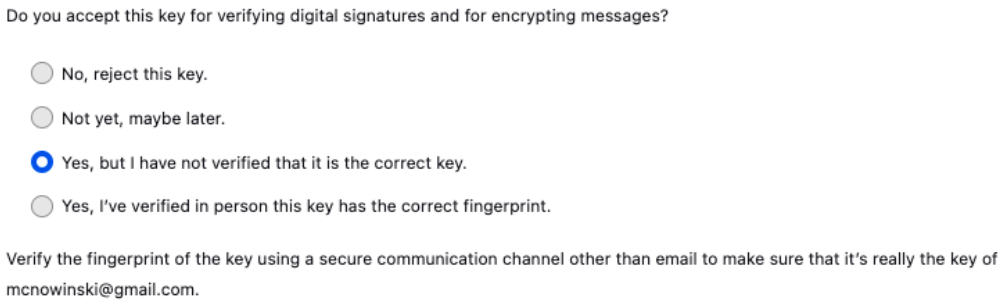
Bits	Created
3072	10/21/2022

Fingerprint

4294	9C58	24B6	D6B6	8232
47EE	2BB3	E19D	EBF0	EB29

View Details and manage key acceptance

Clicking *View Details and manage key acceptance*.



Do you accept this key for verifying digital signatures and for encrypting messages?

○ No, reject this key.

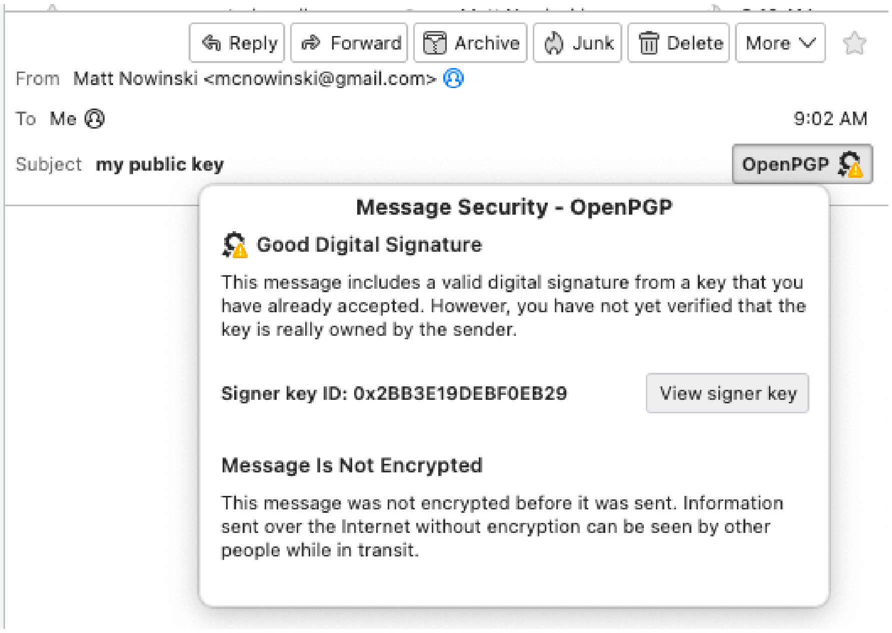
○ Not yet, maybe later.

● Yes, but I have not verified that it is the correct key.

○ Yes, I've verified in person this key has the correct fingerprint.

Verify the fingerprint of the key using a secure communication channel other than email to make sure that it's really the key of mcnowinski@gmail.com.

Reloading the partner email, I notice the OpenPGP button has changed. I see Good Digital Signature with a message that I've yet to verify that the key is really owned by Partner Matt.



From Matt Nowinski <mcnowinski@gmail.com>

To Me

9:02 AM

Subject **my public key**

Message Security - OpenPGP

Good Digital Signature

This message includes a valid digital signature from a key that you have already accepted. However, you have not yet verified that the key is really owned by the sender.

