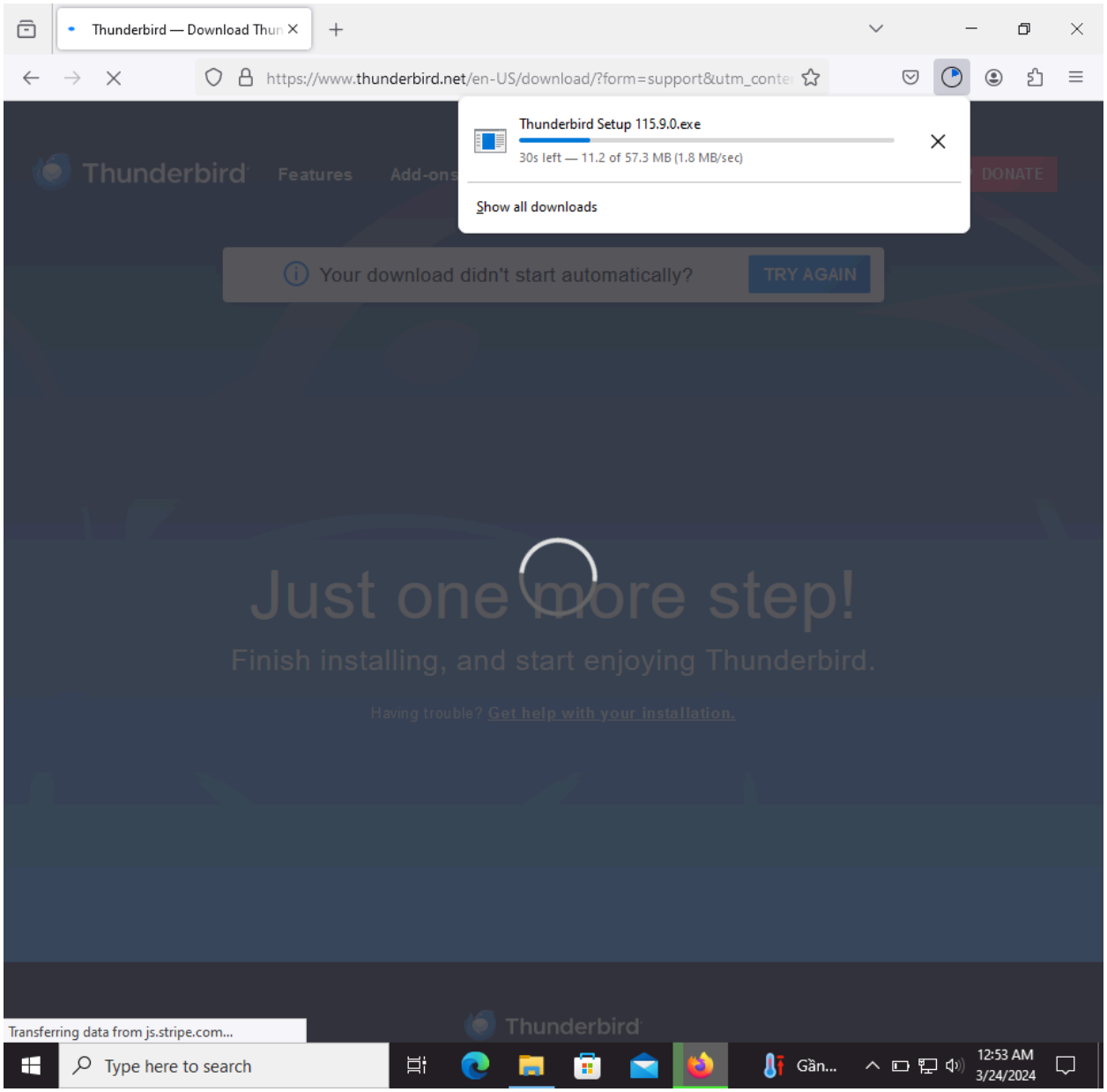
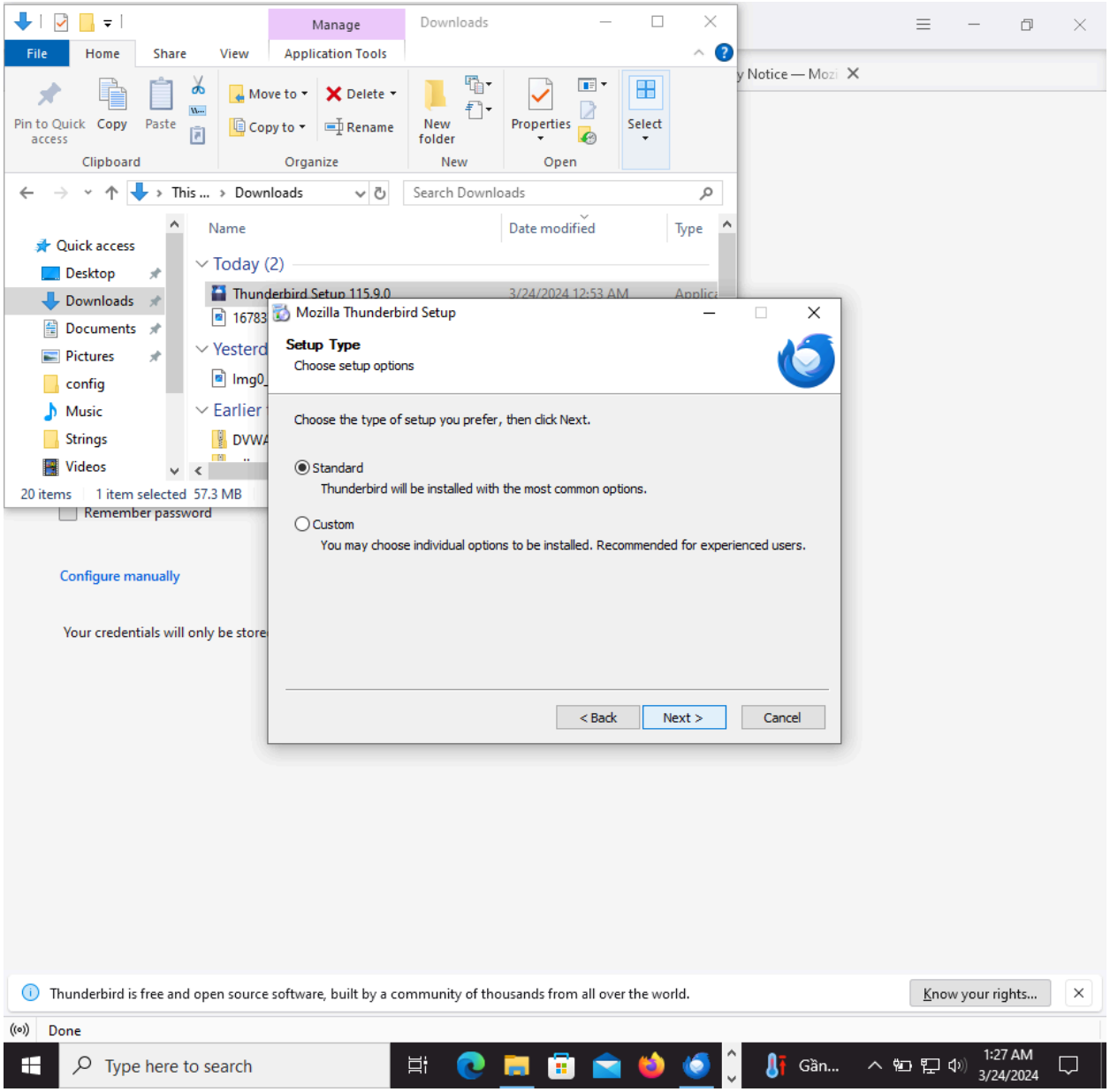
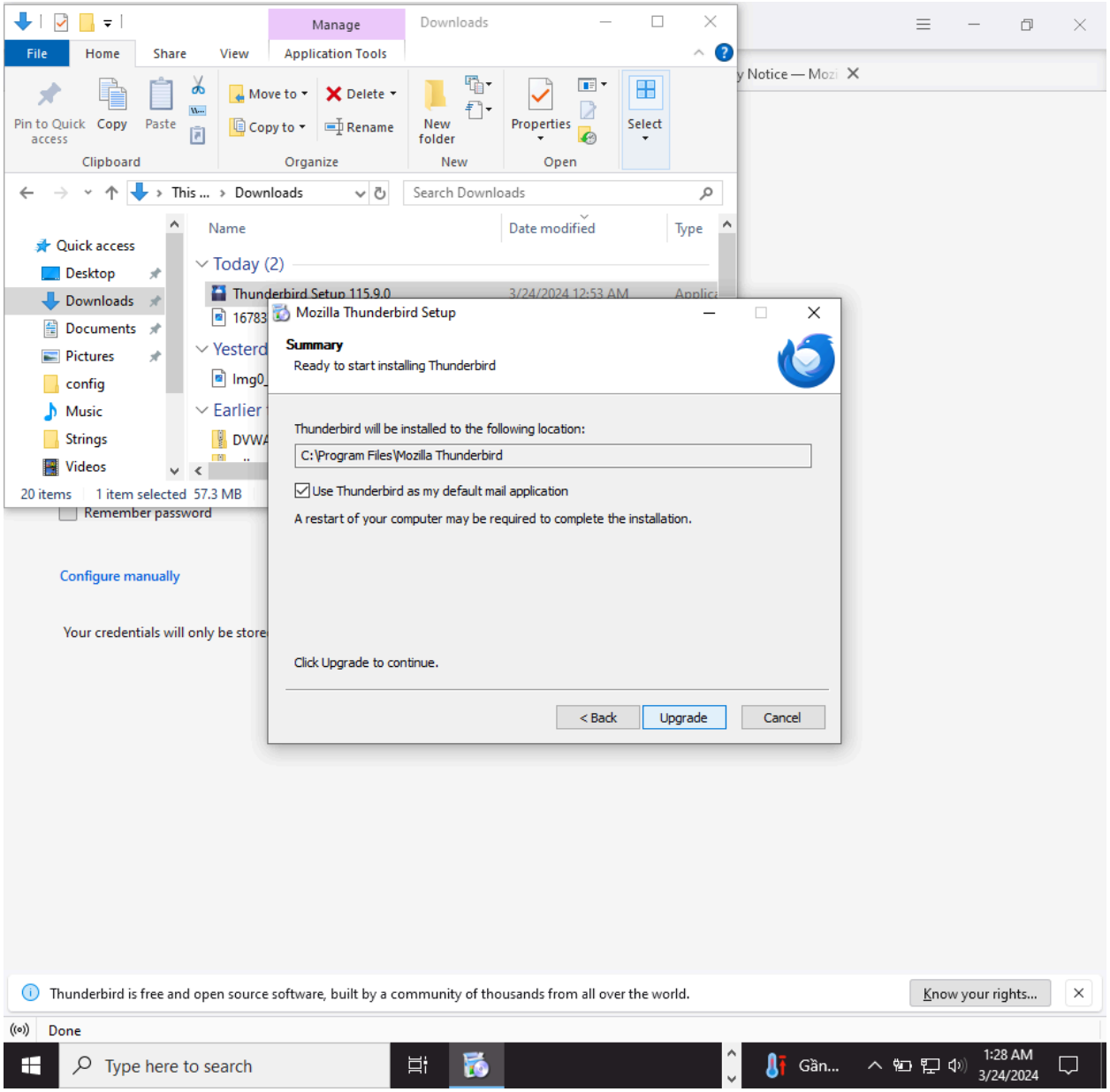
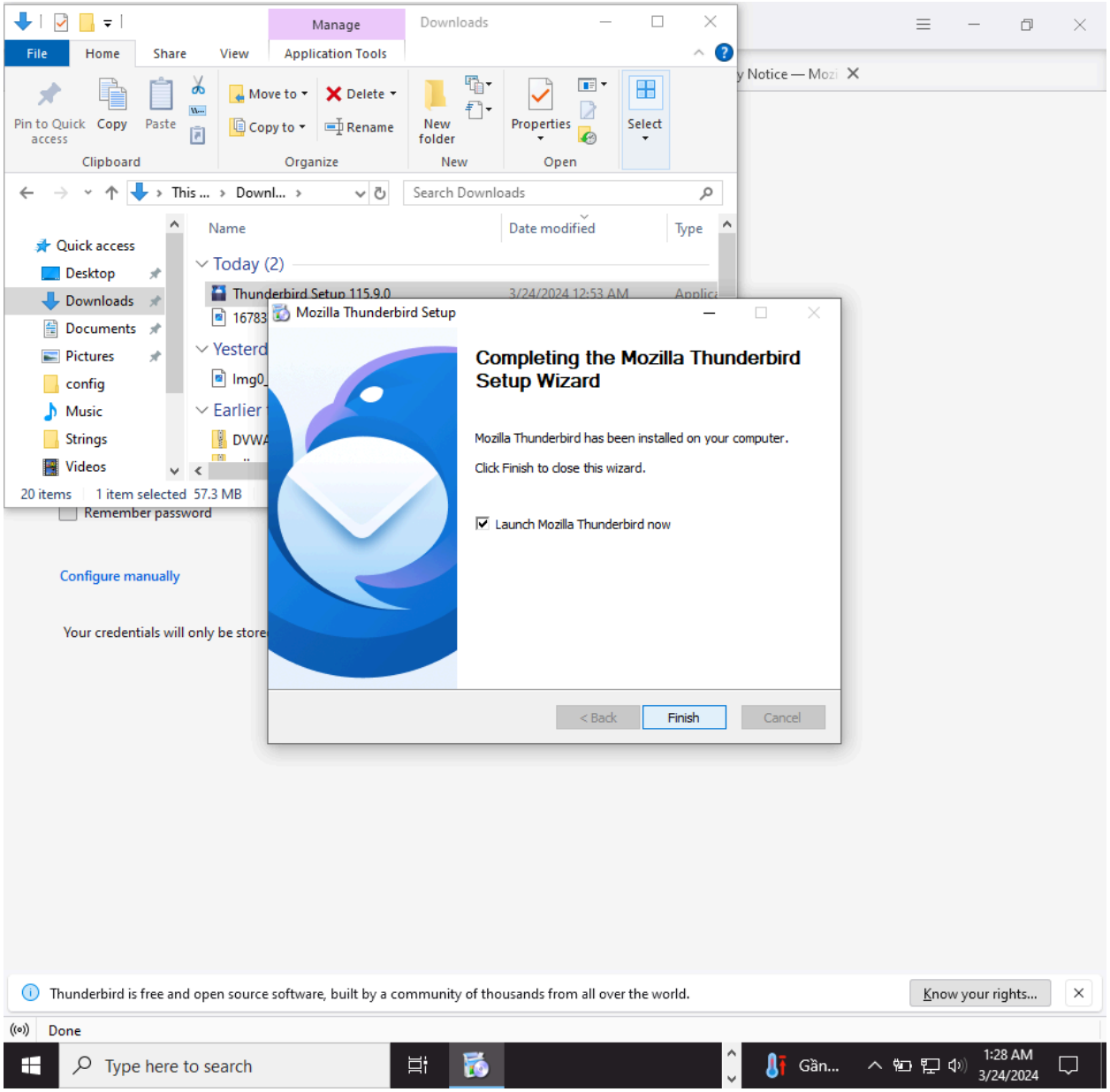
Lab 6.4:

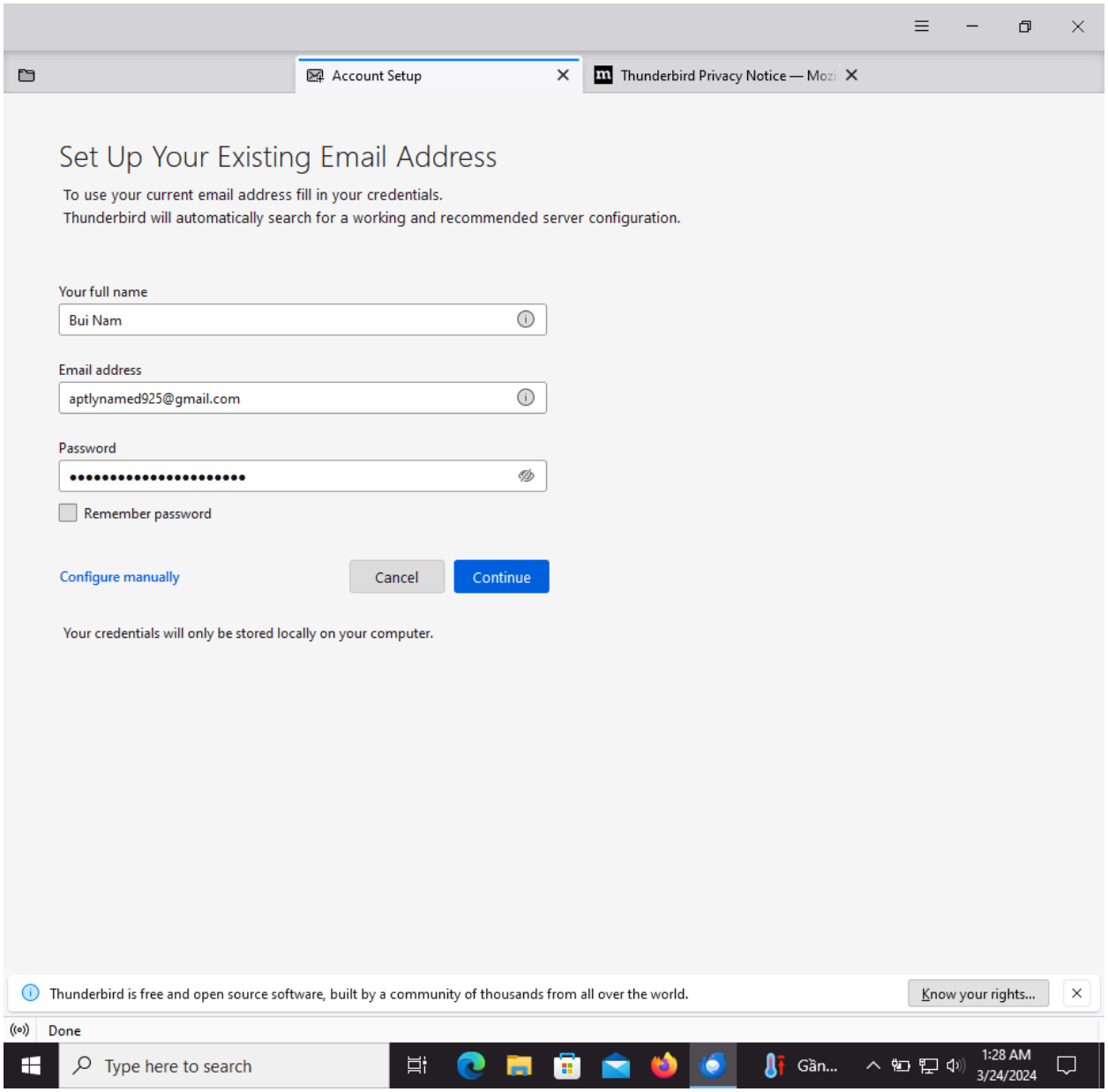
1, cài đặt thunderbird client

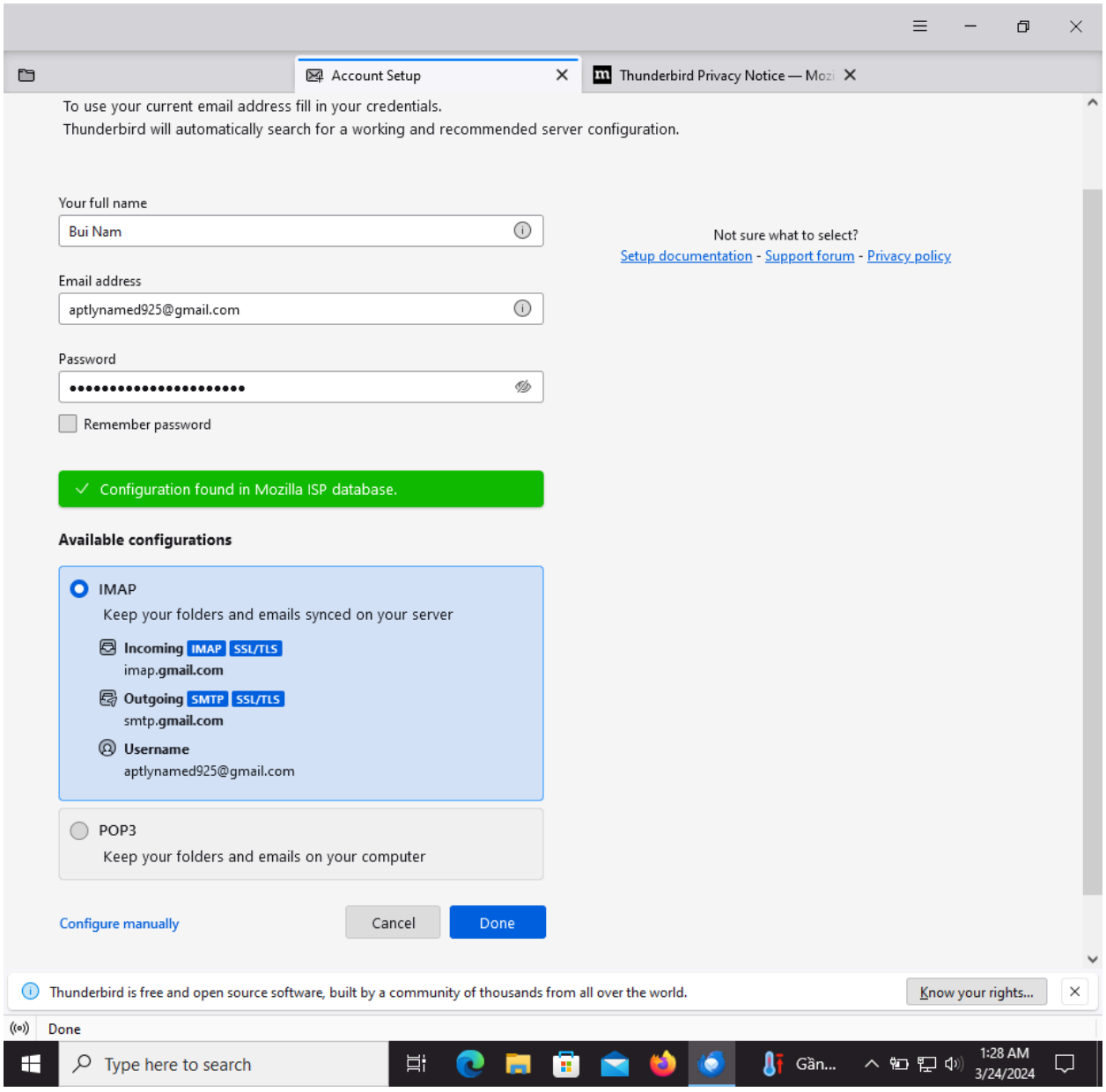


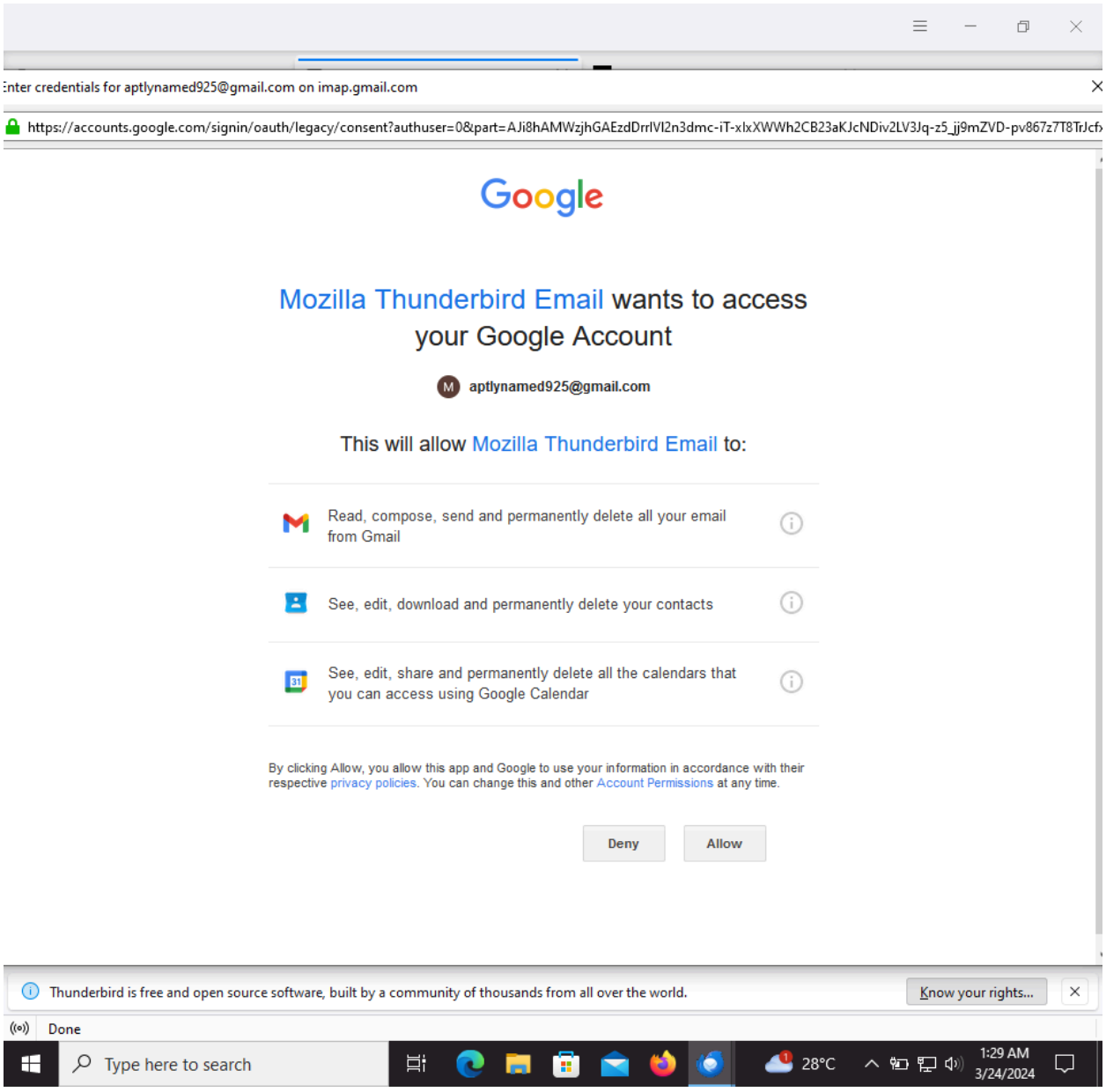

Manage
Downloads
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Move to
Delete
Copy to
Rename
New folder
Properties
Select
Clipboard
Organize
New
Open
This ... › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
Strings
Videos
Name
Date modified
Type
Today (2)
Thunderbird Setup 115.9.0
3/24/2024 12:53 AM
20 items
1 item selected 57.3 MB
Mozilla Thunderbird Setup
Setup Type
Choose setup options
Choose the type of setup you prefer, then click Next.
Standard
Thunderbird will be installed with the most common options.
Custom
You may choose individual options to be installed. Recommended for experienced users.
< Back
Next >
Cancel
Remember password
Configure manually
Your credentials will only be store
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Done
Type here to search
1:27 AM
3/24/2024

