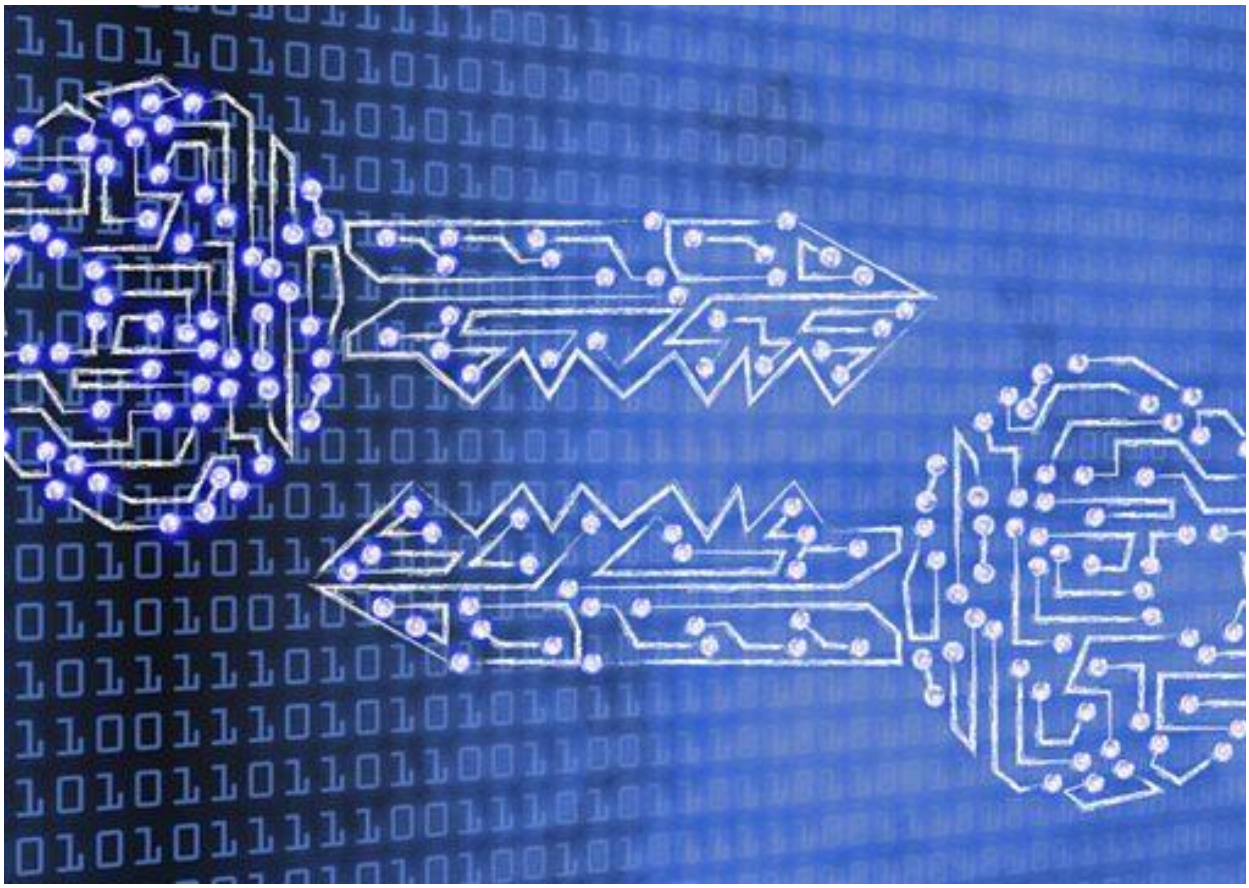
Cryptography

Defensive Security 1 - Assignment 3



by

Uthaya Krishnan
Sheridan College

The Basics:

Public-key cryptography :

It uses a pair of keys - a public key and a private key. The public key can be shared openly, while the private key is kept secret.

In email encryption, the sender uses the recipient's public key to encrypt the email. Only the recipient, who possesses the corresponding private key, can decrypt the message. This ensures that even if the encrypted email is intercepted, it cannot be read without the private key. This method of encryption provides confidentiality and ensures that only the intended recipient can access the message content .

Private-Key Cryptography in Email Security

Private-key cryptography:

It is also known as symmetric cryptography. It uses a single key for both encryption and decryption. This key must be shared between the sender and recipient securely. While it is efficient for encrypting and decrypting large amounts of data, its main drawback is the challenge of securely sharing the key.

In email communications, private-key cryptography is less common due to the difficulties in key distribution and management compared to public-key cryptography .

Public Key Infrastructure (PKI) in Email Encryption

Public Key Infrastructure (PKI) :

It is a framework that manages public-key encryption and digital certificates.