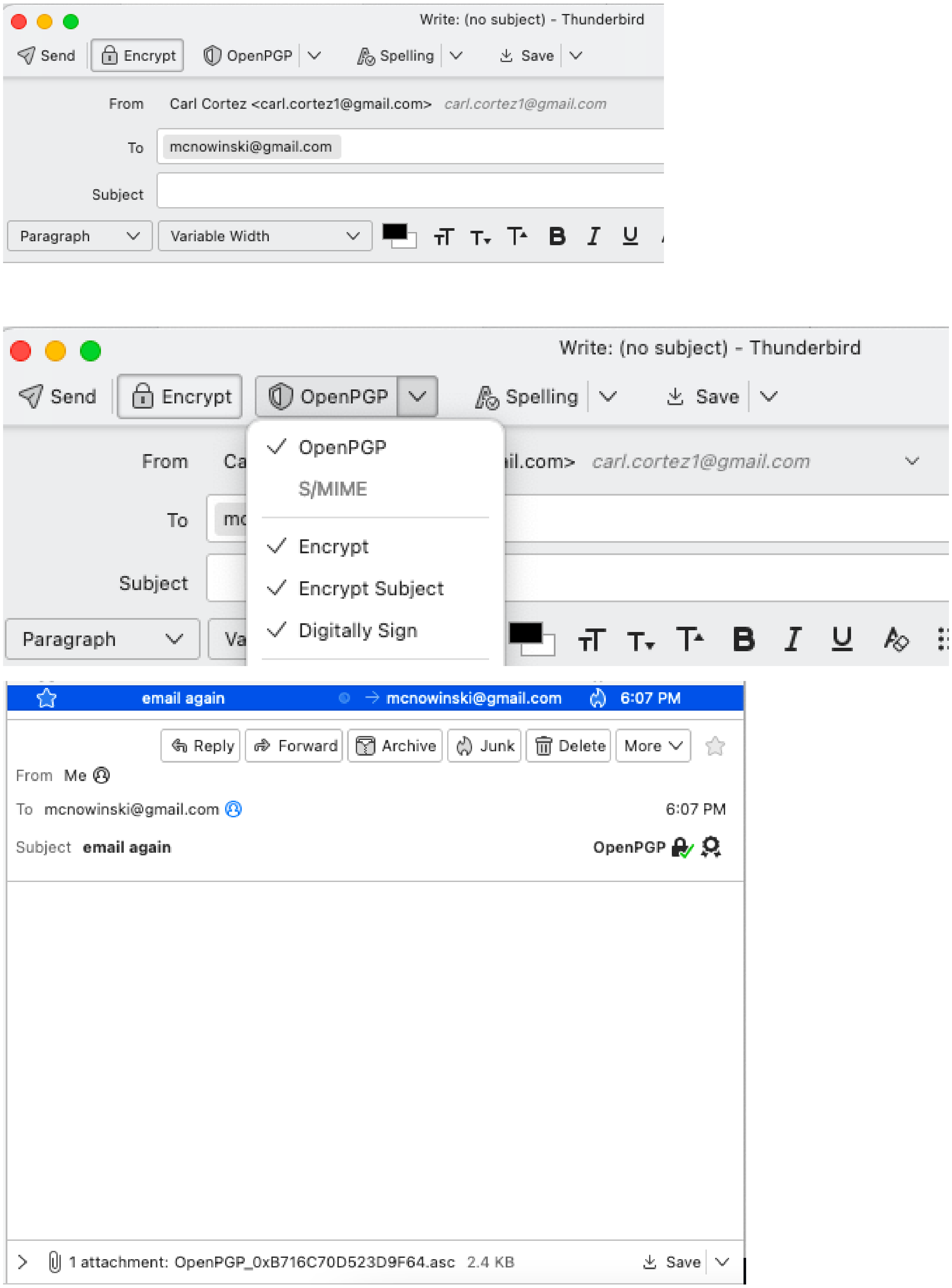
Signer key ID: 0x2BB3E19DEBF0EB29

Message Is Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

<u>Step5A-5C:</u>

Composing a new email to my partner. Including the options require encryption and digitally signing the message. Continuing to send the email.