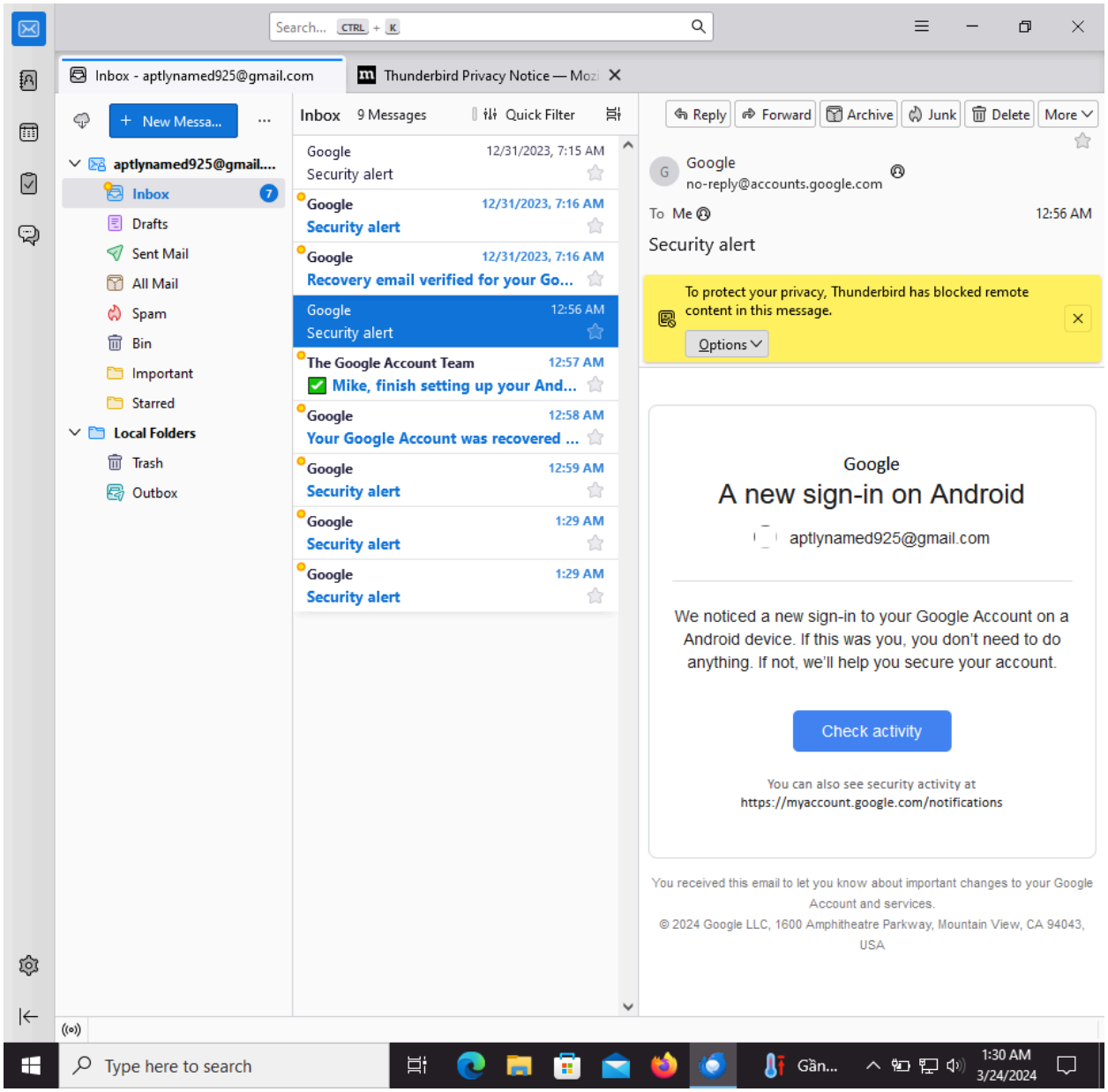

Manage
Downloads
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Move to
Delete
Copy to
Rename
New folder
Properties
Select
Clipboard
Organize
New
Open
This ... › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
Strings
Videos
Name
Date modified
Type
Today (2)
Thunderbird Setup 115.9.0
3/24/2024 12:53 AM
20 items
1 item selected 57.3 MB
Mozilla Thunderbird Setup
Summary
Ready to start installing Thunderbird
Thunderbird will be installed to the following location:
C:\Program Files\Mozilla Thunderbird
Use Thunderbird as my default mail application
A restart of your computer may be required to complete the installation.
Click Upgrade to continue.
< Back
Upgrade
Cancel
Remember password
Configure manually
Your credentials will only be store
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Done
Type here to search
Gần...
1:28 AM
3/24/2024


Manage
Downloads
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Move to
Delete
Copy to
Rename
New folder
Properties
Select
Clipboard
Organize
New
Open
This ...
Downl...
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
Strings
Videos
Name
Date modified
Type
Today (2)
Thunderbird Setup 115.9.0
3/24/2024 12:53 AM
Yesterd
Earlier
20 items
1 item selected 57.3 MB
Mozilla Thunderbird Setup
Completing the Mozilla Thunderbird Setup Wizard
Mozilla Thunderbird has been installed on your computer.
Click Finish to close this wizard.
Launch Mozilla Thunderbird now
< Back
Finish
Cancel
Remember password
Configure manually
Your credentials will only be store
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Done
Type here to search
Gần...
1:28 AM
3/24/2024

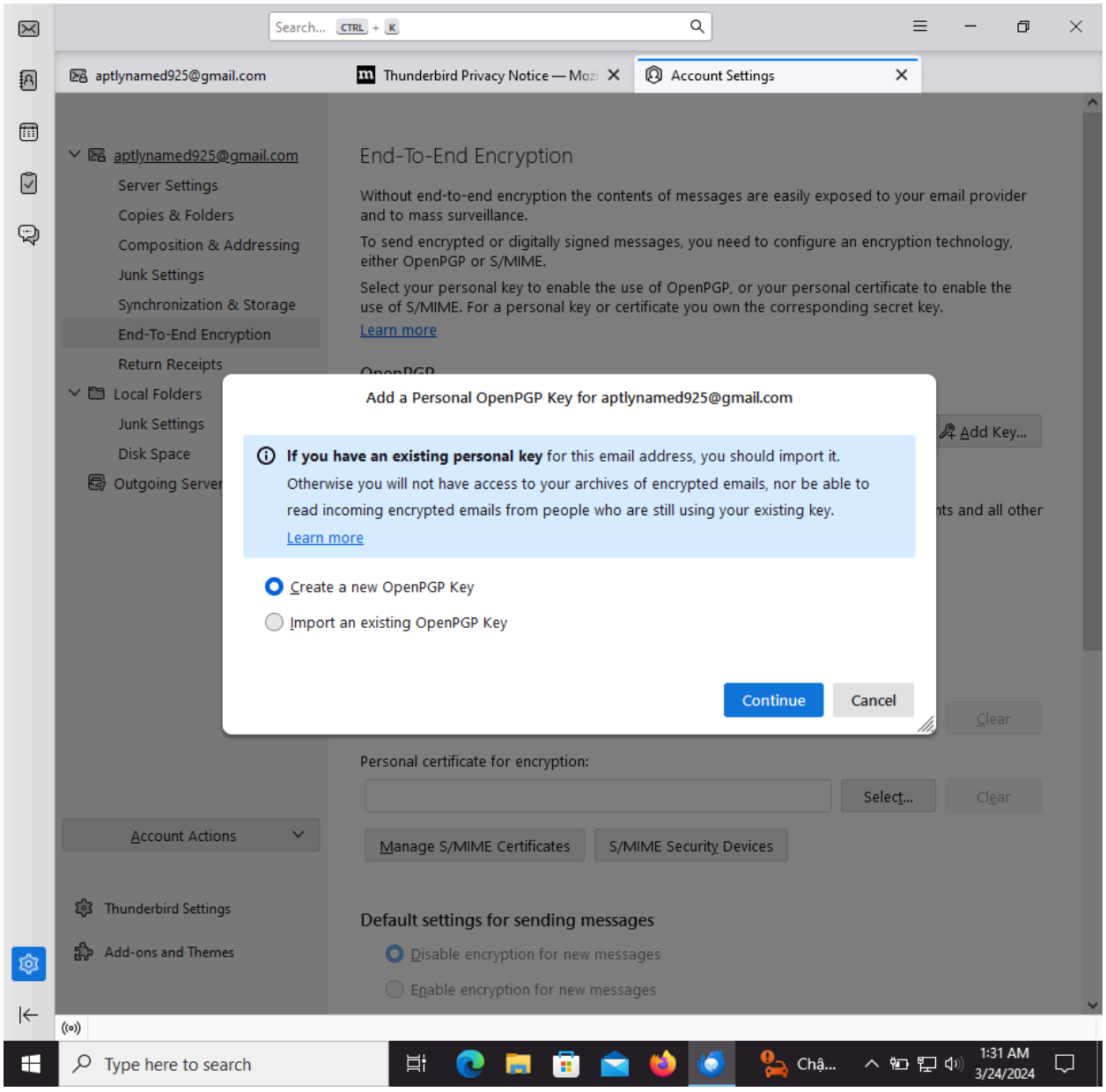

Account Setup
Thunderbird Privacy Notice — Mozi
Set Up Your Existing Email Address
To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.
Your full name
Bui Nam
Email address
aptlynamed925@gmail.com
Password
Remember password
Configure manually
Cancel
Continue
Your credentials will only be stored locally on your computer.
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Done
Type here to search
Gần...
1:28 AM
3/24/2024

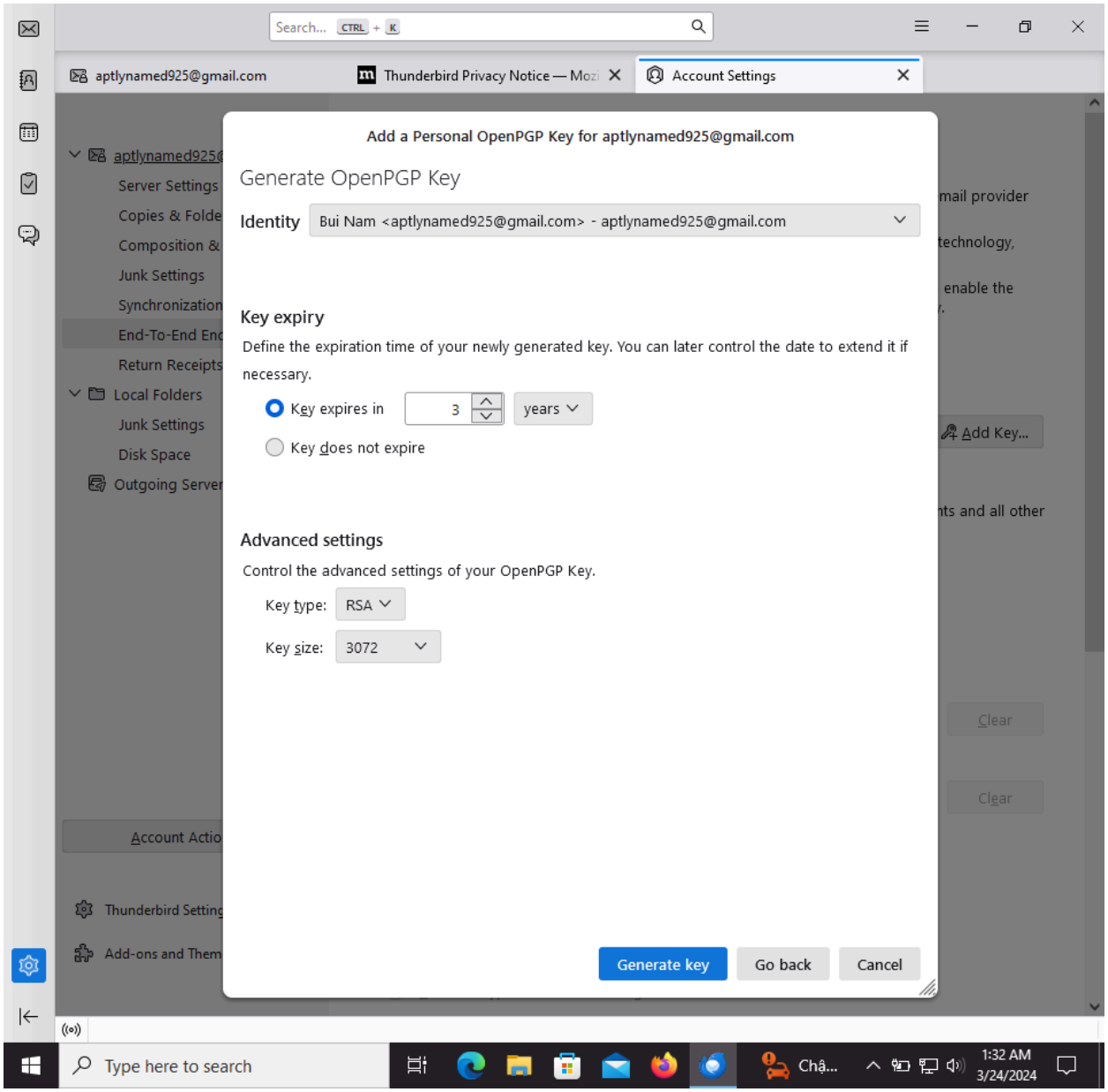

Account Setup
Thunderbird Privacy Notice — Mozi
To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.
Your full name
Bui Nam
Email address
aptlynamed925@gmail.com
Password
Remember password
Not sure what to select?
Setup documentation - Support forum - Privacy policy
Configuration found in Mozilla ISP database.
Available configurations
IMAP
Keep your folders and emails synced on your server
Incoming IMAP SSL/TLS
imap.gmail.com
Outgoing SMTP SSL/TLS
smtp.gmail.com
Username
aptlynamed925@gmail.com
POP3
Keep your folders and emails on your computer
Configure manually
Cancel
Done
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Done
Type here to search
Gần...
1:28 AM
3/24/2024

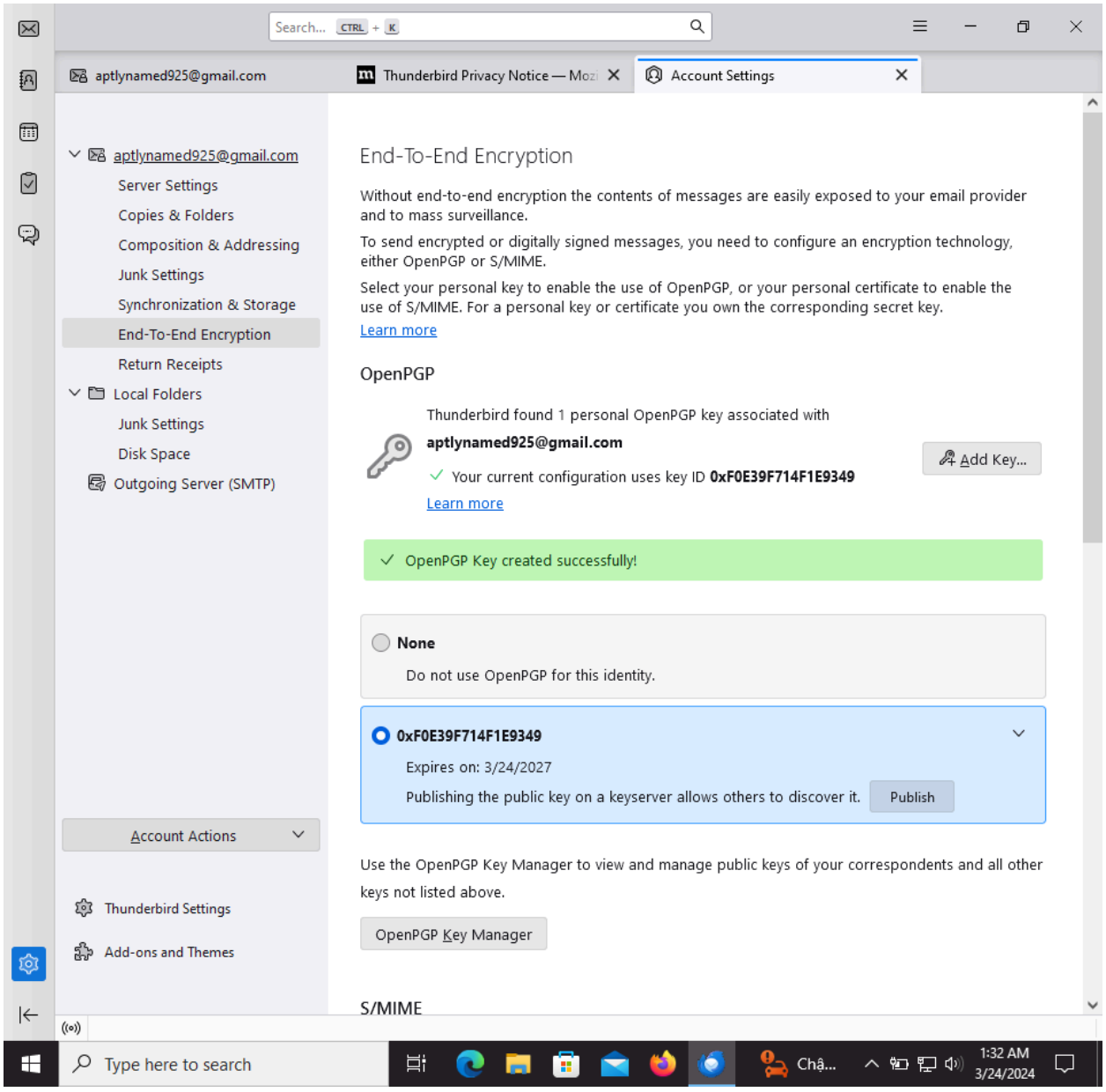

Enter credentials for aptlynamed925@gmail.com on imap.gmail.com
https://accounts.google.com/signin/oauth/legacy/consent?authuser=0&part=AJi8hAMWzjhGAEzdDrrlVl2n3dmc-iT-xlxXWWh2CB23aKJcNDiv2LV3Jq-z5_jj9mZVD-pv867z7T8TrJcf
Google
Mozilla Thunderbird Email wants to access your Google Account
aptlynamed925@gmail.com
This will allow Mozilla Thunderbird Email to:
Read, compose, send and permanently delete all your email from Gmail
See, edit, download and permanently delete your contacts
See, edit, share and permanently delete all the calendars that you can access using Google Calendar
By clicking Allow, you allow this app and Google to use your information in accordance with their respective privacy policies. You can change this and other Account Permissions at any time.
Deny
Allow
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Done
Type here to search
28°C
1:29 AM
3/24/2024