In email encryption, PKI facilitates the creation, distribution, and management of public and private keys. PKI involves a Certificate Authority (CA) that issues digital certificates verifying the ownership of public keys. When sending an encrypted email, the sender can obtain the recipient's public key from their digital certificate, ensuring the key's authenticity. PKI thus provides a scalable and secure way to manage keys and authenticate users in email encryption

Selecting Tools

1. GPG (GNU Privacy Guard)

GPG is an open-source implementation of the OpenPGP standard for encrypting and signing data. Choosing this tool because of following features:

Security: GPG provides robust encryption using RSA and other algorithms, ensuring the confidentiality and integrity of emails.

Open Source: Being open-source, GPG is freely available, regularly audited, and maintained by a strong community, ensuring transparency and security.

Compatibility: GPG is compatible with various operating systems and integrates with numerous applications, making it versatile for different use cases.

Proven Track Record: Widely trusted and used by security professionals worldwide, GPG has a long history of reliability and effectiveness in secure communications.

2. Thunderbird with OpenPGP

Thunderbird is a free, open-source, cross-platform email client developed by Mozilla.

OpenPGP is a standard for encrypting and signing data used by GPG and other encryption tools.

User-Friendly: Thunderbird offers an intuitive interface, making it easy for users to manage their emails and integrate encryption tools.

Customizable: With a wide range of add-ons and extensions like Enigmail, Thunderbird can be customized to enhance its functionality, including encryption.

Secure: Thunderbird provides robust security features, including spam filters and phishing protection, and supports integration with GPG for encrypted communications.

Open Source: As an open-source application, Thunderbird benefits from community contributions and regular updates, ensuring it remains secure and up-to-date.

Standardization: OpenPGP is an established standard for encryption and digital signatures, ensuring interoperability between different applications and systems.

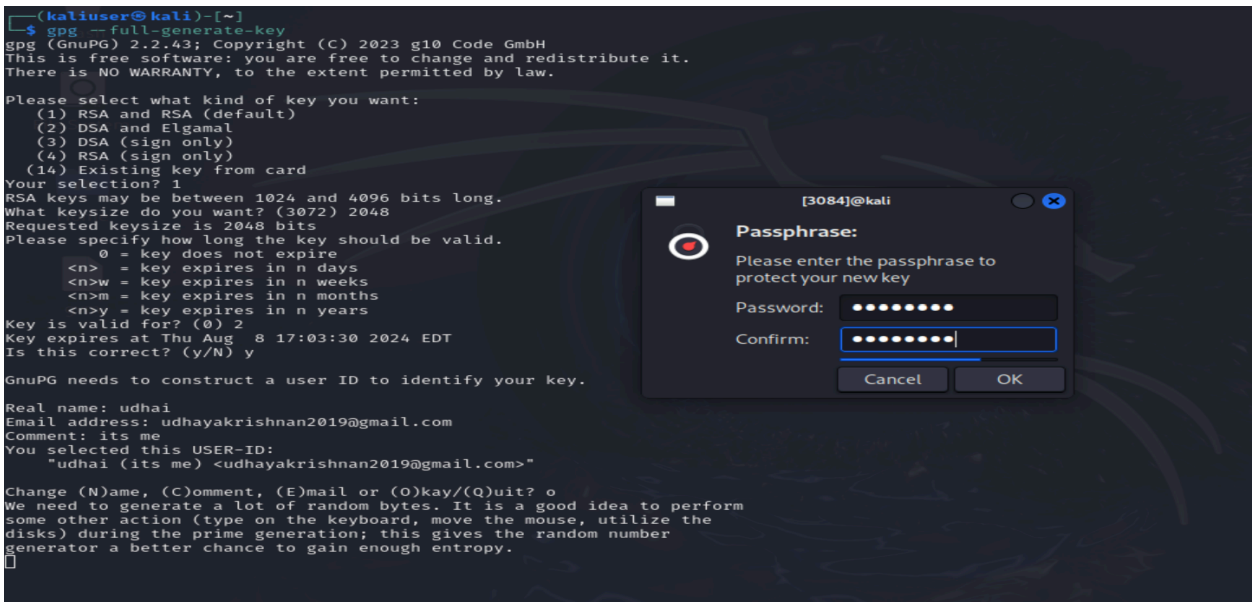
Security: It provides strong encryption and authentication mechanisms to protect data integrity and confidentiality.