Write: (no subject) - Thunderbird

From Carl Cortez <carl.cortez1@gmail.com> carl.cortez1@gmail.com

To mcnowinski@gmail.com

Subject

Write: (no subject) - Thunderbird

✓ OpenPGP

S/MIME

✓ Encrypt

✓ Encrypt Subject

✓ Digitally Sign

email again → mcnowinski@gmail.com 6:07 PM

From Me

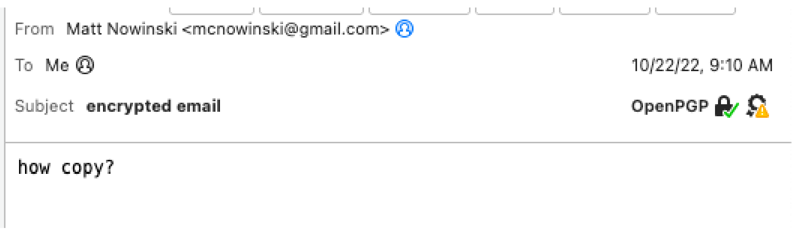
To mcnowinski@gmail.com 6:07 PM

Subject **email again** OpenPGP

1 attachment: OpenPGP_0xB716C70D523D9F64.asc 2.4 KB

Step 6A-6B:

Reloading my partner's email, with a selection in between, to see new status messages.

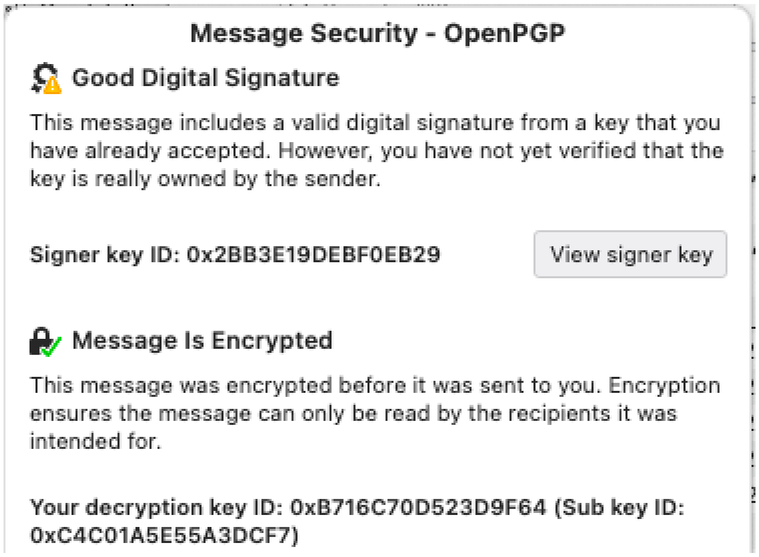


From Matt Nowinski <mcnowinski@gmail.com>

To Me 10/22/22, 9:10 AM

Subject **encrypted email** OpenPGP

```
how copy?
```



Message Security - OpenPGP

Good Digital Signature

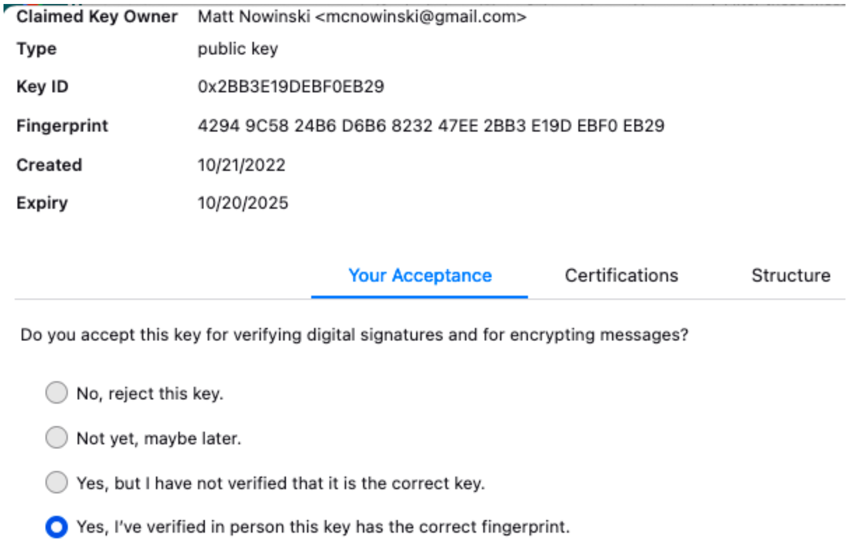
This message includes a valid digital signature from a key that you have already accepted. However, you have not yet verified that the key is really owned by the sender.