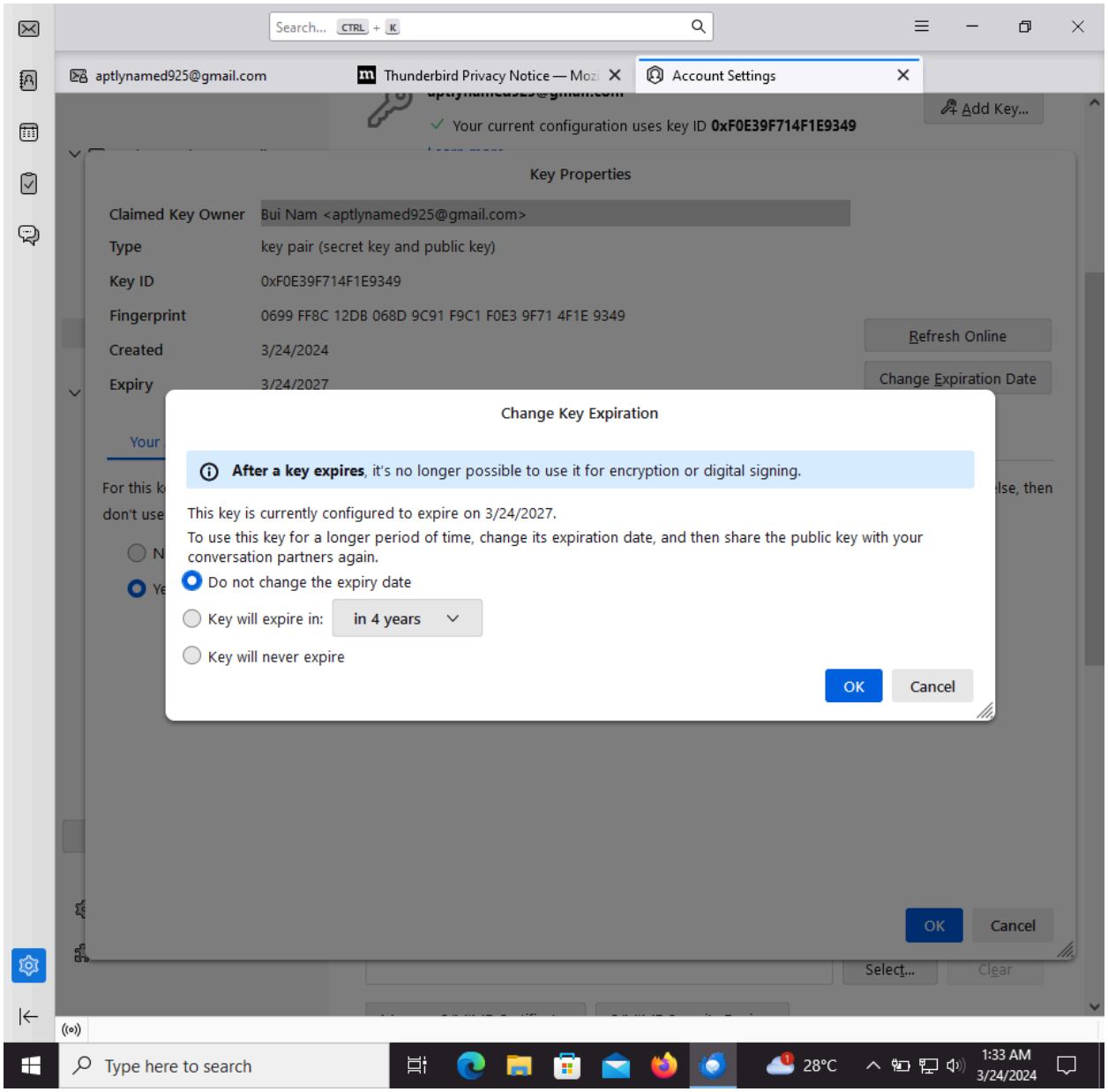


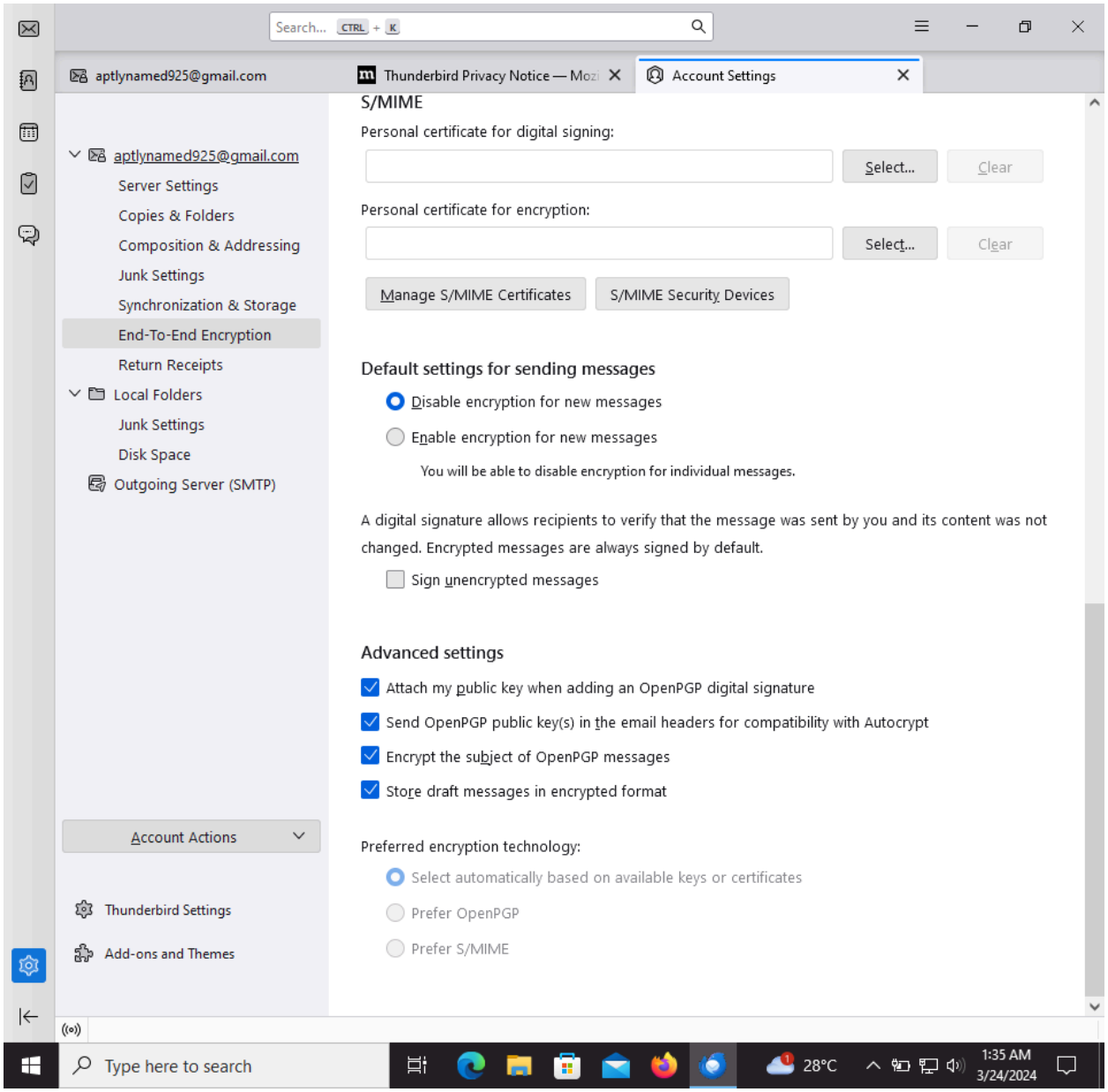
2, Cài đặt cặp chìa khóa công khai/ bí mật và cài đặt mã hóa cho tài khoản


Search... CTRL + K
aptlynamed925@gmail.com
Thunderbird Privacy Notice — Mozi
Account Settings
aptlynamed925@gmail.com
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
End-To-End Encryption
Return Receipts
Local Folders
Junk Settings
Disk Space
Outgoing Server
End-To-End Encryption
Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.
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
Add Key...
Add a Personal OpenPGP Key for aptlynamed925@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
Continue
Cancel
Clear
Personal certificate for encryption:
Select...
Clear
Account Actions
Manage S/MIME Certificates
S/MIME Security Devices
Thunderbird Settings
Add-ons and Themes
Default settings for sending messages
Disable encryption for new messages
Enable encryption for new messages
Type here to search
1:31 AM
3/24/2024

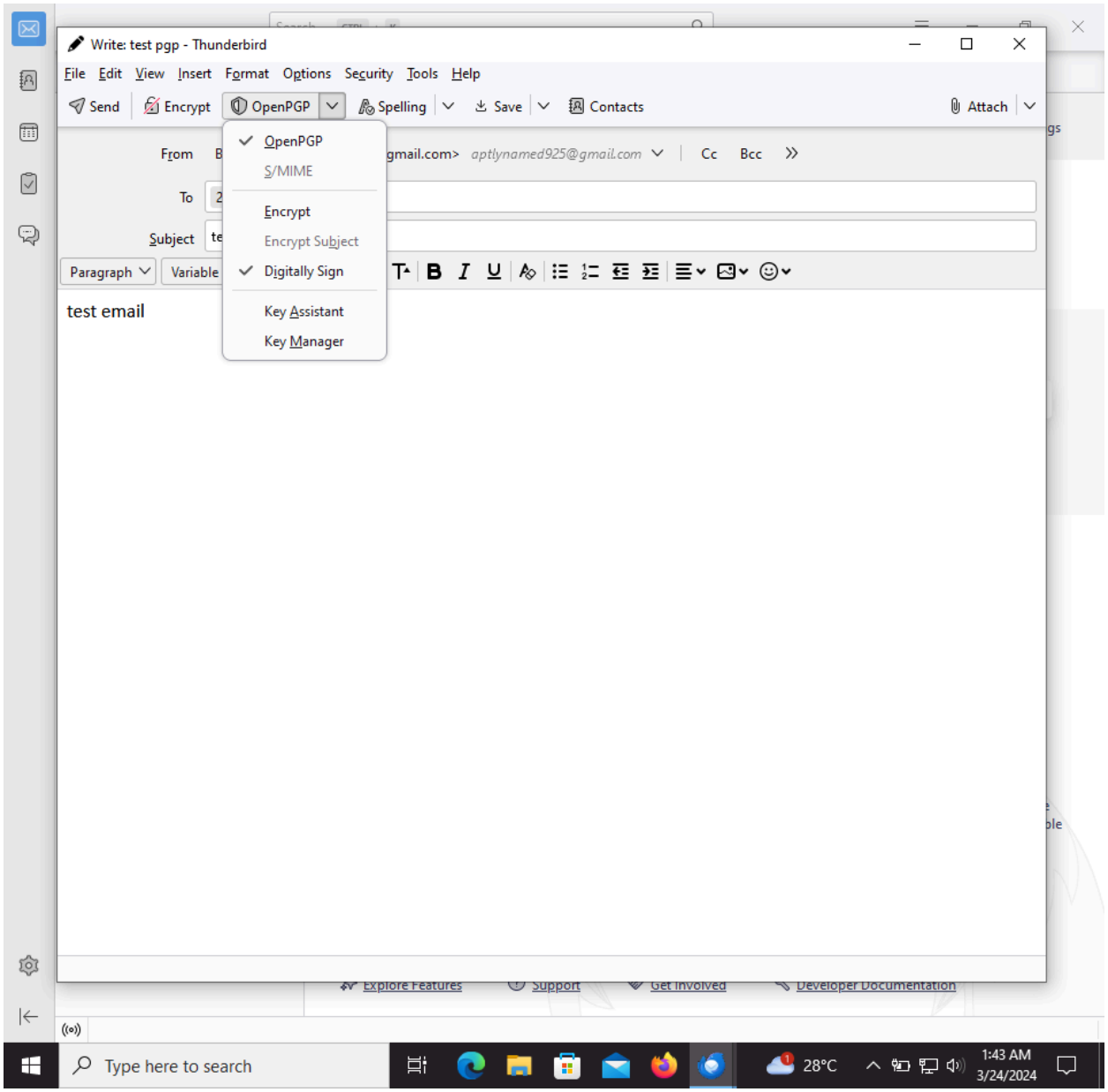

Search... CTRL + K
aptlynamed925@gmail.com
Thunderbird Privacy Notice — Mozi
Account Settings
Add a Personal OpenPGP Key for aptlynamed925@gmail.com
Generate OpenPGP Key
Identity
Bui Nam <aptlynamed925@gmail.com> - aptlynamed925@gmail.com
Key expiry
Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.
Key expires in
3
years
Key does not expire
Advanced settings
Control the advanced settings of your OpenPGP Key.
Key type:
RSA
Key size:
3072
Generate key
Go back
Cancel
Server Settings
Copies & Folde
Composition &
Junk Settings
Synchronization
End-To-End Enc
Return Receipts
Local Folders
Junk Settings
Disk Space
Outgoing Server
Add Key...
Clear
Clear
Account Actio
Thunderbird Setting
Add-ons and Them
Type here to search
1:32 AM
3/24/2024


Search... CTRL + K
aptlynamed925@gmail.com
Thunderbird Privacy Notice — Mozi
Account Settings
aptlynamed925@gmail.com
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
End-To-End Encryption
Return Receipts
Local Folders
Junk Settings
Disk Space
Outgoing Server (SMTP)
Account Actions
Thunderbird Settings
Add-ons and Themes
End-To-End Encryption
Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.
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
aptlynamed925@gmail.com
Your current configuration uses key ID 0xF0E39F714F1E9349
Add Key...
Learn more
OpenPGP Key created successfully!
None
Do not use OpenPGP for this identity.
0xF0E39F714F1E9349
Expires on: 3/24/2027
Publishing the public key on a keyserver allows others to discover it.
Publish
Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.
OpenPGP Key Manager
S/MIME
Type here to search
1:32 AM
3/24/2024

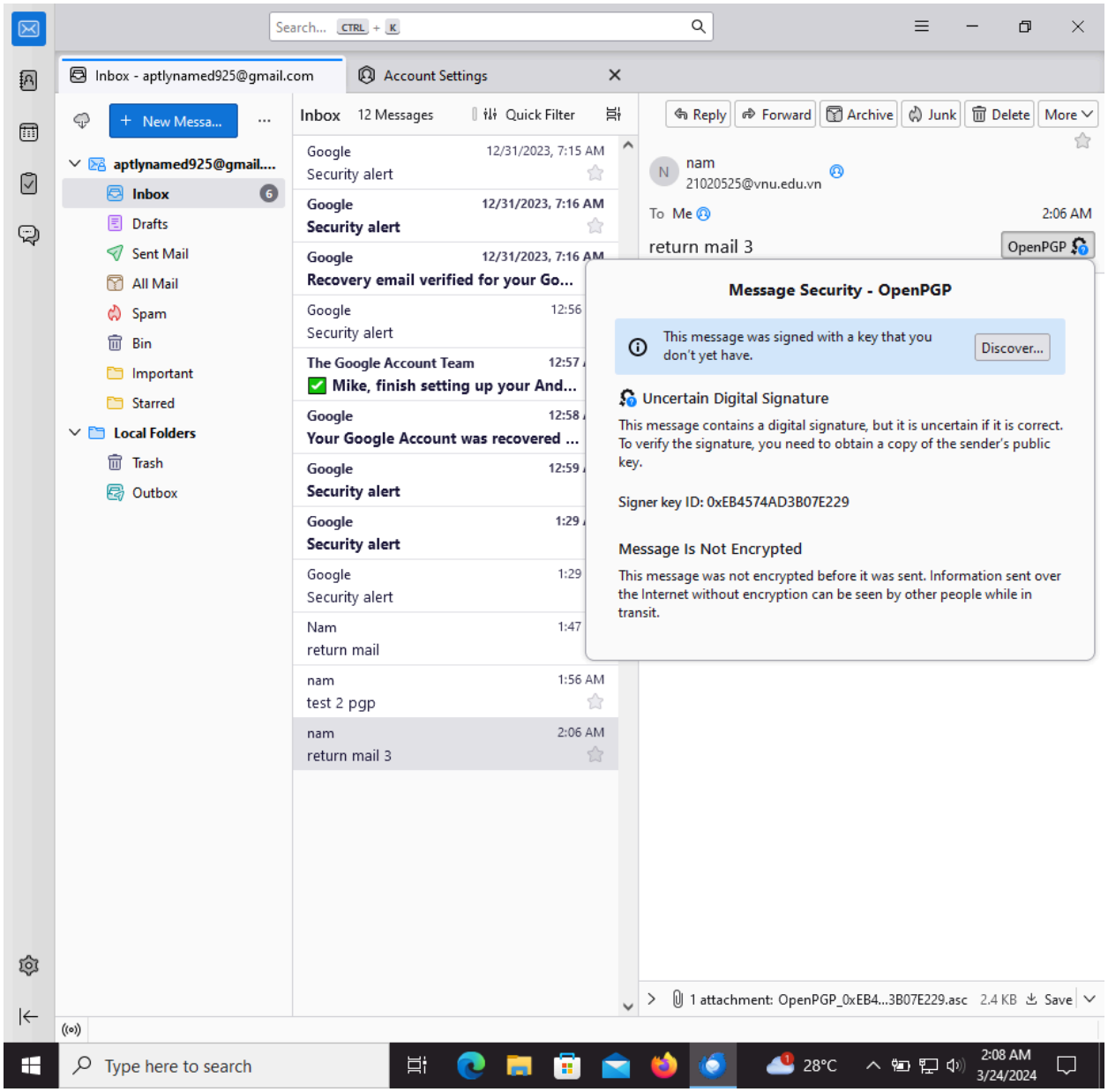

Search... CTRL + K
aptlynamed925@gmail.com
Thunderbird Privacy Notice — Mozi
Account Settings
Add Key...
Your current configuration uses key ID 0xF0E39F714F1E9349
Key Properties
Claimed Key Owner Bui Nam <aptlynamed925@gmail.com>
Type key pair (secret key and public key)
Key ID 0xF0E39F714F1E9349
Fingerprint 0699 FF8C 12DB 068D 9C91 F9C1 F0E3 9F71 4F1E 9349
Created 3/24/2024
Expiry 3/24/2027
Refresh Online
Change Expiration Date
Change Key Expiration
After a key expires, it's no longer possible to use it for encryption or digital signing.
This key is currently configured to expire on 3/24/2027.
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: in 4 years
Key will never expire
OK
Cancel
OK
Cancel
Select...
Clear
Type here to search
28°C
1:33 AM
3/24/2024

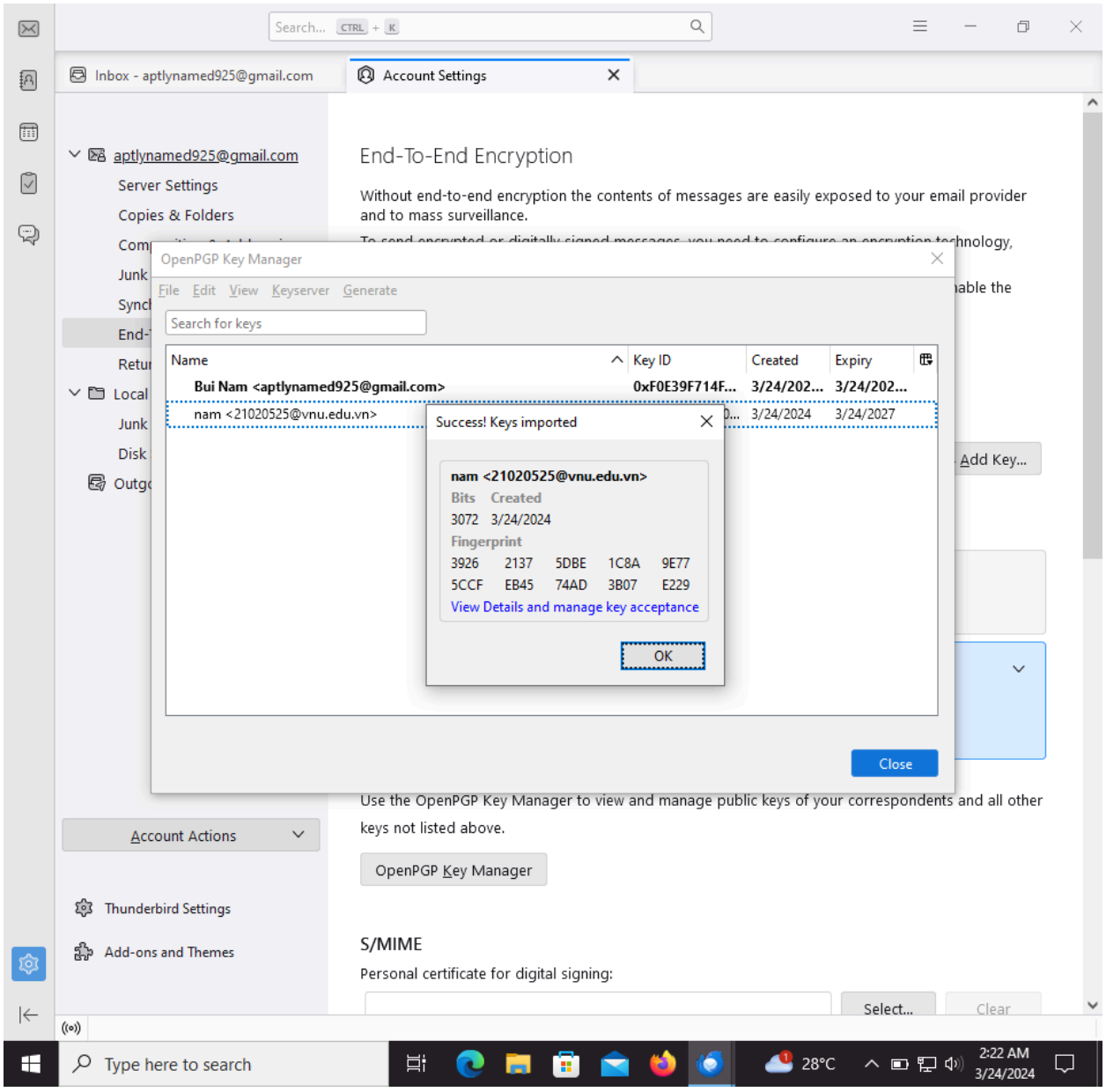


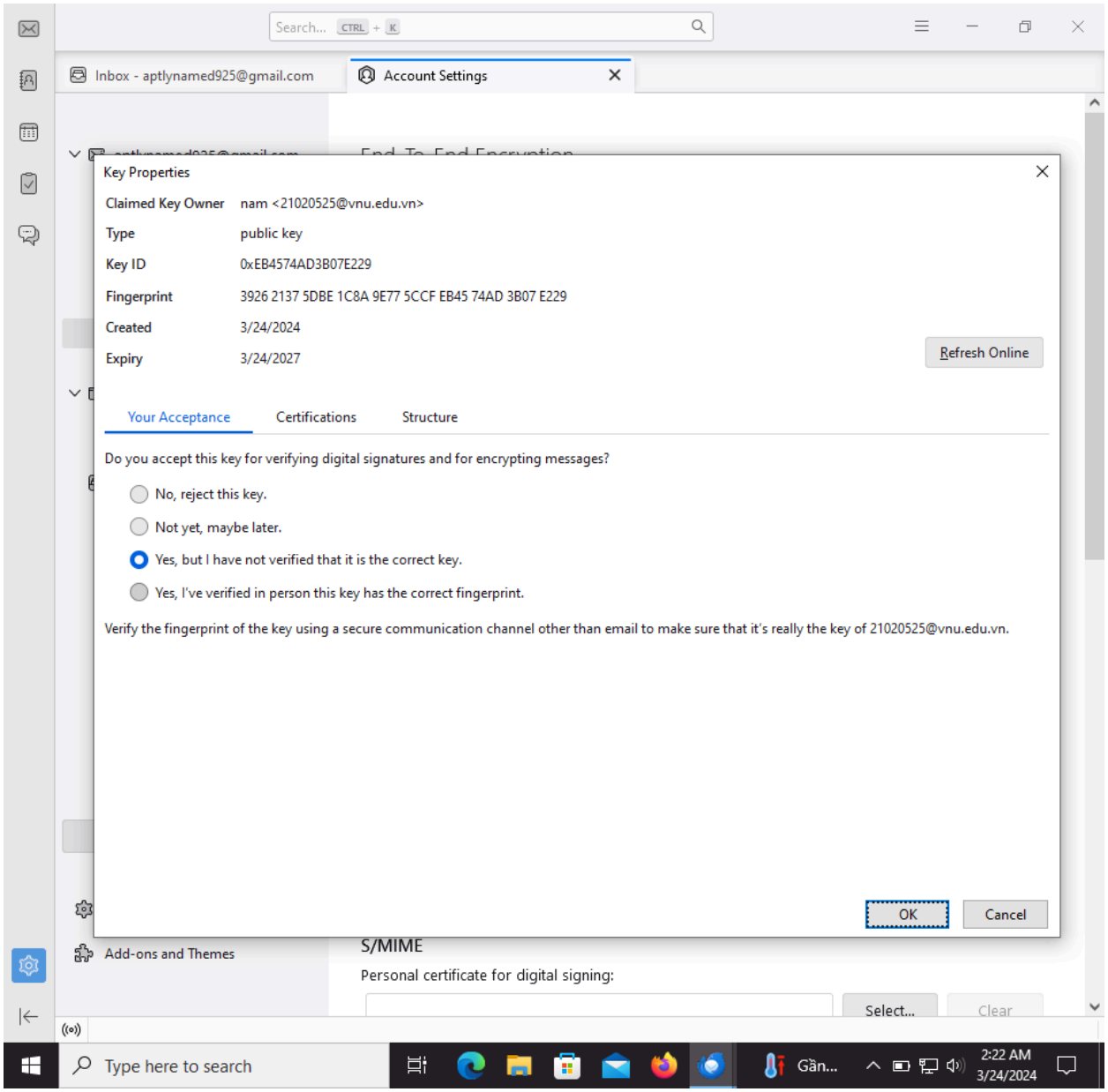
3, Gửi email cho 1 tải khoán khác được ký điện tử và có chìa công khai của bản thân