Generating Keys

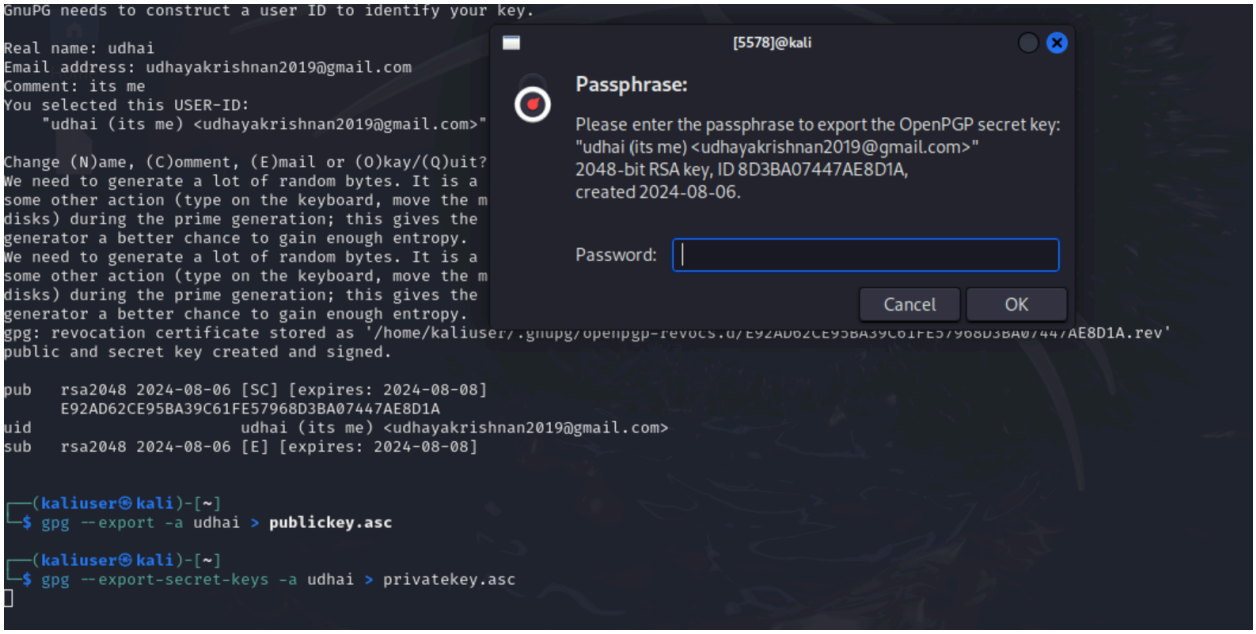
Generate a pair of public and private keys using the selected encryption tool.