Signer key ID: 0x2BB3E19DEBF0EB29

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption ensures the message can only be read by the recipients it was intended for.

Your decryption key ID: 0xB716C70D523D9F64 (Sub key ID: 0xC4C01A5E55A3DCF7)



Claimed Key Owner	Matt Nowinski <mcnowinski@gmail.com>
Type	public key
Key ID	0x2BB3E19DEBF0EB29
Fingerprint	4294 9C58 24B6 D6B6 8232 47EE 2BB3 E19D EBF0 EB29
Created	10/21/2022
Expiry	10/20/2025

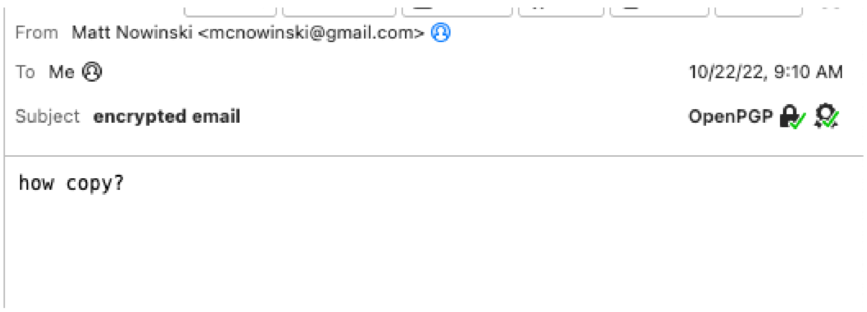
Do you accept this key for verifying digital signatures and for encrypting messages?

○ No, reject this key.

○ Not yet, maybe later.

○ Yes, but I have not verified that it is the correct key.

● Yes, I've verified in person this key has the correct fingerprint.



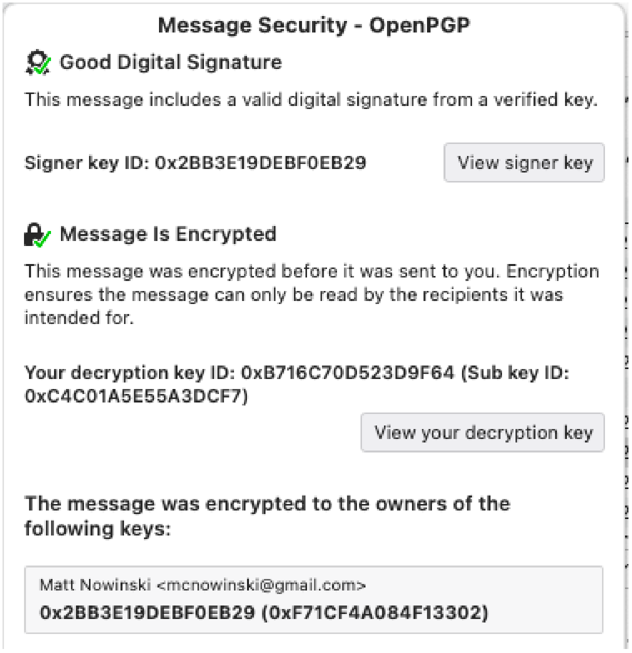
From Matt Nowinski <mcnowinski@gmail.com>

To Me

10/22/22, 9:10 AM

Subject **encrypted email**

```
how copy?
```



Message Security - OpenPGP

Good Digital Signature

This message includes a valid digital signature from a verified key.

Signer key ID: 0x2BB3E19DEBF0EB29

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption ensures the message can only be read by the recipients it was intended for.