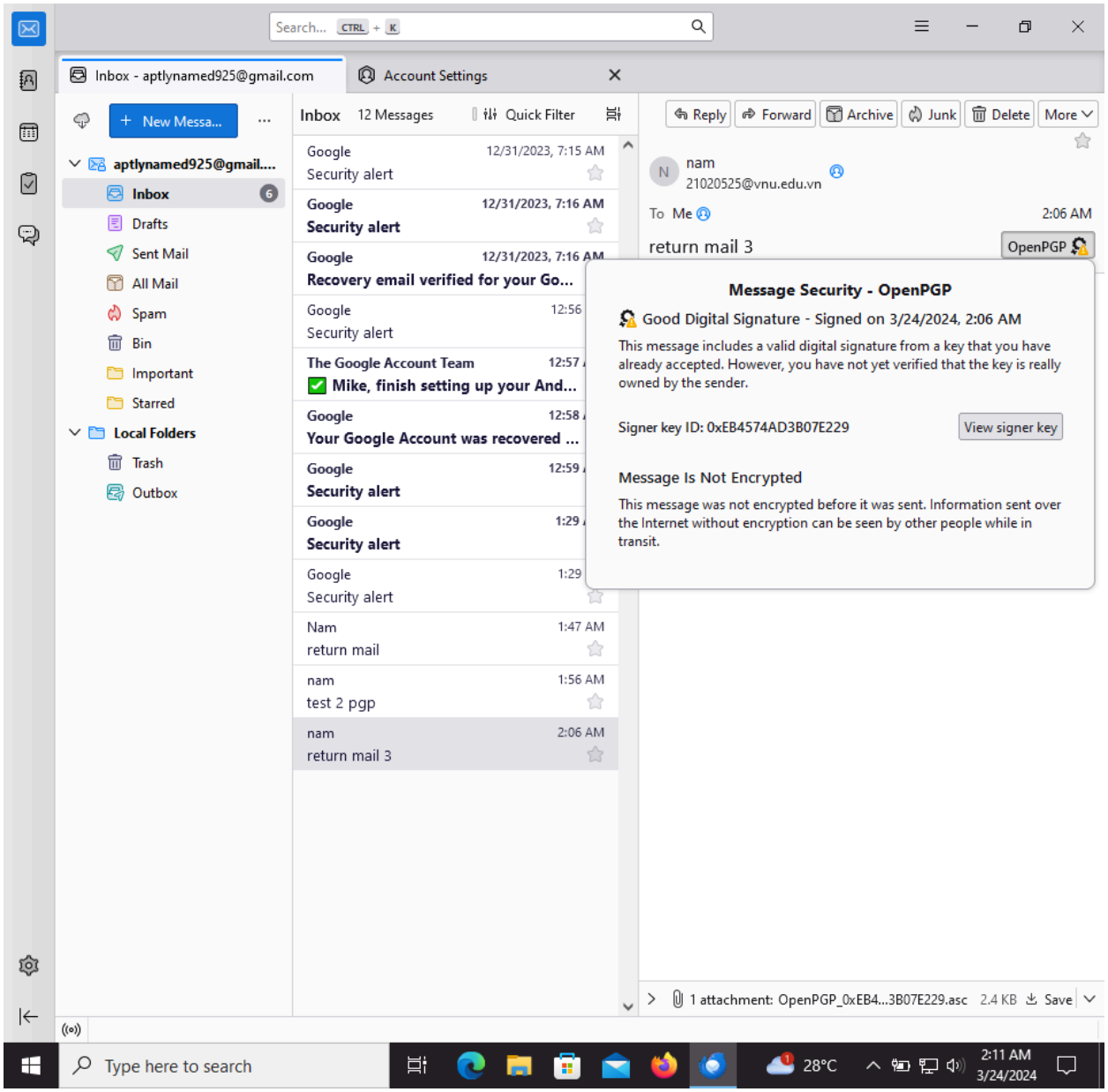


4, nhận email của tài khoản khác được gửi theo bước 3 và import chìa công khai của tài khoản kia

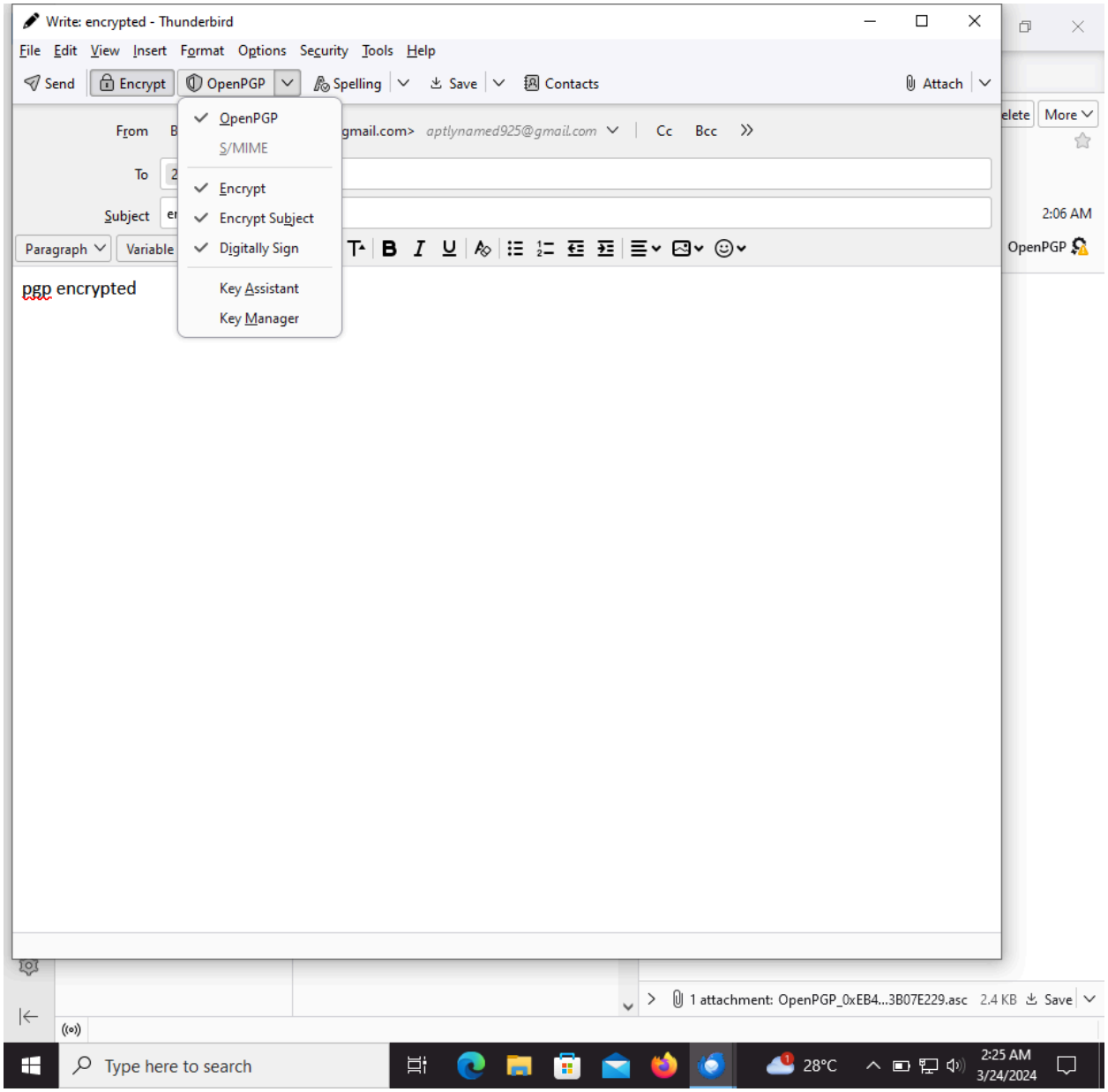

Search... CTRL + K
Inbox - aptlynamed925@gmail.com
Account Settings
New Messa...
aptlynamed925@gmail....
Inbox 6
Drafts
Sent Mail
All Mail
Spam
Bin
Important
Starred
Local Folders
Trash
Outbox
Inbox 12 Messages
Quick Filter
Google 12/31/2023, 7:15 AM
Security alert
Google 12/31/2023, 7:16 AM
Security alert
Google 12/31/2023, 7:16 AM
Recovery email verified for your Go...
Google 12:56
Security alert
The Google Account Team 12:57
Mike, finish setting up your And...
Google 12:58
Your Google Account was recovered ...
Google 12:59
Security alert
Google 1:29
Security alert
Google 1:29
Security alert
Nam 1:47
return mail
nam 1:56 AM
test 2 pgp
nam 2:06 AM
return mail 3
Reply
Forward
Archive
Junk
Delete
More
nam
21020525@vnu.edu.vn
To Me
2:06 AM
return mail 3
OpenPGP
Message Security - OpenPGP
This message was signed with a key that you don't yet have.
Discover...
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: 0xEB4574AD3B07E229
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.
1 attachment: OpenPGP_0xEB4...3B07E229.asc 2.4 KB Save
Type here to search
28°C
2:08 AM
3/24/2024


Search... CTRL + K
Inbox - aptlynamed925@gmail.com
Account Settings
aptlynamed925@gmail.com
Server Settings
Copies & Folders
Junk
Local
Junk
Disk
Account Actions
Thunderbird Settings
Add-ons and Themes
End-To-End Encryption
Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.
Add Key...
Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.
OpenPGP Key Manager
S/MIME
Personal certificate for digital signing:
Select...
Clear
OpenPGP Key Manager
File Edit View Keyserver Generate
Search for keys
Name
Key ID
Created
Expiry
Bui Nam <aptlynamed925@gmail.com>
0xF0E39F714F...
3/24/202...
3/24/202...
nam <21020525@vnu.edu.vn>
3/24/2024
3/24/2027
Success! Keys imported
nam <21020525@vnu.edu.vn>
Bits Created
3072 3/24/2024
Fingerprint
3926 2137 5DBE 1C8A 9E77
5CCF EB45 74AD 3B07 E229
View Details and manage key acceptance
OK
Close
Type here to search
28°C
2:22 AM
3/24/2024

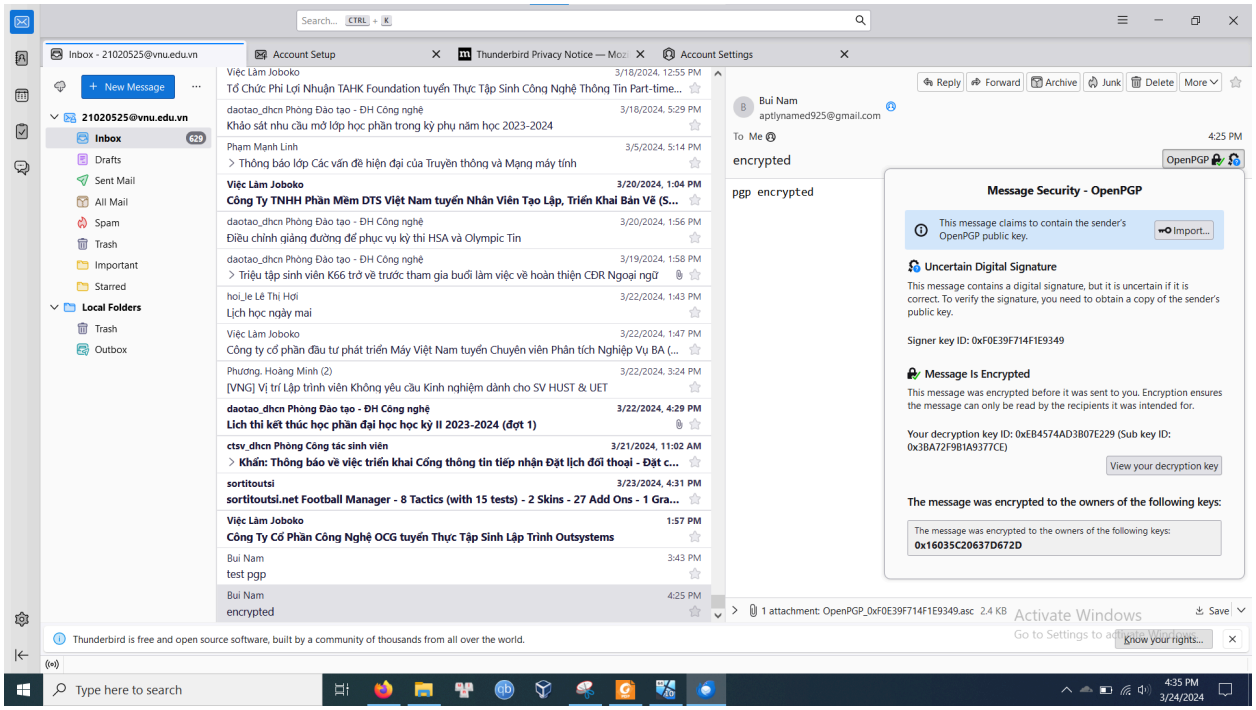

Search... CTRL + K
Inbox - aptlynamed925@gmail.com
Account Settings
Key Properties
Claimed Key Owner nam <21020525@vnu.edu.vn>
Type public key
Key ID 0xEB4574AD3B07E229
Fingerprint 3926 2137 5DBE 1C8A 9E77 5CCF EB45 74AD 3B07 E229
Created 3/24/2024
Expiry 3/24/2027
Refresh Online
Your Acceptance
Certifications
Structure
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 21020525@vnu.edu.vn.
OK
Cancel
Add-ons and Themes
S/MIME
Personal certificate for digital signing:
Select...
Clear
Type here to search
Gần...
2:22 AM
3/24/2024

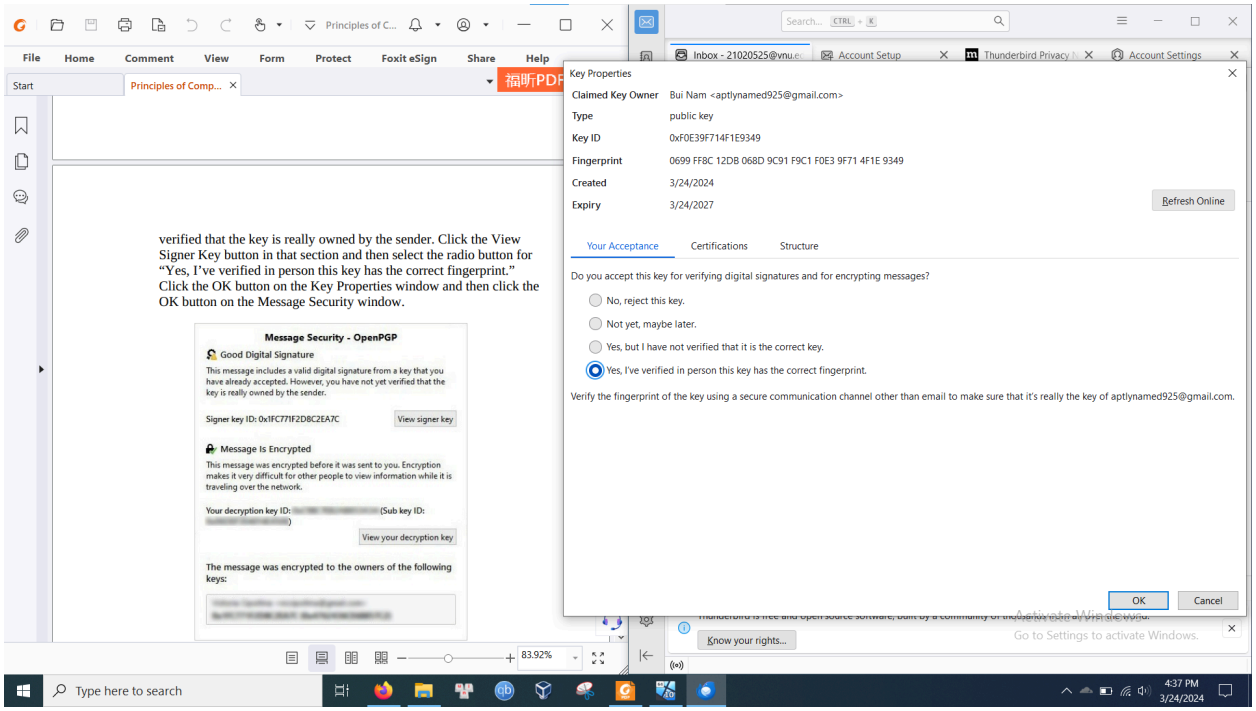


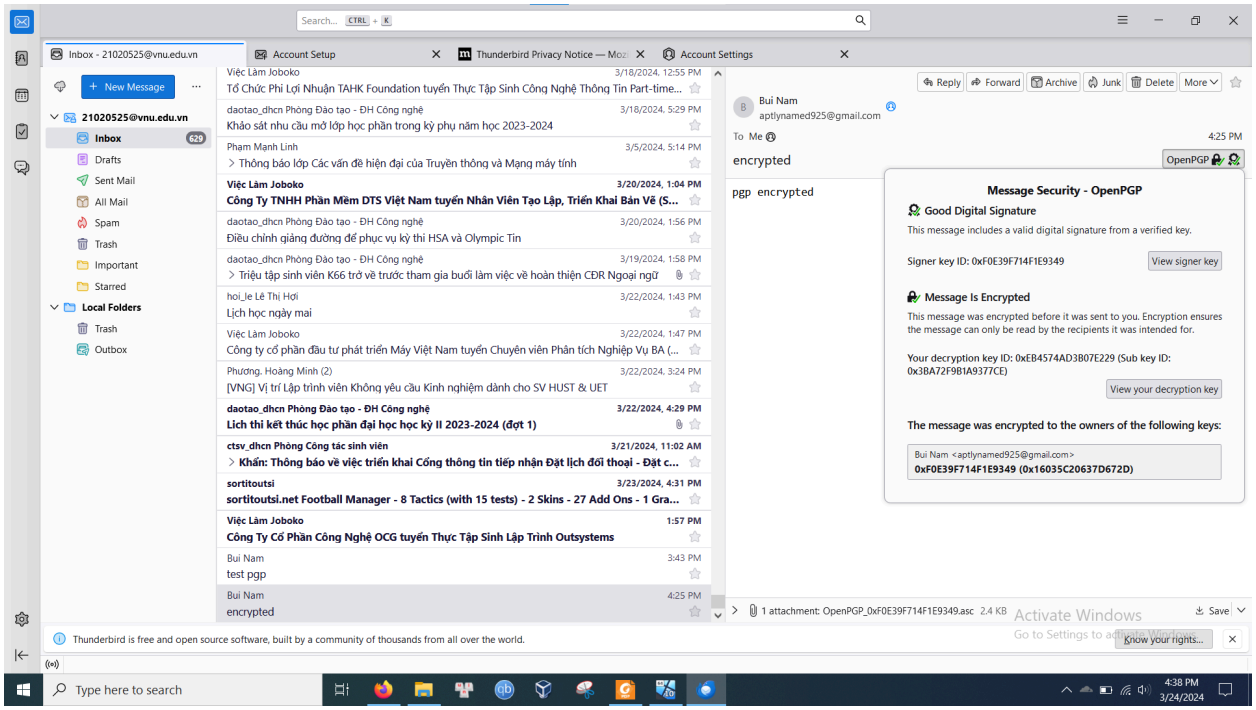
5, Mã hóa email với chìa khóa công khai vừa được gửi

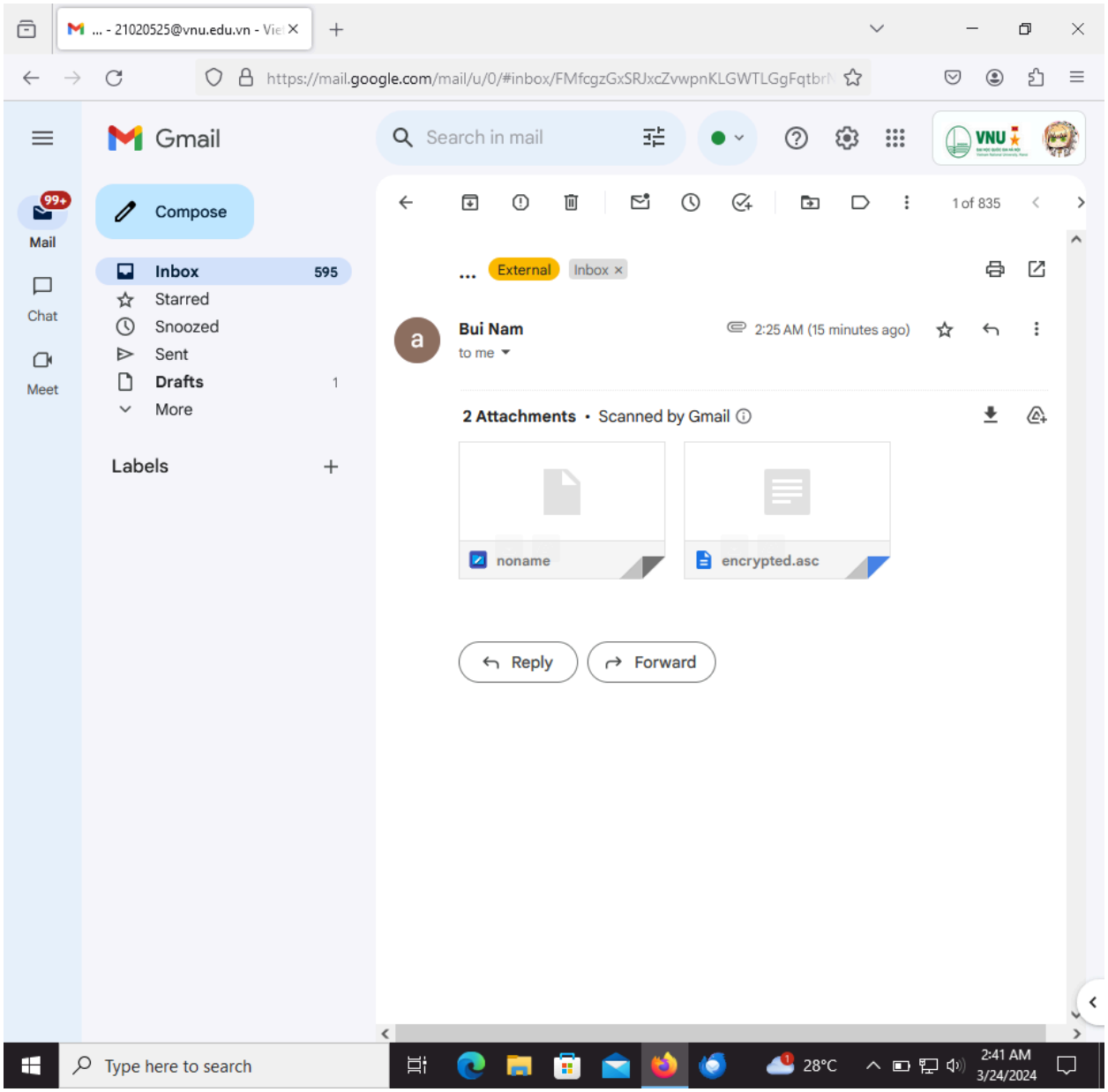


6: Mở client bên tài khoản được nhận email mã hóa


Inbox - 21020525@vnu.edu.vn
Account Setup
Thunderbird Privacy Notice — Moz
Account Settings
New Message
21020525@vnu.edu.vn
Inbox 629
Drafts
Sent Mail
All Mail
Spam
Trash
Important
Starred
Local Folders
Trash
Outbox
Việc Làm Joboko 3/18/2024, 12:55 PM
Tổ Chức Phi Lợi Nhuận TAHK Foundation tuyển Thực Tập Sinh Công Nghệ Thông Tin Part-time...
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/18/2024, 5:29 PM
Khảo sát nhu cầu mở lớp học phần trong kỳ phụ năm học 2023-2024
Phạm Mạnh Linh 3/5/2024, 5:14 PM
Thông báo lớp Các vấn đề hiện đại của Truyền thông và Mạng máy tính
Việc Làm Joboko 3/20/2024, 1:04 PM
Công Ty TNHH Phần Mềm DTS Việt Nam tuyển Nhân Viên Tạo Lập, Triển Khai Bản Vẽ (S...
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/20/2024, 1:56 PM
Điều chỉnh giảng đường để phục vụ kỳ thi HSA và Olympic Tin
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/19/2024, 1:58 PM
Triệu tập sinh viên K66 trở về trước tham gia buổi làm việc về hoàn thiện CĐR Ngoại ngữ
hoi_le Lê Thị Hợi 3/22/2024, 1:43 PM
Lịch học ngày mai
Việc Làm Joboko 3/22/2024, 1:47 PM
Công ty cổ phần đầu tư phát triển Máy Việt Nam tuyển Chuyên viên Phân tích Nghiệp Vụ BA (...
Phương. Hoàng Minh (2) 3/22/2024, 3:24 PM
[VNG] Vị trí Lập trình viên Không yêu cầu Kinh nghiệm dành cho SV HUST & UET
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/22/2024, 4:29 PM
Lịch thi kết thúc học phần đại học học kỳ II 2023-2024 (đợt 1)
ctsv_dhcn Phòng Công tác sinh viên 3/21/2024, 11:02 AM
Khẩn: Thông báo về việc triển khai Cổng thông tin tiếp nhận Đặt lịch đối thoại - Đặt c...
sortitoutsi 3/23/2024, 4:31 PM
sortitoutsi.net Football Manager - 8 Tactics (with 15 tests) - 2 Skins - 27 Add Ons - 1 Gra...
Việc Làm Joboko 1:57 PM
Công Ty Cổ Phần Công Nghệ OCG tuyển Thực Tập Sinh Lập Trình Outsystems
Bui Nam 3:43 PM
test pgp
Bui Nam 4:25 PM
encrypted
Reply
Forward
Archive
Junk
Delete
More
Bui Nam
aptlynamed925@gmail.com
To Me
4:25 PM
encrypted
OpenPGP
pgp encrypted
Message Security - OpenPGP
This message claims to contain the sender's OpenPGP public key.
Import...
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: 0xF0E39F714F1E9349
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: 0xEB4574AD3B07E229 (Sub key ID: 0x3BA72F9B1A9377CE)
View your decryption key
The message was encrypted to the owners of the following keys:
The message was encrypted to the owners of the following keys:
0x16035C20637D672D
1 attachment: OpenPGP_0xF0E39F714F1E9349.asc 2.4 KB
Save
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Activate Windows
Go to Settings to activate Windows.
Type here to search
4:35 PM
3/24/2024


File Home Comment View Form Protect Foxit eSign Share Help
Start
Principles of Comp...
verified that the key is really owned by the sender. Click the View Signer Key button in that section and then select the radio button for "Yes, I've verified in person this key has the correct fingerprint." Click the OK button on the Key Properties window and then click the OK button on the Message Security window.
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: 0x1FC771F2DBC2EA7C
View signer key
Message Is Encrypted
This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.
Your decryption key ID: (Sub key ID:
View your decryption key
The message was encrypted to the owners of the following keys:
Key Properties
Claimed Key Owner Bui Nam <aptlynamed925@gmail.com>
Type public key
Key ID 0xF0E39F714F1E9349
Fingerprint 0699 FF8C 12DB 068D 9C91 F9C1 F0E3 9F71 4F1E 9349
Created 3/24/2024
Expiry 3/24/2027
Refresh Online
Your Acceptance
Certifications
Structure
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 aptlynamed925@gmail.com.
OK
Cancel
83.92%
Know your rights...
Activate Windows
Go to Settings to activate Windows.
Type here to search
4:37 PM
3/24/2024


Inbox - 21020525@vnu.edu.vn
Account Setup
Thunderbird Privacy Notice — Moz
Account Settings
New Message
21020525@vnu.edu.vn
Inbox 629
Drafts
Sent Mail
All Mail
Spam
Trash
Important
Starred
Local Folders
Trash
Outbox
Việc Làm Joboko 3/18/2024, 12:55 PM
Tổ Chức Phi Lợi Nhuận TAHK Foundation tuyển Thực Tập Sinh Công Nghệ Thông Tin Part-time...
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/18/2024, 5:29 PM
Khảo sát nhu cầu mở lớp học phần trong kỳ phụ năm học 2023-2024
Phạm Mạnh Linh 3/5/2024, 5:14 PM
Thông báo lớp Các vấn đề hiện đại của Truyền thông và Mạng máy tính
Việc Làm Joboko 3/20/2024, 1:04 PM
Công Ty TNHH Phần Mềm DTS Việt Nam tuyển Nhân Viên Tạo Lập, Triển Khai Bản Vẽ (S...
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/20/2024, 1:56 PM
Điều chỉnh giảng đường để phục vụ kỳ thi HSA và Olympic Tin
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/19/2024, 1:58 PM
Triệu tập sinh viên K66 trở về trước tham gia buổi làm việc về hoàn thiện CĐR Ngoại ngữ
hoi_le Lê Thị Hợi 3/22/2024, 1:43 PM
Lịch học ngày mai
Việc Làm Joboko 3/22/2024, 1:47 PM
Công ty cổ phần đầu tư phát triển Máy Việt Nam tuyển Chuyên viên Phân tích Nghiệp Vụ BA (...
Phương, Hoàng Minh (2) 3/22/2024, 3:24 PM
[VNG] Vị trí Lập trình viên Không yêu cầu Kinh nghiệm dành cho SV HUST & UET
daotao_dhcn Phòng Đào tạo - ĐH Công nghệ 3/22/2024, 4:29 PM
Lịch thi kết thúc học phần đại học học kỳ II 2023-2024 (đợt 1)
ctsv_dhcn Phòng Công tác sinh viên 3/21/2024, 11:02 AM
Khẩn: Thông báo về việc triển khai Cổng thông tin tiếp nhận Đặt lịch đối thoại - Đặt c...
sortitoutsi 3/23/2024, 4:31 PM
sortitoutsi.net Football Manager - 8 Tactics (with 15 tests) - 2 Skins - 27 Add Ons - 1 Gra...
Việc Làm Joboko 1:57 PM
Công Ty Cổ Phần Công Nghệ OCG tuyển Thực Tập Sinh Lập Trình Outsystems
Bui Nam 3:43 PM
test pgp
Bui Nam 4:25 PM
encrypted
Reply
Forward
Archive
Junk
Delete
More
Bui Nam
aptlynamed925@gmail.com
To Me
4:25 PM
encrypted
OpenPGP
pgp encrypted
Message Security - OpenPGP
Good Digital Signature
This message includes a valid digital signature from a verified key.
Signer key ID: 0xF0E39F714F1E9349
View signer key
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: 0xEB4574AD3B07E229 (Sub key ID: 0x3BA72F9B1A9377CE)
View your decryption key
The message was encrypted to the owners of the following keys:
Bui Nam <aptlynamed925@gmail.com>
0xF0E39F714F1E9349 (0x16035C20637D672D)
1 attachment: OpenPGP_0xF0E39F714F1E9349.asc 2.4 KB
Save
Activate Windows
Go to Settings to activate Windows.
Thunderbird is free and open source software, built by a community of thousands from all over the world.
Know your rights...
Type here to search
4:38 PM
3/24/2024



7: Trả lời câu hỏi

a, Thunderbird chỉ có chìa khóa công khai của người gửi trong khi gmail có 2 file đính kèm với 1 trong đó là chìa khóa phiên. Điều này xảy ra vì 2 file đính kèm trong gmail gồm chìa khóa phiên và thông điệp được mã hóa bằng chìa khóa phiên, do thunderbird giải mã chìa khóa phiên được nên có thể giải mã thông điệp và hiện ra bình thường trong khi gmail không có chìa bí mật của người nhận nên để nguyên.

B, Khi ta mã hóa email để gửi, chìa khóa phiên mã hóa email.

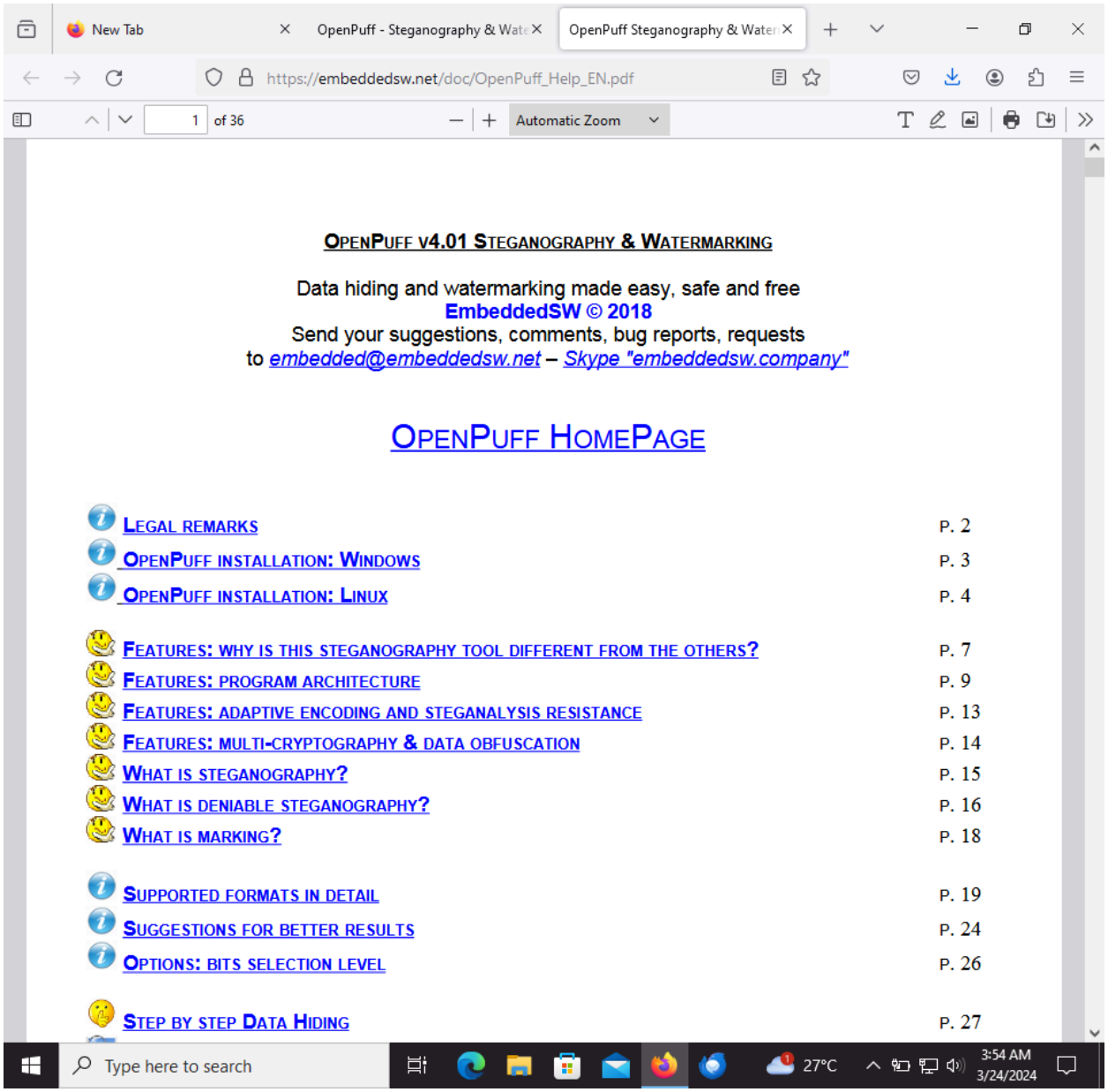
C, Khi ta mã hóa email, chìa khóa phiên được mã hóa bằng chìa công khai người nhận

D, Khi người nhận giải mã, chìa khóa phiên giải mã email

E, khi người nhận giải mã, chìa khóa bí mật người nhận giải mã chìa khóa phiên

F, một chìa phiên mã hóa email còn một chìa khác mã hóa chìa phiên vì pgp kết hợp mã hóa đối xứng và mã hóa chìa công khai để đảm bảo tốc độ lẫn bảo mật. Mã hóa chìa công khai bảo

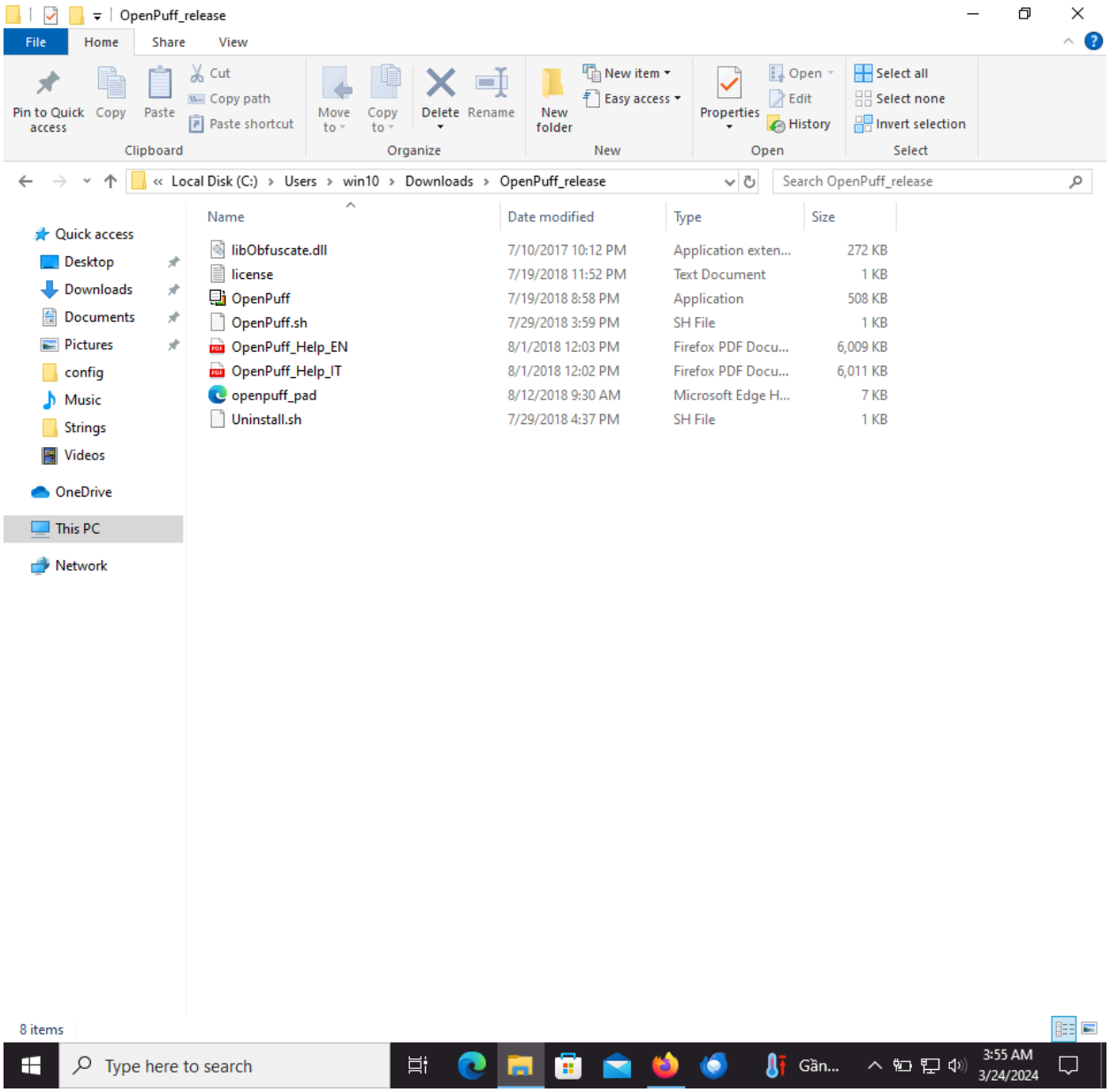
mật nhưng tốn thời gian nên được sử dụng để mã khóa chìa khóa phiên có chiều dài cố định và kích cỡ đa phần nhỏ hơn so với thông điệp được gửi. Thông điệp được mã hóa đối xứng để tăng tốc độ giải mã nhưng vẫn giữ được bảo mật do chìa phiên được mã hóa bất đối xứng.
G, Khi ta kí email , ta dùng chìa bí mật của ta để ký
H, khi người nhận xác nhận chữ kí, họ dùng chìa công khai của người gửi
I, Tính bí mật được đảm bảo bởi thông điệp chỉ có thể được giải mã bởi người có chìa bí mật đúng
J, tính toàn vẹn được đảm bảo bởi nếu bên thứ 3 muốn chỉnh sửa nội dung thì họ cần chìa bí mật của người gửi để ký cũng như chìa khóa bí mật của người nhận để biết khóa phiên để mã hóa lại thông điệp chỉnh sửa. Nếu không có thì ta biết tin nhắn đã bị chỉnh sửa.
k,Tính không thể chối cãi được đảm bảo do chìa khóa bí mật để ký vào thông điệp là độc nhất nên người ký để gửi email có thể được xác định lại.
Project 6.1:

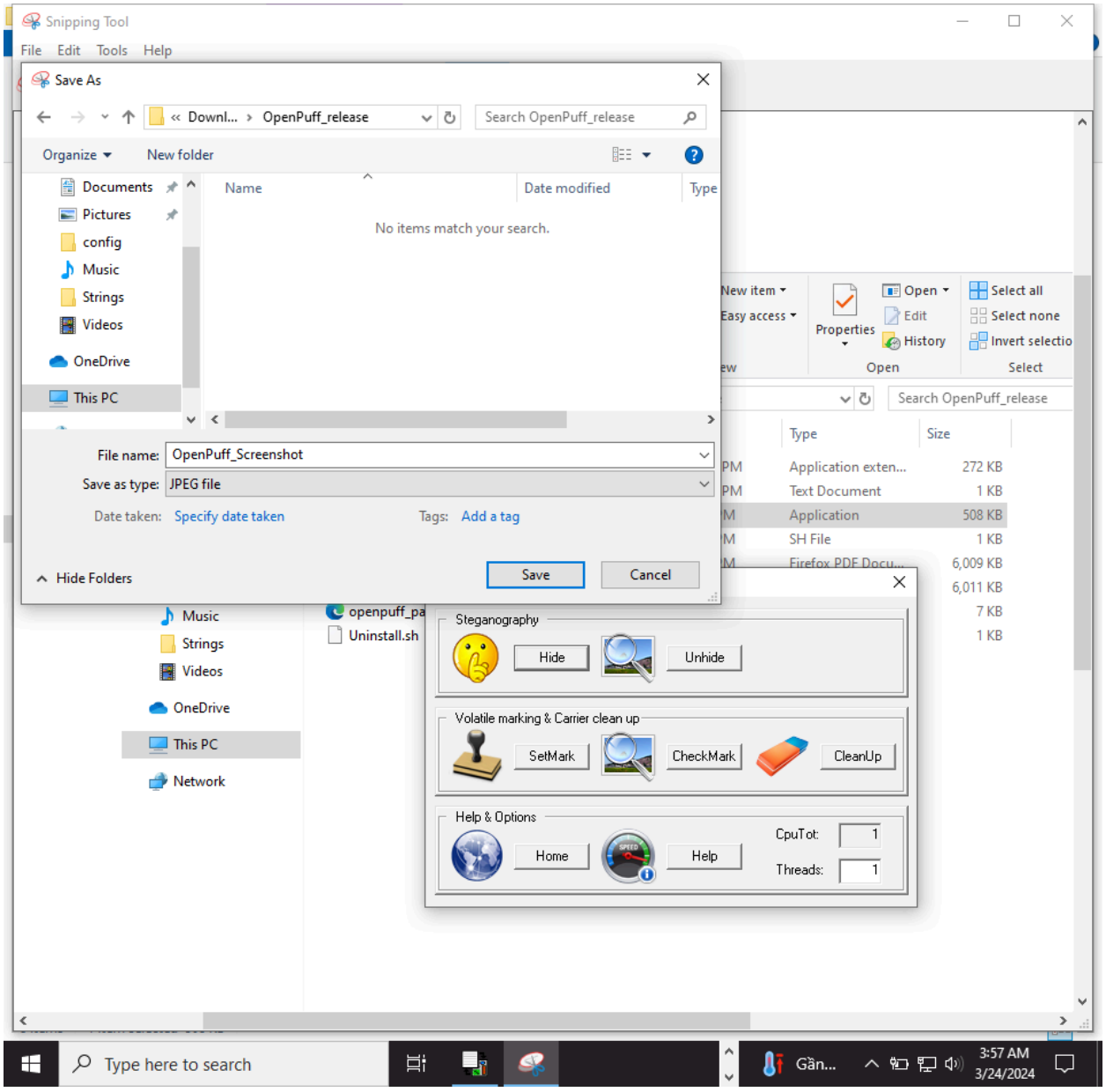


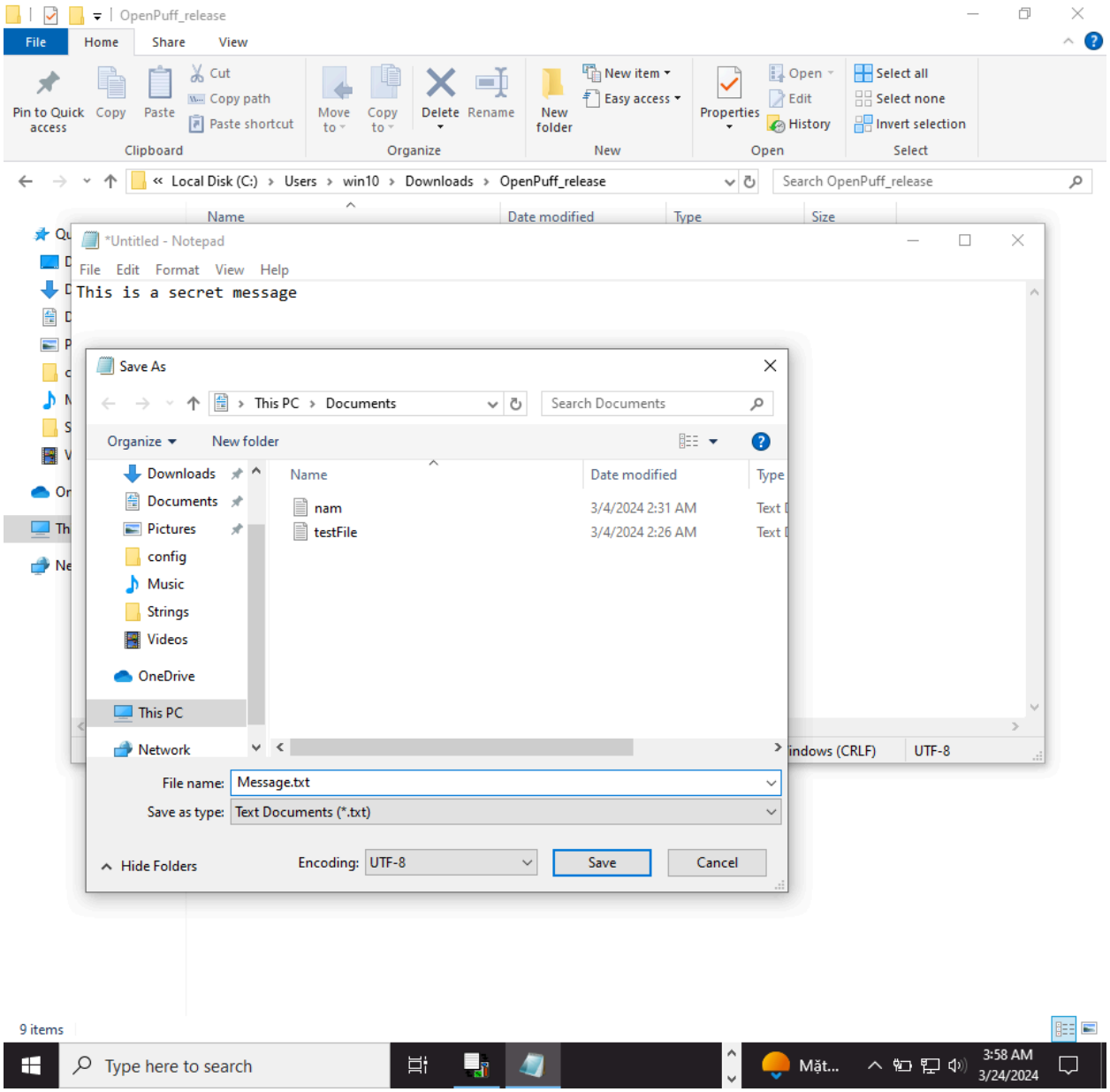
OpenPuff v4.01 Steganography & Watermarking

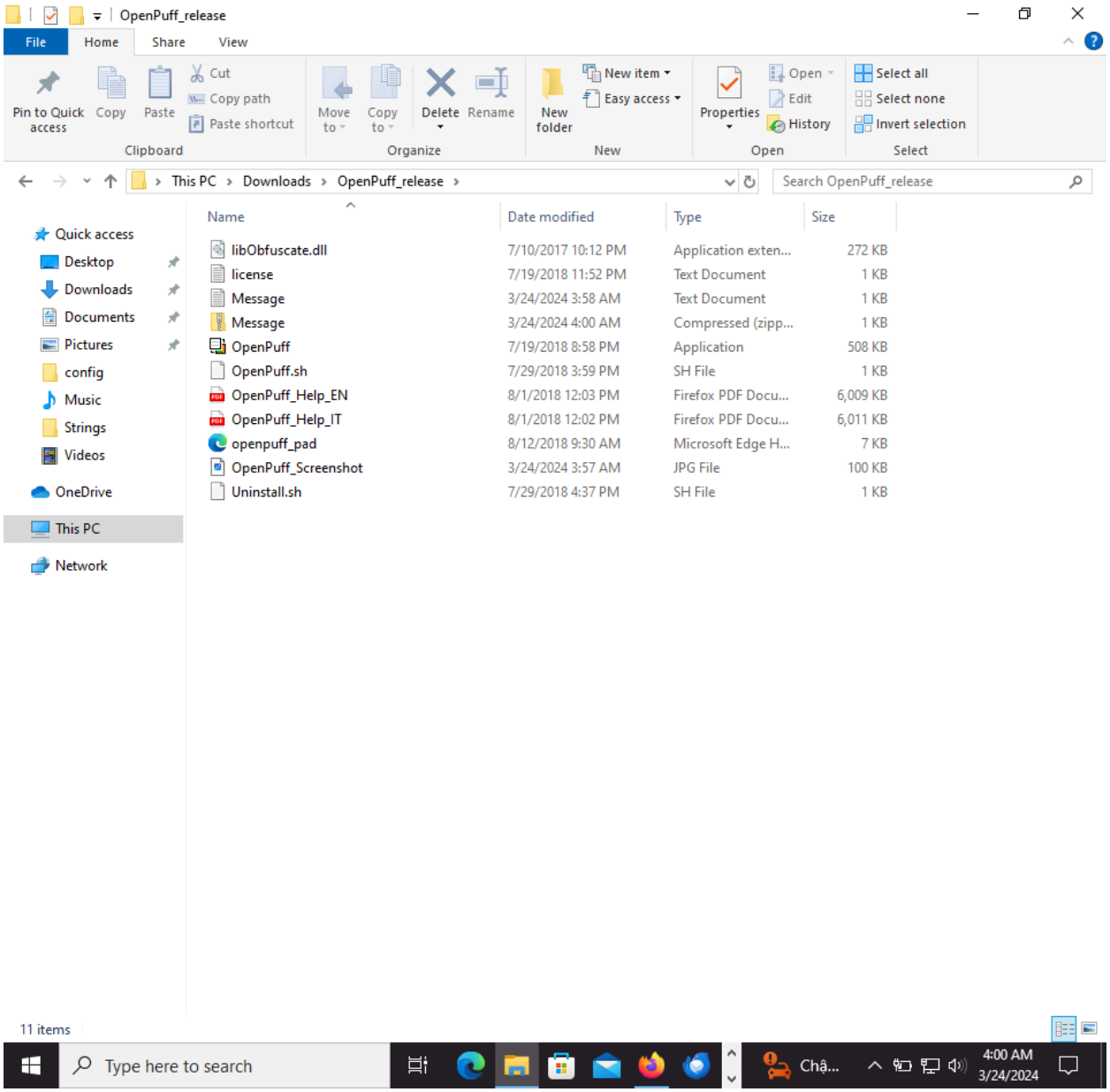
Data hiding and watermarking made easy, safe and free
EmbeddedSW © 2018
Send your suggestions, comments, bug reports, requests
to *embedded@embeddedsw.net* – *Skype "embeddedsw.company"*