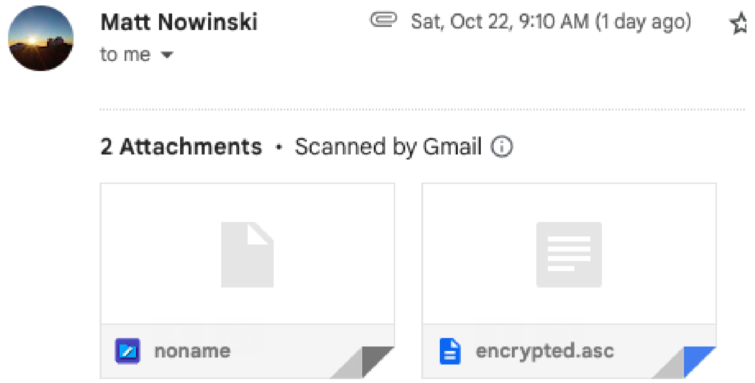
Your decryption key ID: 0xB716C70D523D9F64 (Sub key ID: 0xC4C01A5E55A3DCF7)

The message was encrypted to the owners of the following keys:

Matt Nowinski <mcnowinski@gmail.com>
0x2BB3E19DEBF0EB29 (0xF71CF4A084F13302)

Task 6C:

Heading to google, opening the second email from my partner, and admiring the attachments.



Matt Nowinski

to me

Sat, Oct 22, 9:10 AM (1 day ago)

2 Attachments • Scanned by Gmail

Step 7

a. How does the e-mail look in the web browser compared to how it looks in Thunderbird? Why is this the case?

The web browser version has two attachments instead of one. This is due to the additional attachment.

b. When you encrypted the e-mail to your partner, which key encrypted the e-mail?

The e-mail I sent was encrypted by the session key.

c. When you encrypted the e-mail to your partner, which key encrypted the key that encrypted the e-mail? In other words, which key encrypted your answer to Step 7b?

The session key was encrypted with the public key.

d. When your partner decrypted that e-mail, which key decrypted the e-mail?

The encrypted session key decrypted the e-mail.

e. When your partner decrypted that e-mail, which key decrypted the key that decrypted the e-mail?In other words, which key decrypted your answer to Step 7d?

My partner used their private ey to decrypt the session key.

f. Why did one key encrypt the e-mail and another key encrypt that key?

The key that encrypted the e-mail was encrypted so that only my partner could open the e-mail.

g. When you signed your e-mail to your partner, which key did you use?

I used my private key to sign the e-mail that I sent.

h. When your partner verified your signature, which key did he or she use?

My partner used my public key to verify my signature.
i. How was confidentiality accomplished?

Confidentiality was accomplished because only the sender and reader could see the message.

j. How was integrity accomplished?

Integrity was accomplished because only the sender and reader could change the message.

k. How was nonrepudiation accomplished?

By signing the email with a digital signature, nonrepudiation is accomplished. My partner knows that I sent the email and I'm aware that they received it.

Lab Analysis

1. What is the single biggest takeaway you had from the dispute between Apple and the FBI?

Sometimes, it's better to ask for forgiveness instead of permission.

2. What is the single biggest takeaway you had from Australia's Assistance and Access Bill?

Big companies creating bonds with the government can be a mix of scary, messy, and comforting for their power potential together.

3. What cryptography lesson does The Twilight Zone's "To Serve Man" bring out the best?

The Twilight Zone brings out the idea of owning information that isn't available to just everybody. The aliens were in charge of their agenda and mission while outside groups were trying to disrupt their agenda.

4. Will you use e-mail encryption from this point going forward? Why or why not?

I probably won't encrypt my emails because I don't send important information frequently.
Perhaps, I'll encrypt my text messages instead.

Key Term Quiz

Use the terms from the list to complete the sentences that follow: backdoor decrypt encrypt hash

1. If someone in Australia wants to *encrypt* a message for privacy, the Assistance and Access Bill allows for that message to be intercepted and read.

2. The FBI wanted Apple to build a(n) *backdoor* that would allow them to access an iPhone of a terrorist.

3. The employees of the United States government were trying to *decrypt* the Kanamits' book in The Twilight Zone's "To Serve Man" episode.

4. Signing an e-mail with OpenPGP, like a digital signature on a digital certificate for TLS, involves encrypting a(n) *hash.*