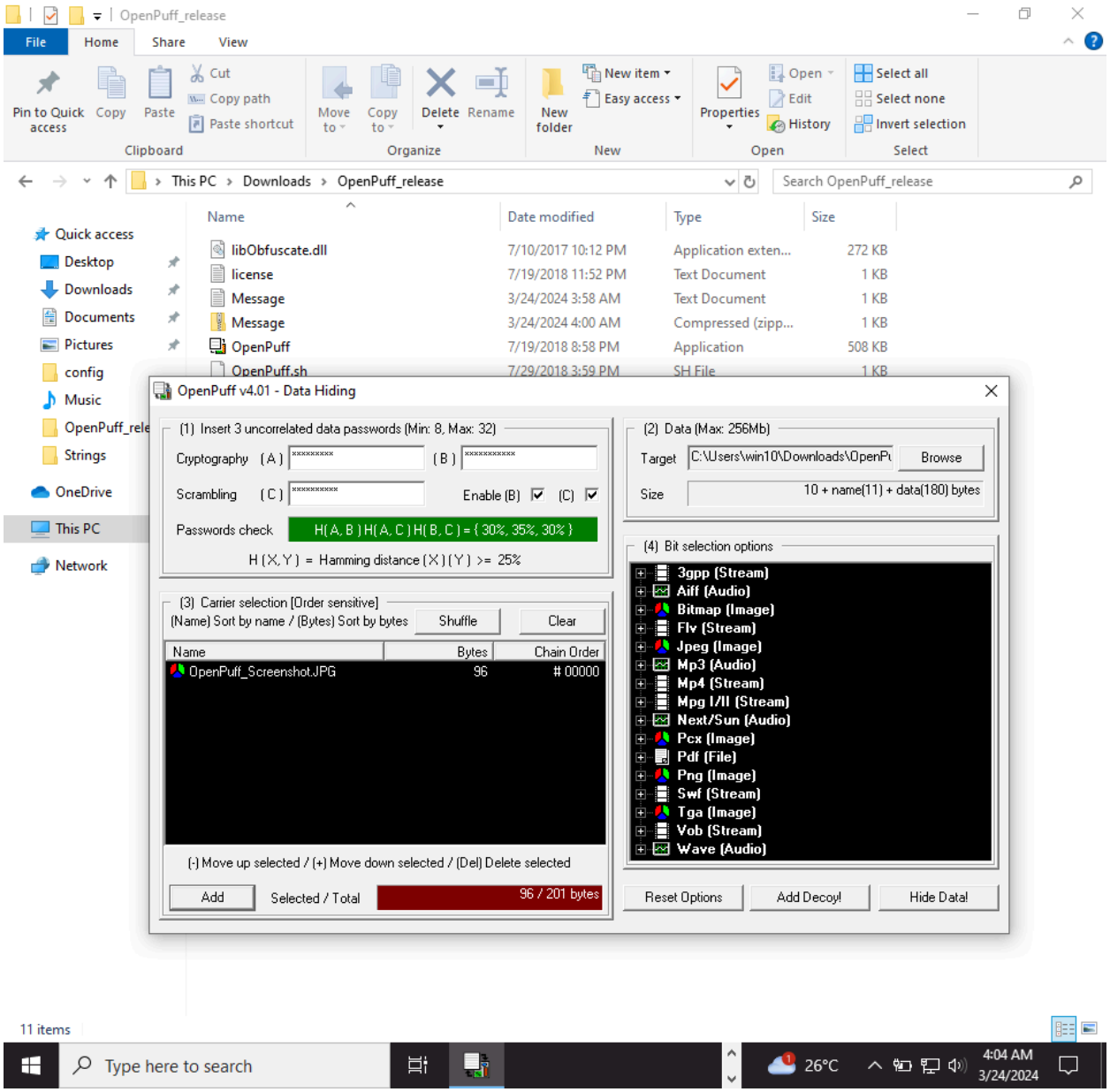
OpenPuff HomePage

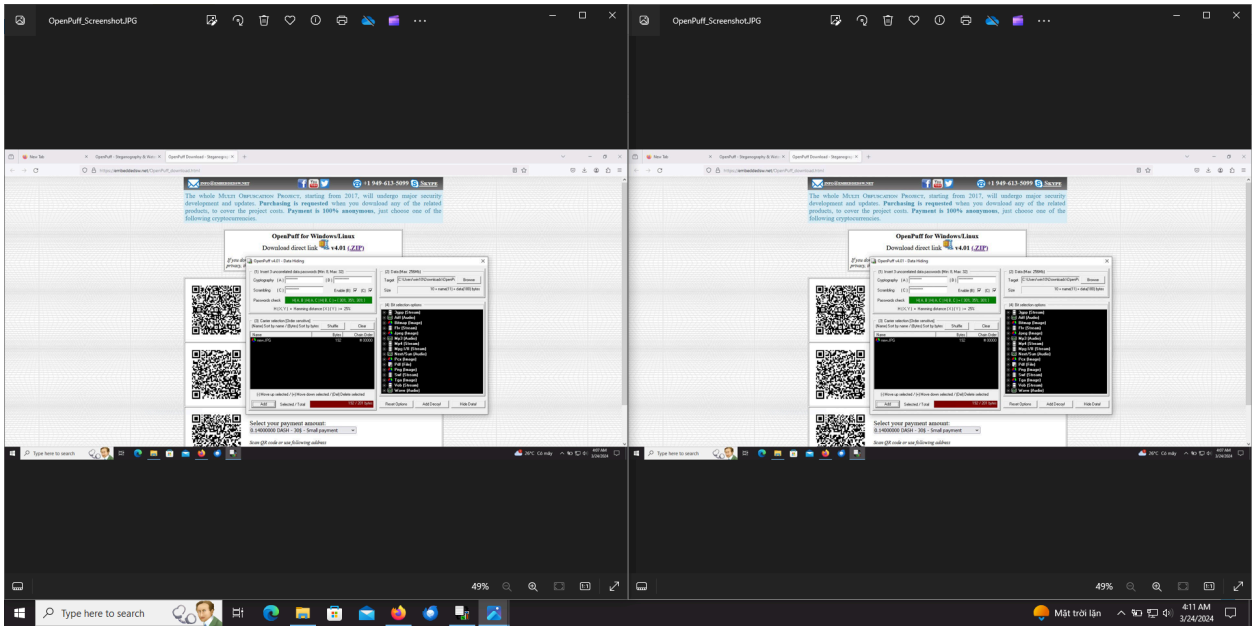

OpenPuff_release
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
« Local Disk (C:) › Users › win10 › Downloads › OpenPuff_release
Search OpenPuff_release
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
libObfuscate.dll 7/10/2017 10:12 PM Application exten... 272 KB
license 7/19/2018 11:52 PM Text Document 1 KB
OpenPuff 7/19/2018 8:58 PM Application 508 KB
OpenPuff.sh 7/29/2018 3:59 PM SH File 1 KB
OpenPuff_Help_EN 8/1/2018 12:03 PM Firefox PDF Docu... 6,009 KB
OpenPuff_Help_IT 8/1/2018 12:02 PM Firefox PDF Docu... 6,011 KB
openpuff_pad 8/12/2018 9:30 AM Microsoft Edge H... 7 KB
Uninstall.sh 7/29/2018 4:37 PM SH File 1 KB
8 items
Type here to search
Gần...
3:55 AM
3/24/2024


Snipping Tool
File Edit Tools Help
Save As
Organize
New folder
Documents
Pictures
config
Music
Strings
Videos
OneDrive
This PC
Name
Date modified
Type
No items match your search.
File name: OpenPuff_Screenshot
Save as type: JPEG file
Date taken: Specify date taken
Tags: Add a tag
Hide Folders
Save
Cancel
Steganography
Hide
Unhide
Volatile marking & Carrier clean up
SetMark
CheckMark
CleanUp
Help & Options
Home
Help
CpuTot:
Threads:
Search OpenPuff_release
Application exten... 272 KB
Text Document 1 KB
Application 508 KB
SH File 1 KB
6,009 KB
6,011 KB
7 KB
1 KB
openpuff_pa
Uninstall.sh
Network
Type here to search
3:57 AM
3/24/2024

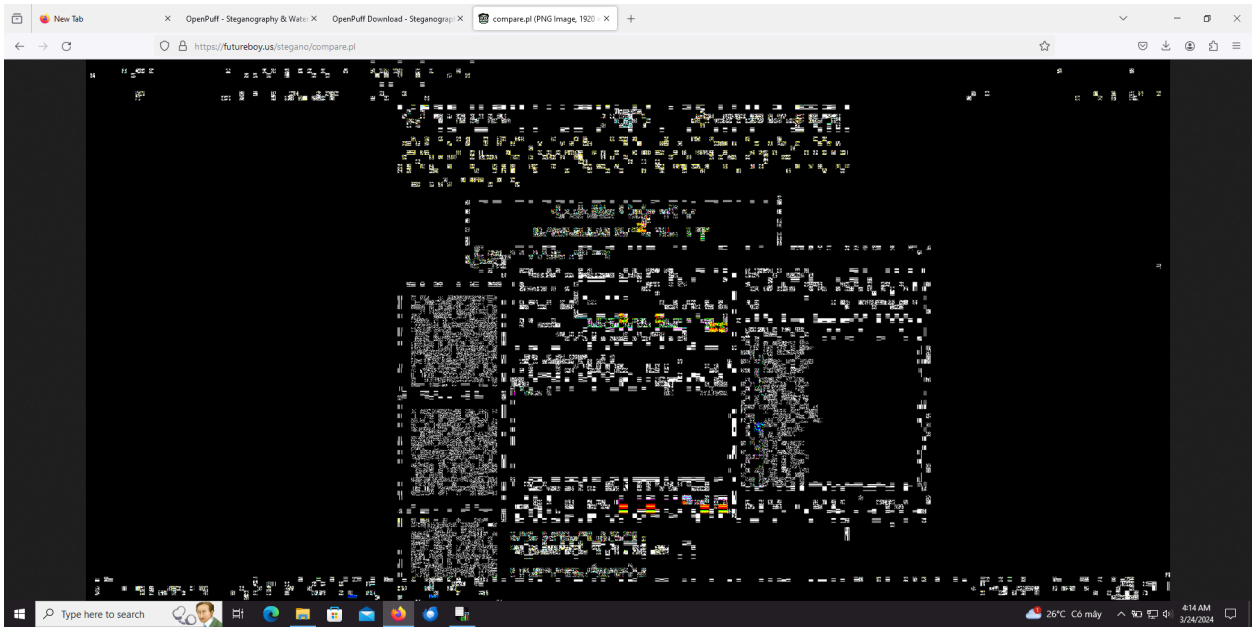

OpenPuff_release
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
« Local Disk (C:) › Users › win10 › Downloads › OpenPuff_release
Search OpenPuff_release
Name
Date modified
Type
Size
*Untitled - Notepad
File Edit Format View Help
This is a secret message
Save As
This PC › Documents
Search Documents
Organize
New folder
Downloads
Documents
Pictures
config
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
nam
3/4/2024 2:31 AM
testFile
3/4/2024 2:26 AM
File name: Message.txt
Save as type: Text Documents (*.txt)
Hide Folders
Encoding: UTF-8
Save
Cancel
9 items
Type here to search
Mặt...
3:58 AM
3/24/2024


OpenPuff_release
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › OpenPuff_release ›
Search OpenPuff_release
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
Strings
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
libObfuscate.dll 7/10/2017 10:12 PM Application exten... 272 KB
license 7/19/2018 11:52 PM Text Document 1 KB
Message 3/24/2024 3:58 AM Text Document 1 KB
Message 3/24/2024 4:00 AM Compressed (zipp... 1 KB
OpenPuff 7/19/2018 8:58 PM Application 508 KB
OpenPuff.sh 7/29/2018 3:59 PM SH File 1 KB
OpenPuff_Help_EN 8/1/2018 12:03 PM Firefox PDF Docu... 6,009 KB
OpenPuff_Help_IT 8/1/2018 12:02 PM Firefox PDF Docu... 6,011 KB
openpuff_pad 8/12/2018 9:30 AM Microsoft Edge H... 7 KB
OpenPuff_Screenshot 3/24/2024 3:57 AM JPG File 100 KB
Uninstall.sh 7/29/2018 4:37 PM SH File 1 KB
11 items
Type here to search
Chậ...
4:00 AM
3/24/2024

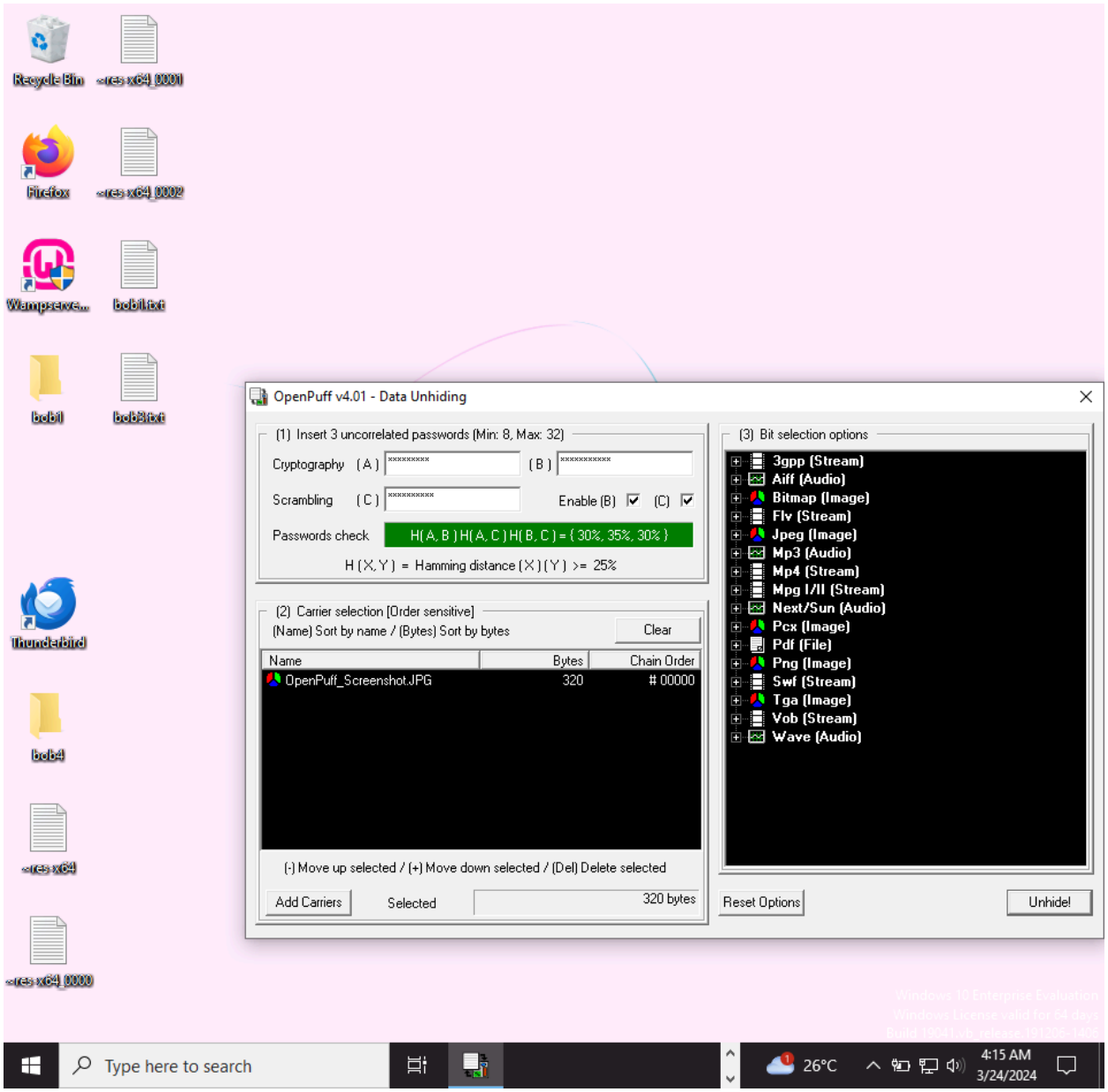

OpenPuff_release
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › OpenPuff_release
Search OpenPuff_release
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
OpenPuff_rele
Strings
OneDrive
This PC
Network
Name
Date modified
Type
Size
libObfuscate.dll 7/10/2017 10:12 PM Application exten... 272 KB
license 7/19/2018 11:52 PM Text Document 1 KB
Message 3/24/2024 3:58 AM Text Document 1 KB
Message 3/24/2024 4:00 AM Compressed (zipp... 1 KB
OpenPuff 7/19/2018 8:58 PM Application 508 KB
OpenPuff.sh 7/29/2018 3:59 PM SH File 1 KB
OpenPuff v4.01 - Data Hiding
(1) Insert 3 uncorrelated data passwords (Min: 8, Max: 32)
Cryptography (A)
(B)
Scrambling (C)
Enable (B) (C)
Passwords check
H(A, B) H(A, C) H(B, C) = { 30%, 35%, 30% }
H(X, Y) = Hamming distance (X) (Y) >= 25%
(2) Data (Max: 256Mb)
Target C:\Users\win10\Downloads\OpenPu
Browse
Size
10 + name(11) + data(180) bytes
(3) Carrier selection [Order sensitive]
(Name) Sort by name / (Bytes) Sort by bytes
Shuffle
Clear
Name
Bytes
Chain Order
OpenPuff_Screenshot.JPG 96 # 00000
(-) Move up selected / (+) Move down selected / (Del) Delete selected
Add
Selected / Total
96 / 201 bytes
(4) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
Jpeg (Image)
Mp3 (Audio)
Mp4 (Stream)
Mpg I/II (Stream)
Next/Sun (Audio)
Pcx (Image)
Pdf (File)
Png (Image)
Swf (Stream)
Tga (Image)
Vob (Stream)
Wave (Audio)
Reset Options
Add Decoy!
Hide Data!
11 items
Type here to search
26°C
4:04 AM
3/24/2024

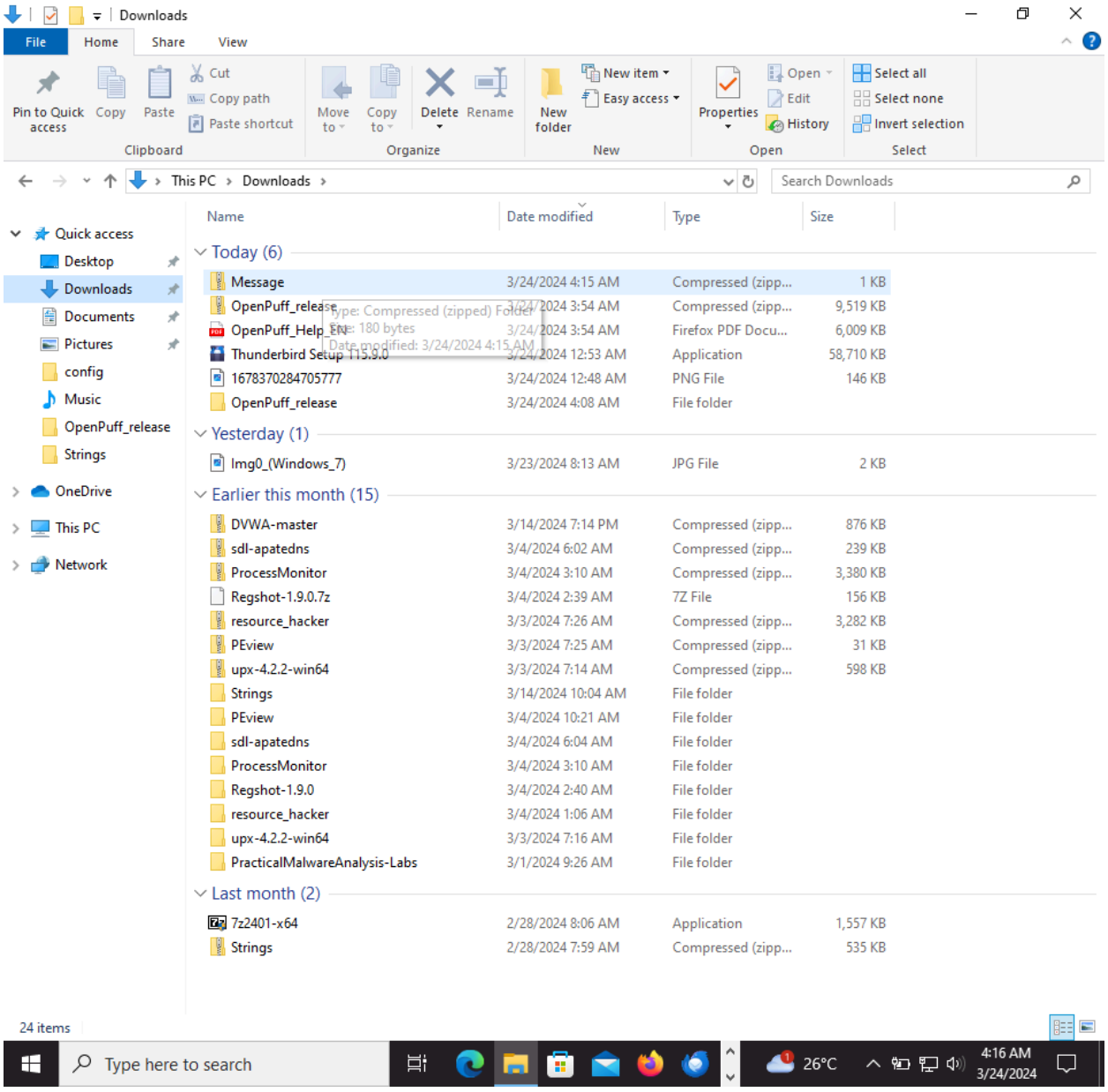


So sánh giữa ảnh qua steganography và ảnh gốc, ta thấy không có thay đổi đáng kể

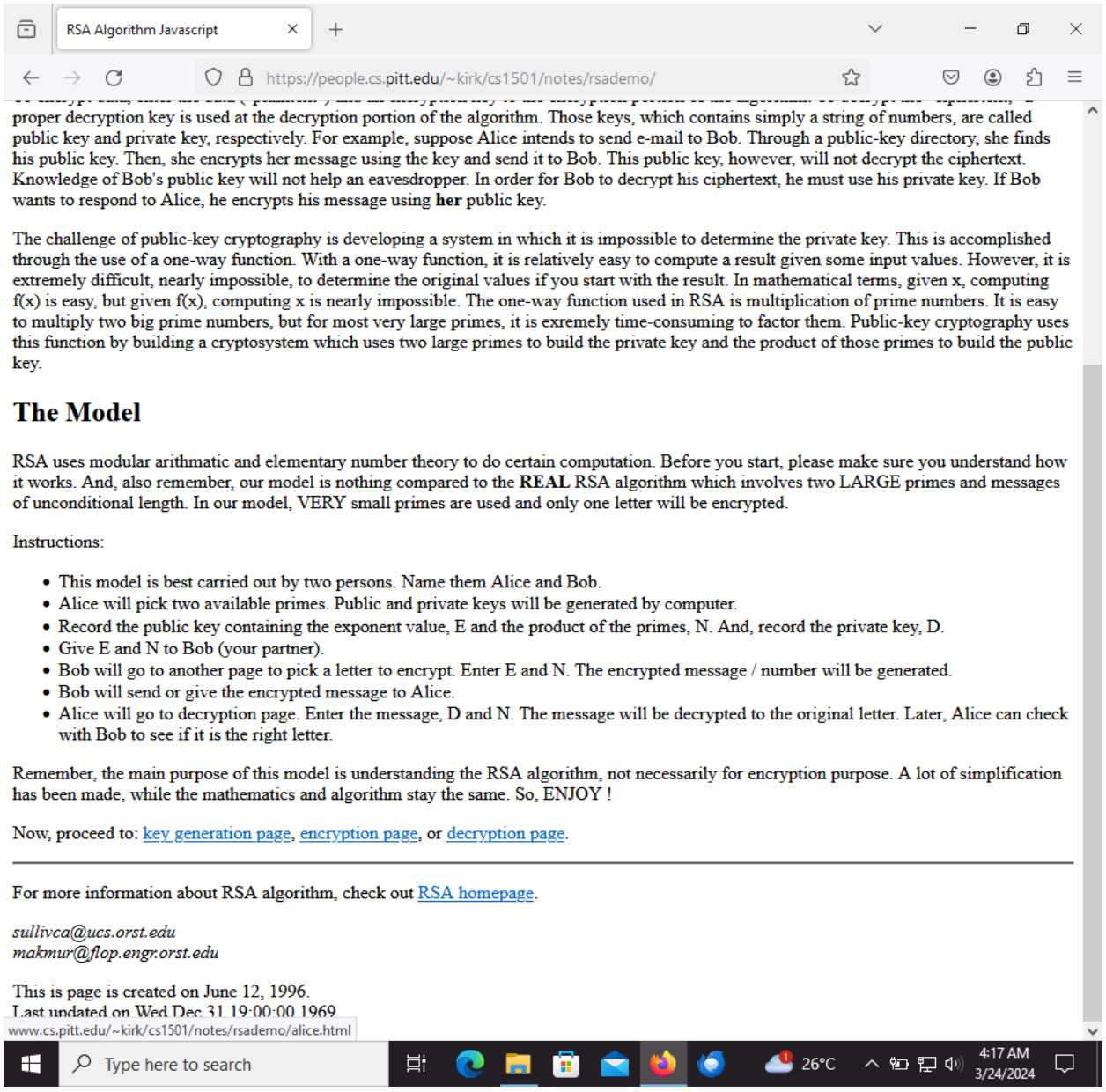


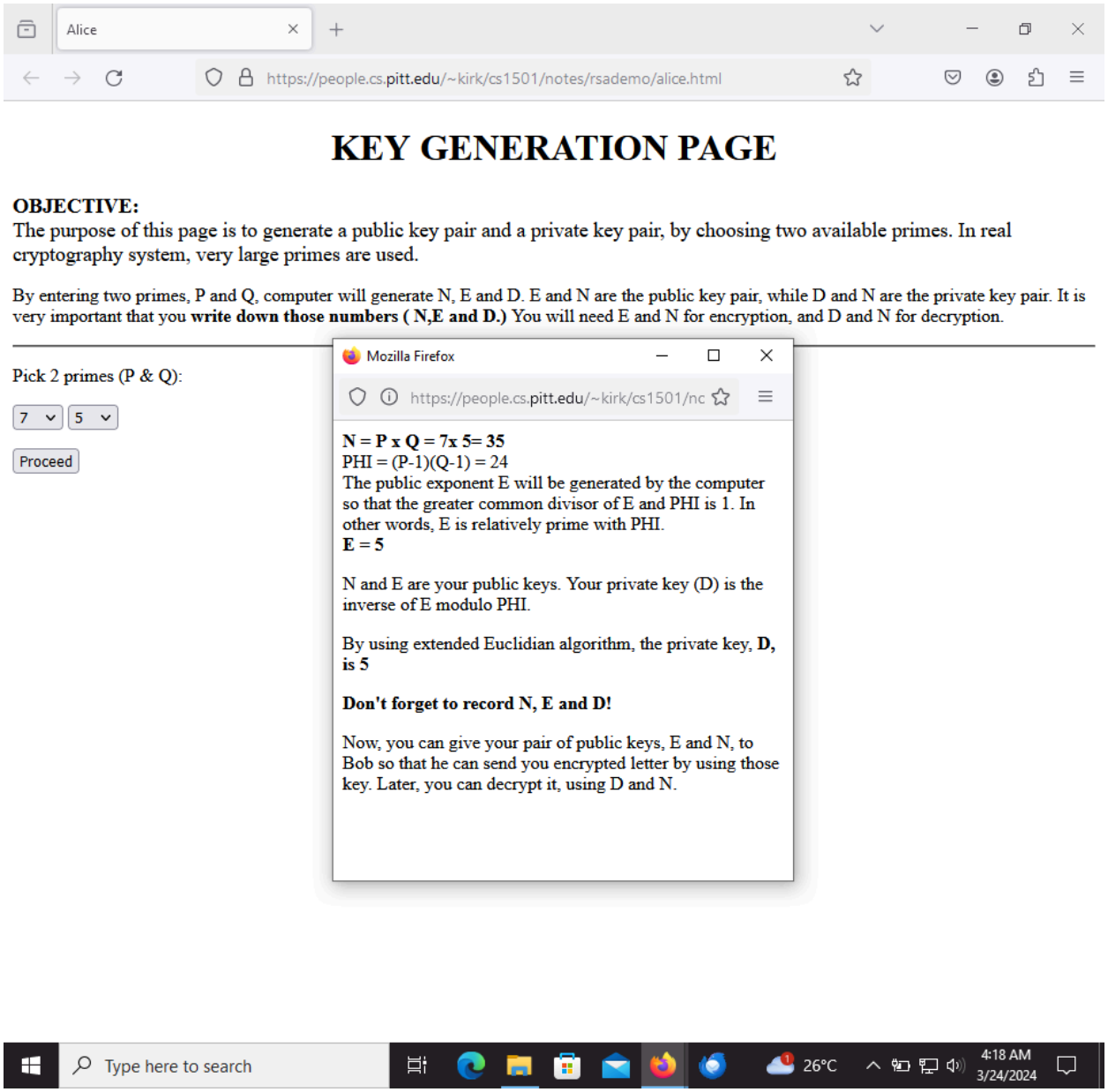
So sánh giữa 2 ảnh bằng máy mới thấy có những chênh lệch nhỏ

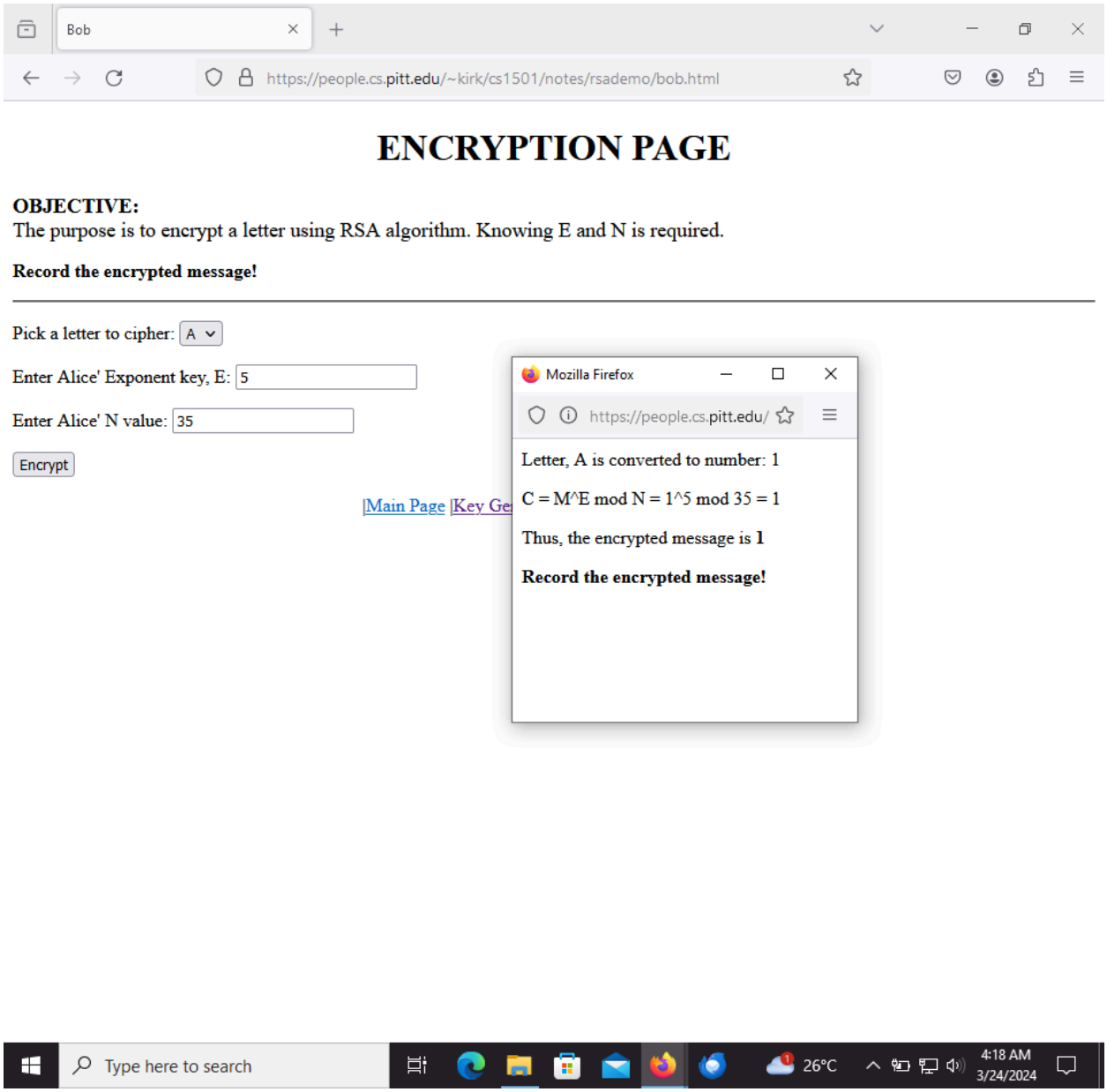

Recycle Bin
~res x64 0001
Firefox
~res x64 0002
Wampserve...
bob1.txt
bob1
bob2.txt
Thunderbird
bob4
~res x64
~res x64 0000
OpenPuff v4.01 - Data Unhiding
(1) Insert 3 uncorrelated passwords (Min: 8, Max: 32)
Cryptography (A)
(B)
Scrambling (C)
Enable (B) (C)
Passwords check
H(A, B) H(A, C) H(B, C) = (30%, 35%, 30%)
H (X, Y) = Hamming distance (X) (Y) >= 25%
(2) Carrier selection [Order sensitive]
(Name) Sort by name / (Bytes) Sort by bytes
Clear
Name
Bytes
Chain Order
OpenPuff_Screenshot.JPG
320
00000
(-) Move up selected / (+) Move down selected / (Del) Delete selected
Add Carriers
Selected
320 bytes
(3) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
Jpeg (Image)
Mp3 (Audio)
Mp4 (Stream)
Mpg I/II (Stream)
Next/Sun (Audio)
Pcx (Image)
Pdf (File)
Png (Image)
Swf (Stream)
Tga (Image)
Vob (Stream)
Wave (Audio)
Reset Options
Unhide!
Type here to search
26°C
4:15 AM
3/24/2024

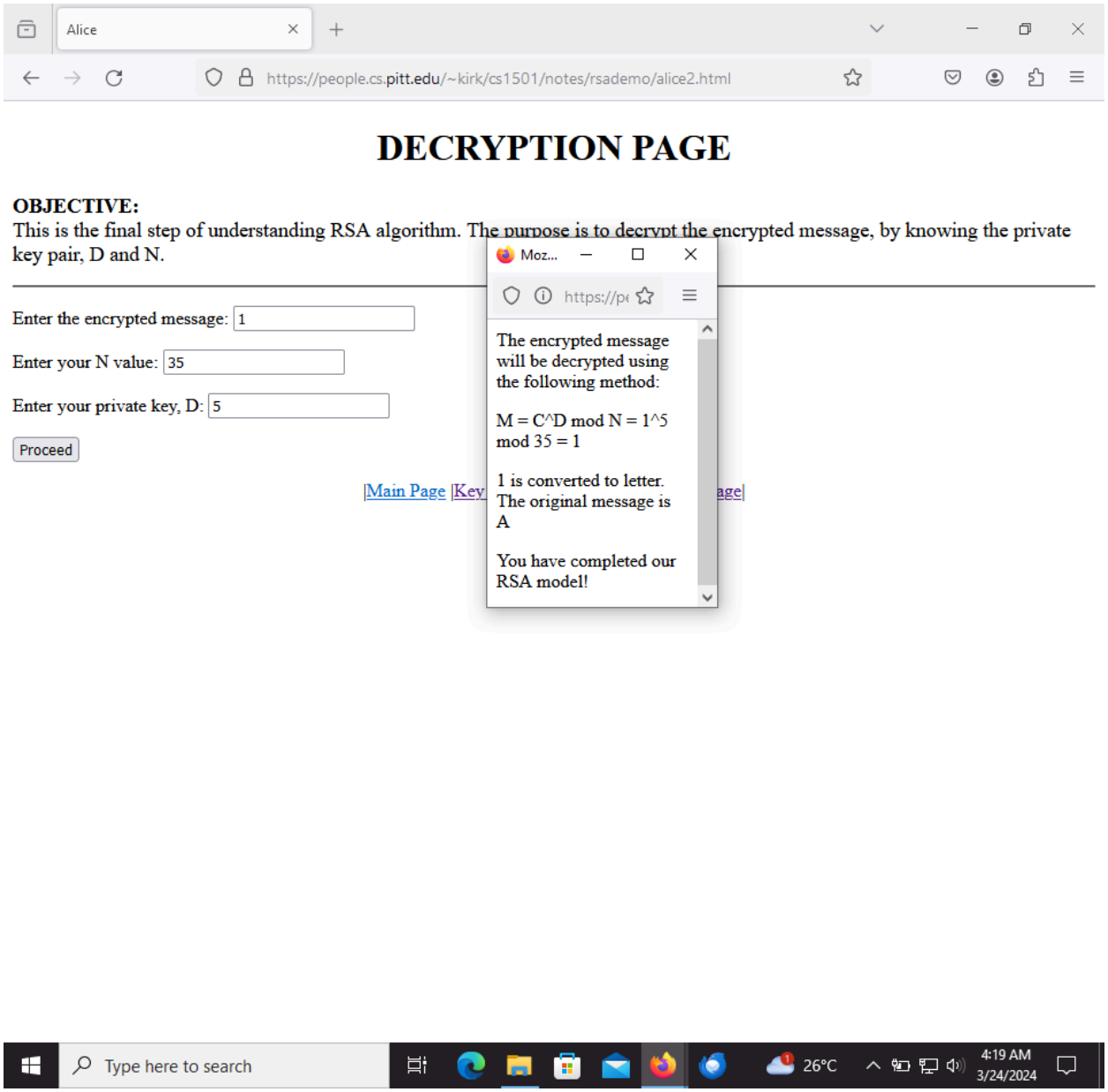

Downloads
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads ›
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
config
Music
OpenPuff_release
Strings
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (6)
Message 3/24/2024 4:15 AM Compressed (zipp... 1 KB
OpenPuff_release 3/24/2024 3:54 AM Compressed (zipp... 9,519 KB
OpenPuff_Help_EN 3/24/2024 3:54 AM Firefox PDF Docu... 6,009 KB
Thunderbird Setup 115.9.0 3/24/2024 12:53 AM Application 58,710 KB
1678370284705777 3/24/2024 12:48 AM PNG File 146 KB
OpenPuff_release 3/24/2024 4:08 AM File folder
Type: Compressed (zipped) Folder
Size: 180 bytes
Date modified: 3/24/2024 4:15 AM
Yesterday (1)
Img0_(Windows_7) 3/23/2024 8:13 AM JPG File 2 KB
Earlier this month (15)
DVWA-master 3/14/2024 7:14 PM Compressed (zipp... 876 KB
sdl-apatedns 3/4/2024 6:02 AM Compressed (zipp... 239 KB
ProcessMonitor 3/4/2024 3:10 AM Compressed (zipp... 3,380 KB
Regshot-1.9.0.7z 3/4/2024 2:39 AM 7Z File 156 KB
resource_hacker 3/3/2024 7:26 AM Compressed (zipp... 3,282 KB
PEview 3/3/2024 7:25 AM Compressed (zipp... 31 KB
upx-4.2.2-win64 3/3/2024 7:14 AM Compressed (zipp... 598 KB
Strings 3/14/2024 10:04 AM File folder
PEview 3/4/2024 10:21 AM File folder
sdl-apatedns 3/4/2024 6:04 AM File folder
ProcessMonitor 3/4/2024 3:10 AM File folder
Regshot-1.9.0 3/4/2024 2:40 AM File folder
resource_hacker 3/4/2024 1:06 AM File folder
upx-4.2.2-win64 3/3/2024 7:16 AM File folder
PracticalMalwareAnalysis-Labs 3/1/2024 9:26 AM File folder
Last month (2)
7z2401-x64 2/28/2024 8:06 AM Application 1,557 KB
Strings 2/28/2024 7:59 AM Compressed (zipp... 535 KB
24 items
Type here to search
26°C
4:16 AM
3/24/2024

Project 6.2

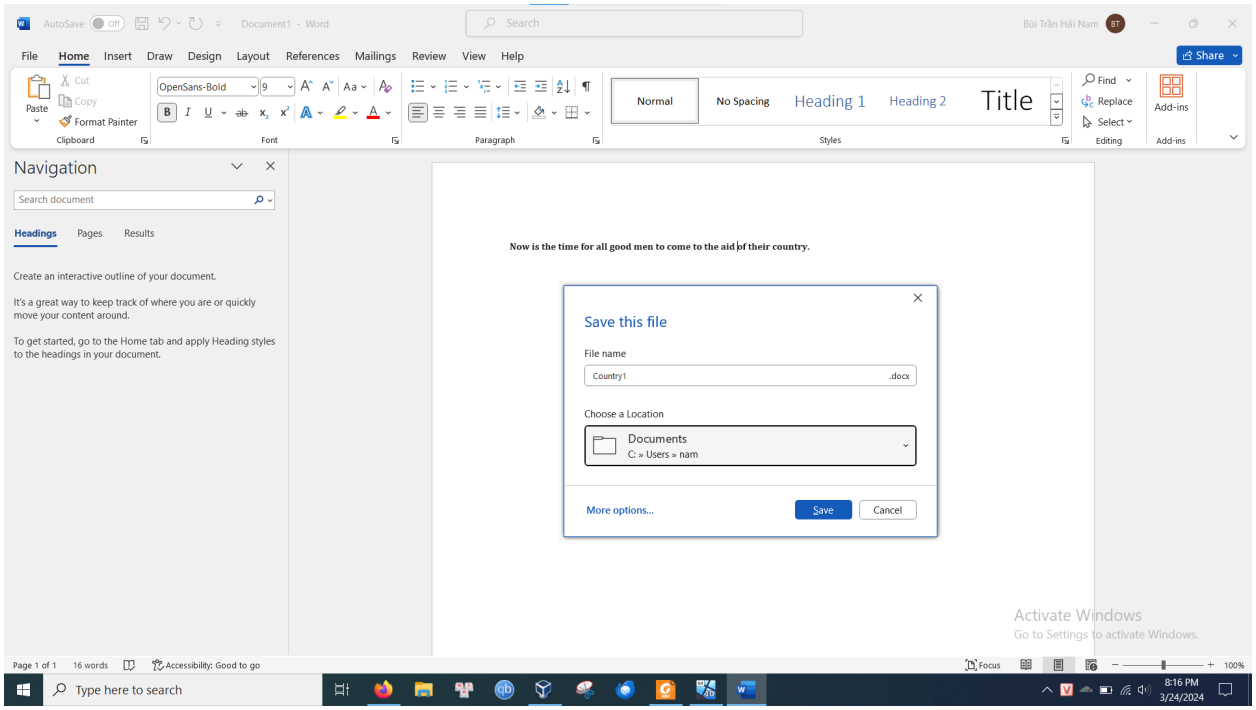

RSA Algorithm Javascript
https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/
proper decryption key is used at the decryption portion of the algorithm. Those keys, which contains simply a string of numbers, are called public key and private key, respectively. For example, suppose Alice intends to send e-mail to Bob. Through a public-key directory, she finds his public key. Then, she encrypts her message using the key and send it to Bob. This public key, however, will not decrypt the ciphertext. Knowledge of Bob's public key will not help an eavesdropper. In order for Bob to decrypt his ciphertext, he must use his private key. If Bob wants to respond to Alice, he encrypts his message using her public key.
The challenge of public-key cryptography is developing a system in which it is impossible to determine the private key. This is accomplished through the use of a one-way function. With a one-way function, it is relatively easy to compute a result given some input values. However, it is extremely difficult, nearly impossible, to determine the original values if you start with the result. In mathematical terms, given x, computing f(x) is easy, but given f(x), computing x is nearly impossible. The one-way function used in RSA is multiplication of prime numbers. It is easy to multiply two big prime numbers, but for most very large primes, it is exremely time-consuming to factor them. Public-key cryptography uses this function by building a cryptosystem which uses two large primes to build the private key and the product of those primes to build the public key.
The Model
RSA uses modular arithmatic and elementary number theory to do certain computation. Before you start, please make sure you understand how it works. And, also remember, our model is nothing compared to the REAL RSA algorithm which involves two LARGE primes and messages of unconditional length. In our model, VERY small primes are used and only one letter will be encrypted.
Instructions:
This model is best carried out by two persons. Name them Alice and Bob.
Alice will pick two available primes. Public and private keys will be generated by computer.
Record the public key containing the exponent value, E and the product of the primes, N. And, record the private key, D.
Give E and N to Bob (your partner).
Bob will go to another page to pick a letter to encrypt. Enter E and N. The encrypted message / number will be generated.
Bob will send or give the encrypted message to Alice.
Alice will go to decryption page. Enter the message, D and N. The message will be decrypted to the original letter. Later, Alice can check with Bob to see if it is the right letter.
Remember, the main purpose of this model is understanding the RSA algorithm, not necessarily for encryption purpose. A lot of simplification has been made, while the mathematics and algorithm stay the same. So, ENJOY !
Now, proceed to: key generation page, encryption page, or decryption page.
For more information about RSA algorithm, check out RSA homepage.
sullivca@ucs.orst.edu
makmur@flop.engr.orst.edu
This is page is created on June 12, 1996.
Last updated on Wed Dec 31 19:00:00 1969
www.cs.pitt.edu/~kirk/cs1501/notes/rsademo/alice.html
Type here to search
26°C
4:17 AM
3/24/2024

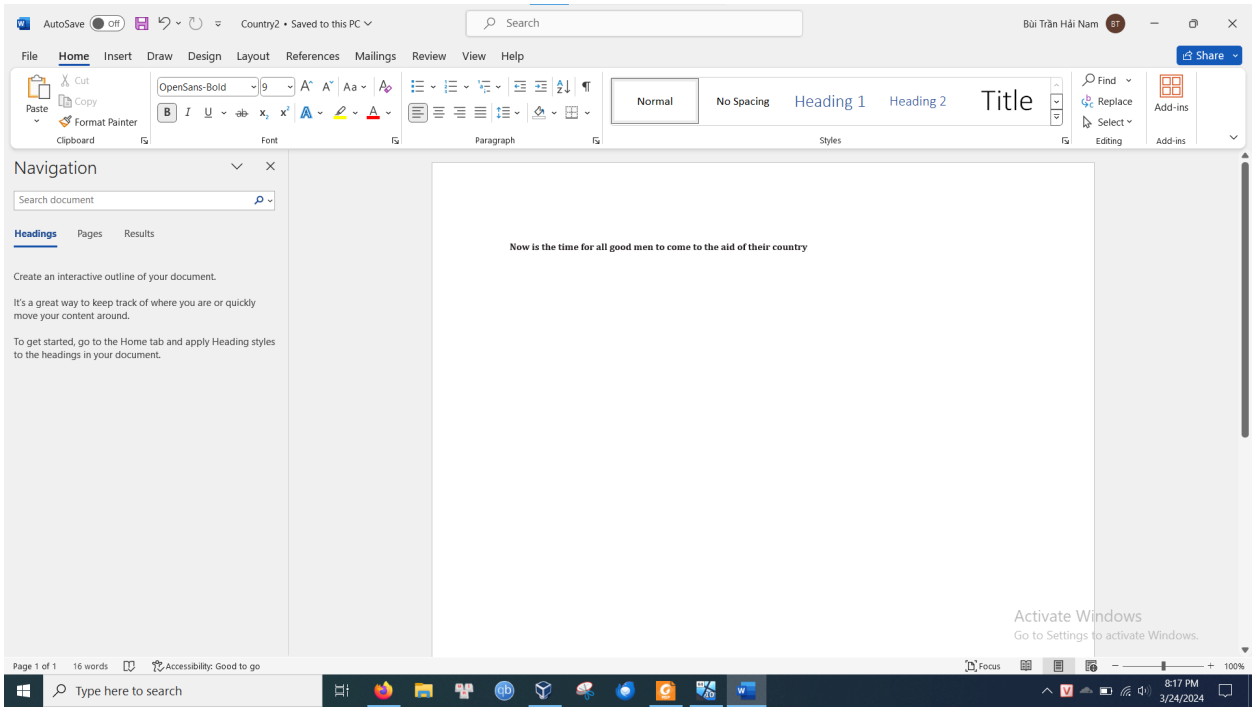

Alice
https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/alice.html
KEY GENERATION PAGE
OBJECTIVE:
The purpose of this page is to generate a public key pair and a private key pair, by choosing two available primes. In real cryptography system, very large primes are used.
By entering two primes, P and Q, computer will generate N, E and D. E and N are the public key pair, while D and N are the private key pair. It is very important that you write down those numbers (N,E and D.) You will need E and N for encryption, and D and N for decryption.
Pick 2 primes (P & Q):
7
5
Proceed
Mozilla Firefox
https://people.cs.pitt.edu/~kirk/cs1501/nc
N = P x Q = 7x 5= 35
PHI = (P-1)(Q-1) = 24
The public exponent E will be generated by the computer so that the greater common divisor of E and PHI is 1. In other words, E is relatively prime with PHI.
E = 5
N and E are your public keys. Your private key (D) is the inverse of E modulo PHI.
By using extended Euclidian algorithm, the private key, D, is 5
Don't forget to record N, E and D!
Now, you can give your pair of public keys, E and N, to Bob so that he can send you encrypted letter by using those key. Later, you can decrypt it, using D and N.
Type here to search
26°C
4:18 AM
3/24/2024

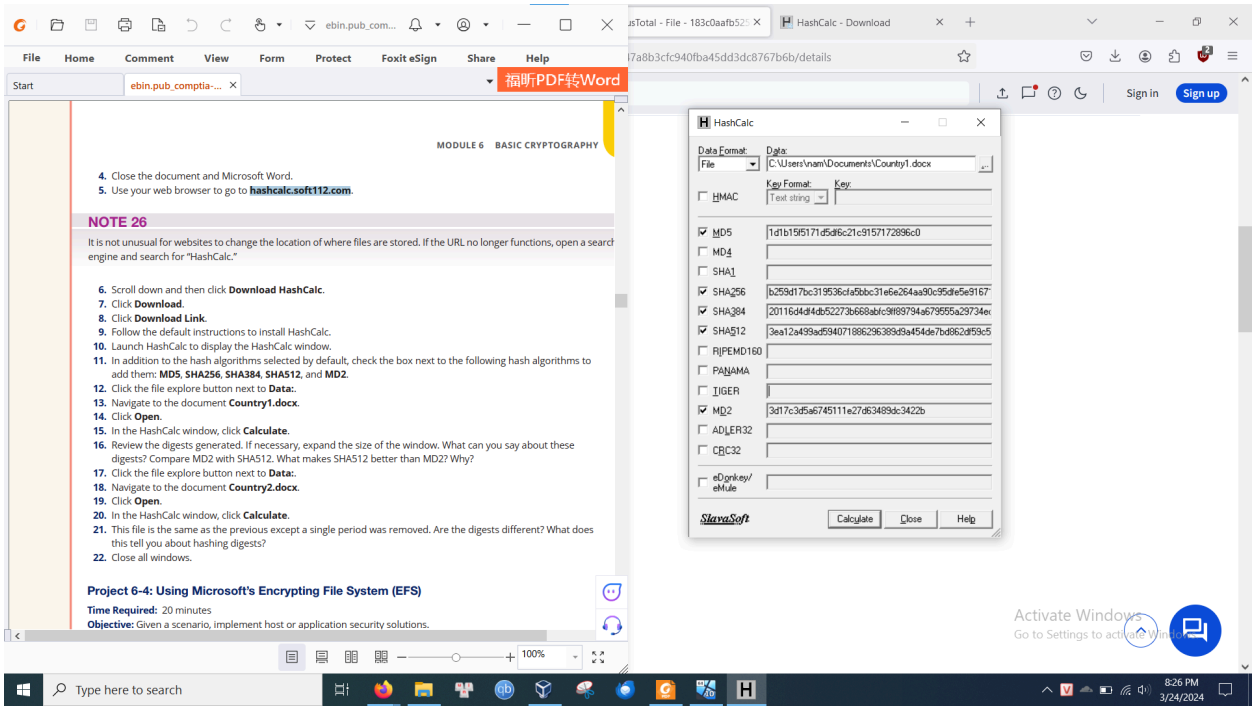

Bob
https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/bob.html
ENCRYPTION PAGE
OBJECTIVE:
The purpose is to encrypt a letter using RSA algorithm. Knowing E and N is required.
Record the encrypted message!
Pick a letter to cipher: A
Enter Alice' Exponent key, E: 5
Enter Alice' N value: 35
Encrypt
|Main Page |Key Ge
Mozilla Firefox
https://people.cs.pitt.edu/
Letter, A is converted to number: 1
C = M^E mod N = 1^5 mod 35 = 1
Thus, the encrypted message is 1
Record the encrypted message!
Type here to search
26°C
4:18 AM
3/24/2024


Alice
https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/alice2.html
DECRYPTION PAGE
OBJECTIVE:
This is the final step of understanding RSA algorithm. The purpose is to decrypt the encrypted message, by knowing the private key pair, D and N.
Enter the encrypted message: 1
Enter your N value: 35
Enter your private key, D: 5
Proceed
|Main Page |Key
age|
Moz...
https://p
The encrypted message will be decrypted using the following method:
M = C^D mod N = 1^5 mod 35 = 1
1 is converted to letter. The original message is A
You have completed our RSA model!
Type here to search
26°C
4:19 AM
3/24/2024

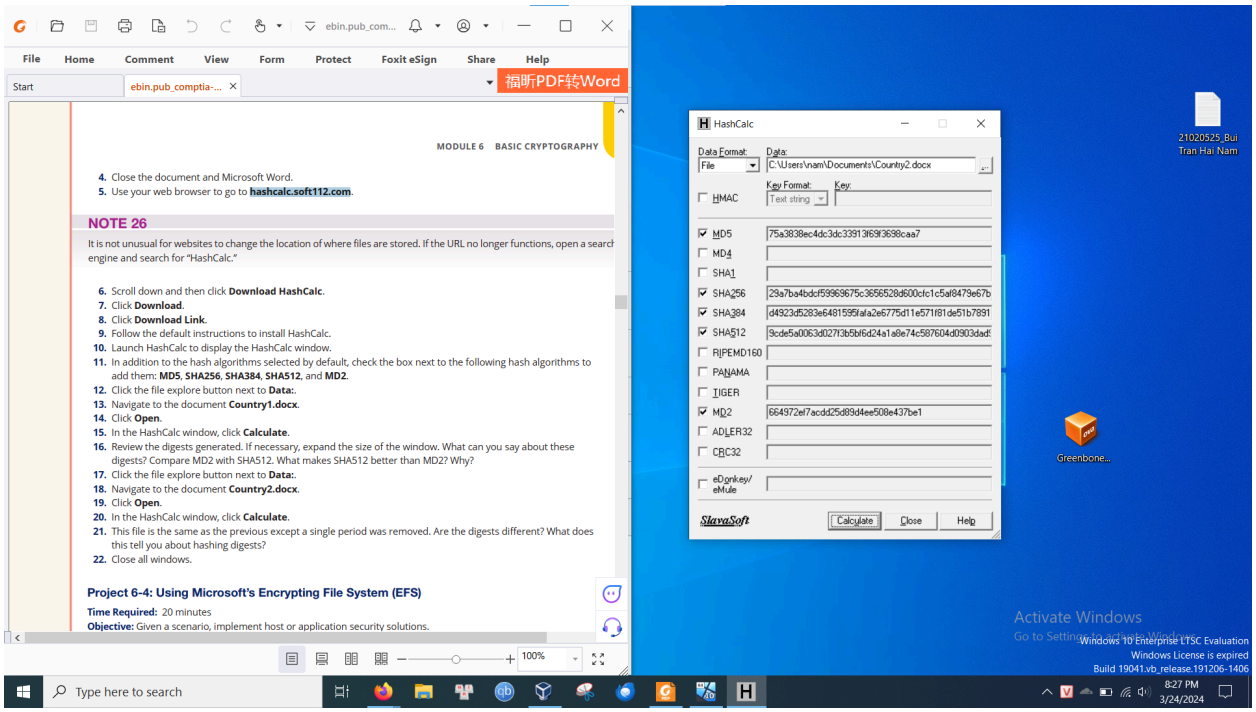
Project 6.3


Document1 - Word
Search
Bùi Trần Hải Nam
File Home Insert Draw Design Layout References Mailings Review View Help
Share
Paste Cut Copy Format Painter
OpenSans-Bold 9
Normal No Spacing Heading 1 Heading 2 Title
Find Replace Select
Add-ins
Clipboard Font Paragraph Styles Editing Add-ins
Navigation
Search document
Headings Pages Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading styles to the headings in your document.
Now is the time for all good men to come to the aid of their country.
Save this file
File name
Country1
.docx
Choose a Location
Documents
C: » Users » nam
More options...
Save
Cancel
Activate Windows
Go to Settings to activate Windows.
Page 1 of 1
16 words
Accessibility: Good to go
Focus
100%
Type here to search
8:16 PM
3/24/2024


Country2 • Saved to this PC
Search
Bùi Trần Hải Nam
File Home Insert Draw Design Layout References Mailings Review View Help
Share
Paste Cut Copy Format Painter
OpenSans-Bold 9
Normal No Spacing Heading 1 Heading 2 Title
Find Replace Select
Add-ins
Clipboard Font Paragraph Styles Editing Add-ins
Navigation
Search document
Headings Pages Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading styles to the headings in your document.
Now is the time for all good men to come to the aid of their country
Activate Windows
Go to Settings to activate Windows.
Page 1 of 1
16 words
Accessibility: Good to go
Focus
100%
Type here to search
8:17 PM
3/24/2024

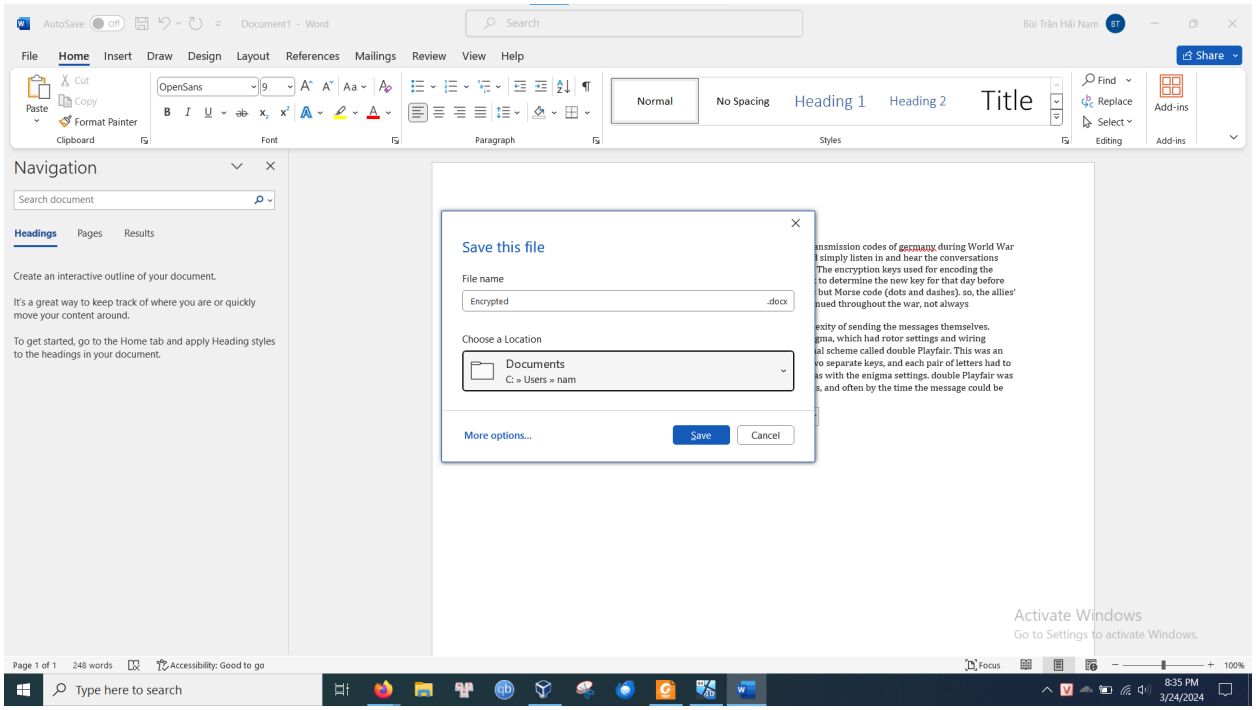


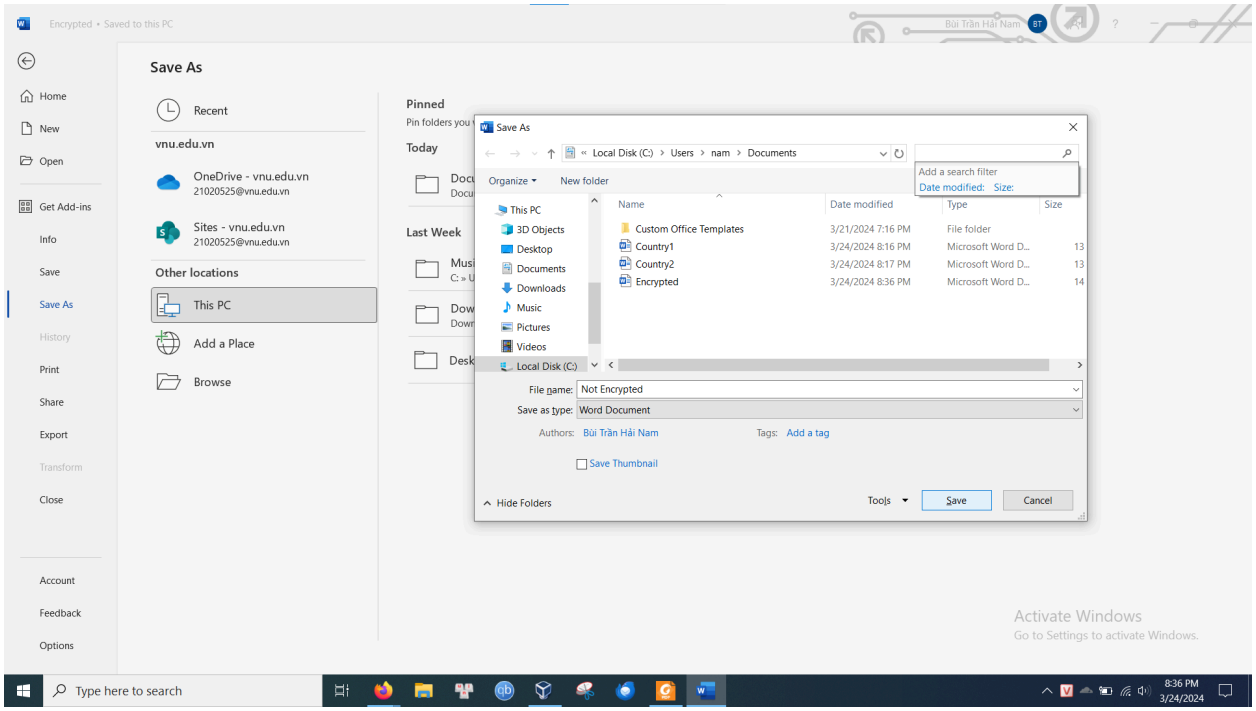
Hash MD2 ngắn hơn so với SHA512. Do đó các kiểu tấn công dựa vào hash collision sẽ khó xảy ra trên SHA512 hơn là MD2

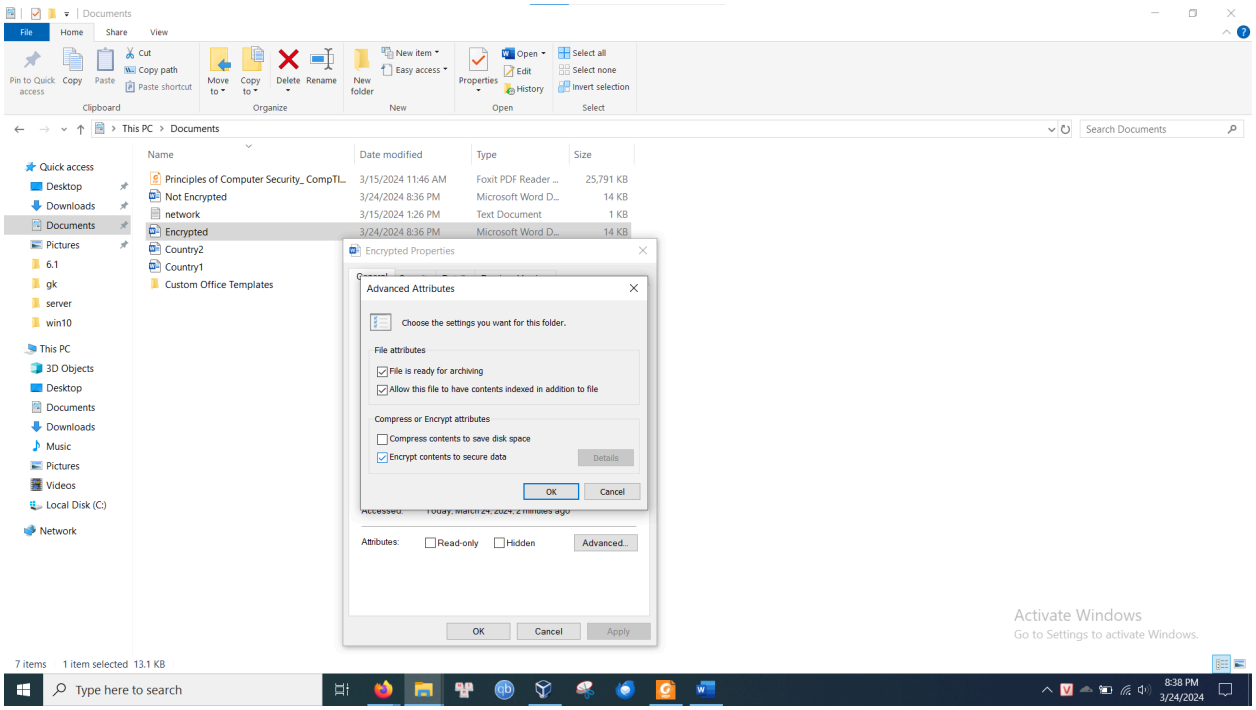


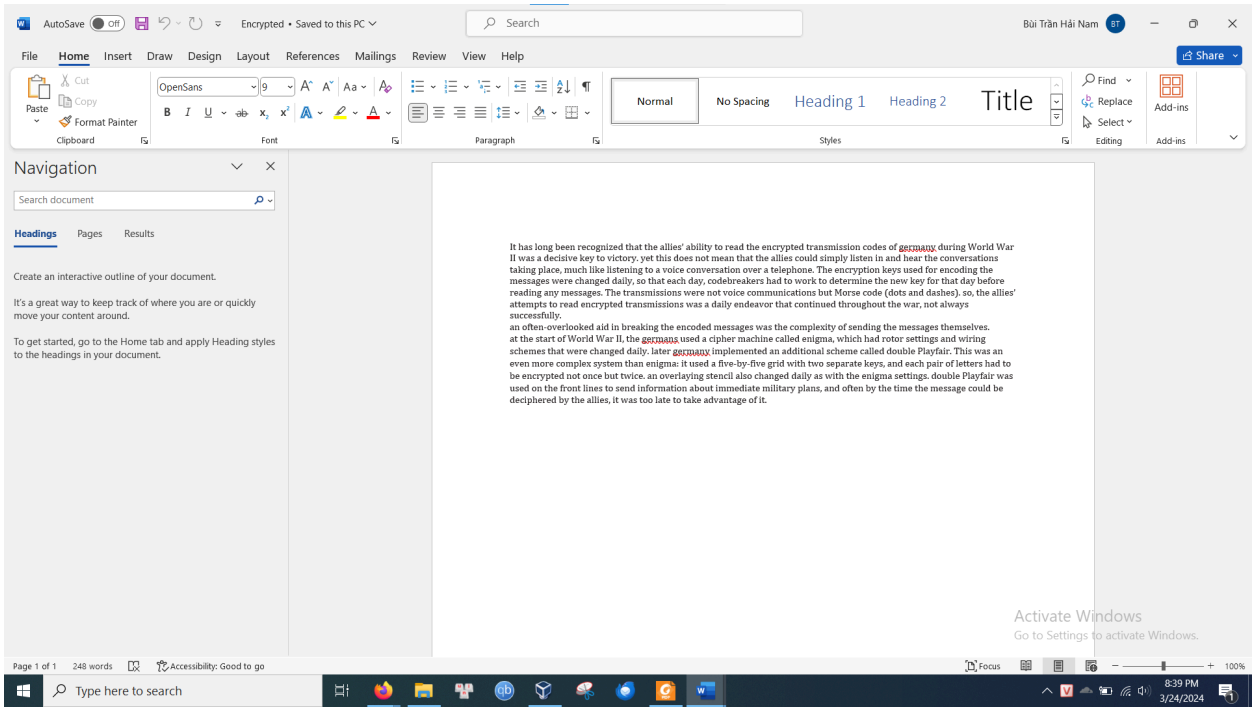
Kết quả hash giữa 2 file khác nhau hoàn toàn. Điều này thể hiện kết quả băm tốt do một thay đổi nhỏ trong đầu vào có thể tạo khác biệt lớn ở đầu ra, phản ánh đúng hiệu ứng thác của hàm băm

Project 6.4:


Document1 - Word
Search
Bùi Trần Hải Nam
File Home Insert Draw Design Layout References Mailings Review View Help
Share
Paste Cut Copy Format Painter
OpenSans 9
Normal No Spacing Heading 1 Heading 2 Title
Find Replace Select
Add-ins
Navigation
Search document
Headings Pages Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading styles to the headings in your document.
Save this file
File name
Encrypted .docx
Choose a Location
Documents
C: » Users » nam
More options...
Save
Cancel
Activate Windows
Go to Settings to activate Windows.
Page 1 of 1 248 words Accessibility: Good to go
Focus 100%
Type here to search
8:35 PM
3/24/2024


Encrypted • Saved to this PC
Bùi Trần Hải Nam
Save As
Home
New
Open
Get Add-ins
Info
Save
Save As
History
Print
Share
Export
Transform
Close
Account
Feedback
Options
Recent
vnu.edu.vn
OneDrive - vnu.edu.vn
21020525@vnu.edu.vn
Sites - vnu.edu.vn
21020525@vnu.edu.vn
Other locations
This PC
Add a Place
Browse
Pinned
Today
Last Week
Save As
Local Disk (C:) › Users › nam › Documents
Organize New folder
Add a search filter
Date modified: Size:
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name Date modified Type Size
Custom Office Templates 3/21/2024 7:16 PM File folder
Country1 3/24/2024 8:16 PM Microsoft Word D... 13
Country2 3/24/2024 8:17 PM Microsoft Word D... 13
Encrypted 3/24/2024 8:36 PM Microsoft Word D... 14
File name: Not Encrypted
Save as type: Word Document
Authors: Bùi Trần Hải Nam Tags: Add a tag
Save Thumbnail
Hide Folders
Tools
Save
Cancel
Activate Windows
Go to Settings to activate Windows.
Type here to search
8:36 PM
3/24/2024





Không có độ trễ đáng kể giữa Not Encrypted.docx và Encrypted.docx