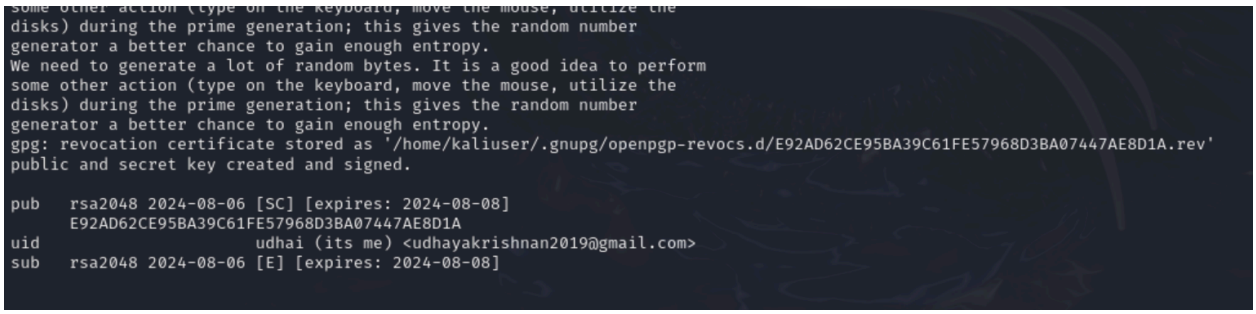
Installing gnupg tool

Generating key for Sender using GPG

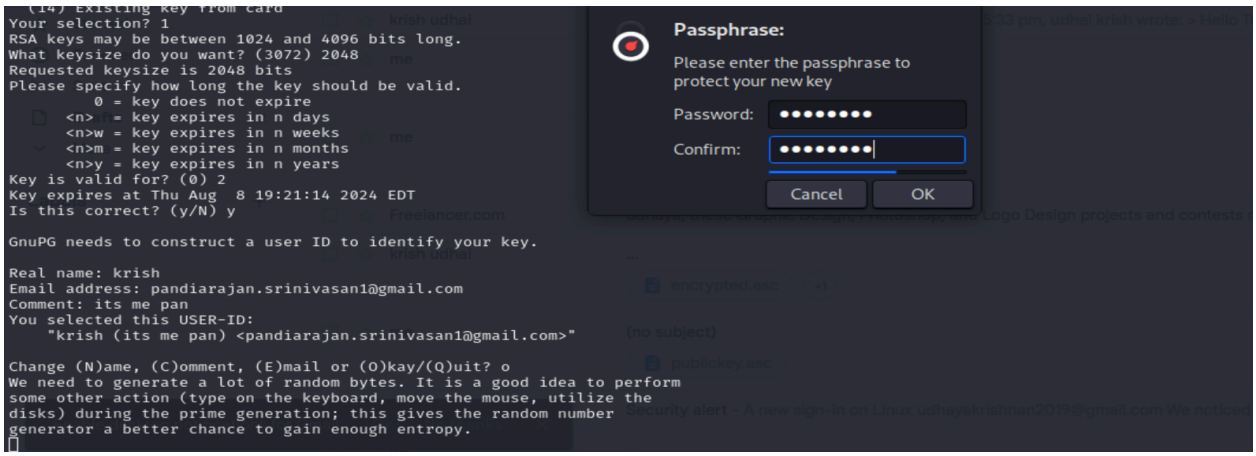


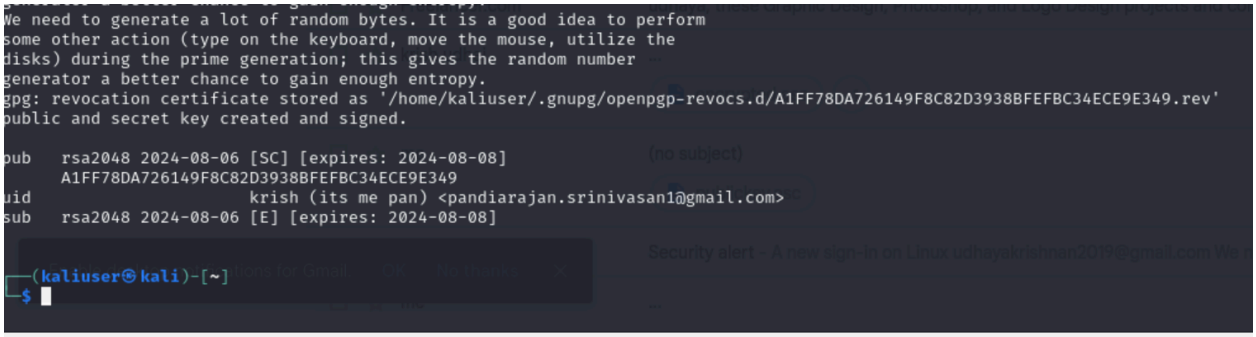
Exporting public key and private key for sender



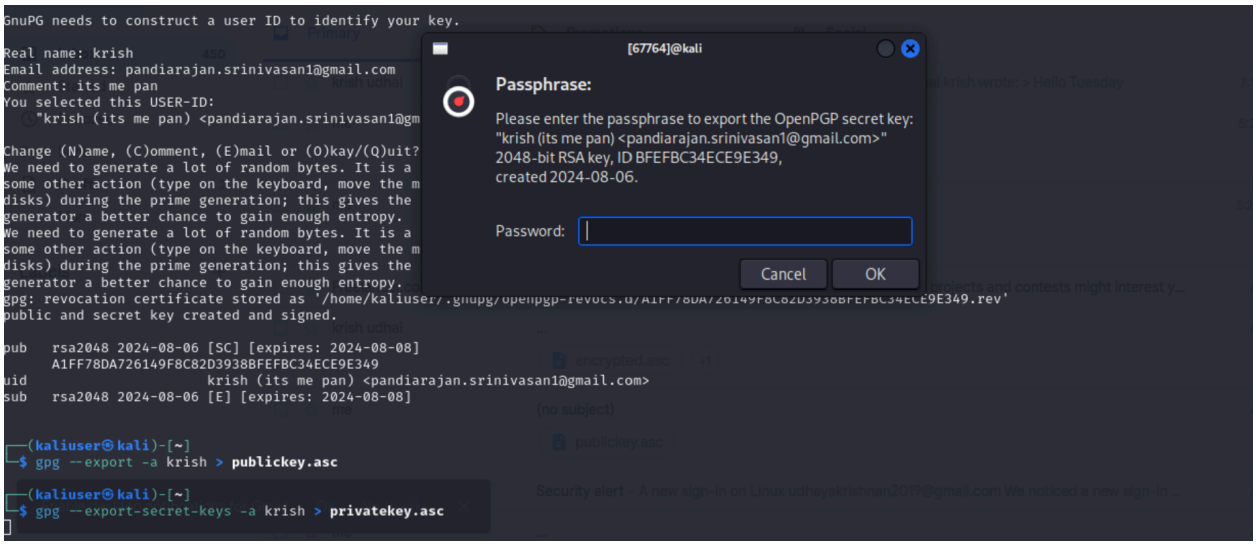


Generating key for Receiver using GPG





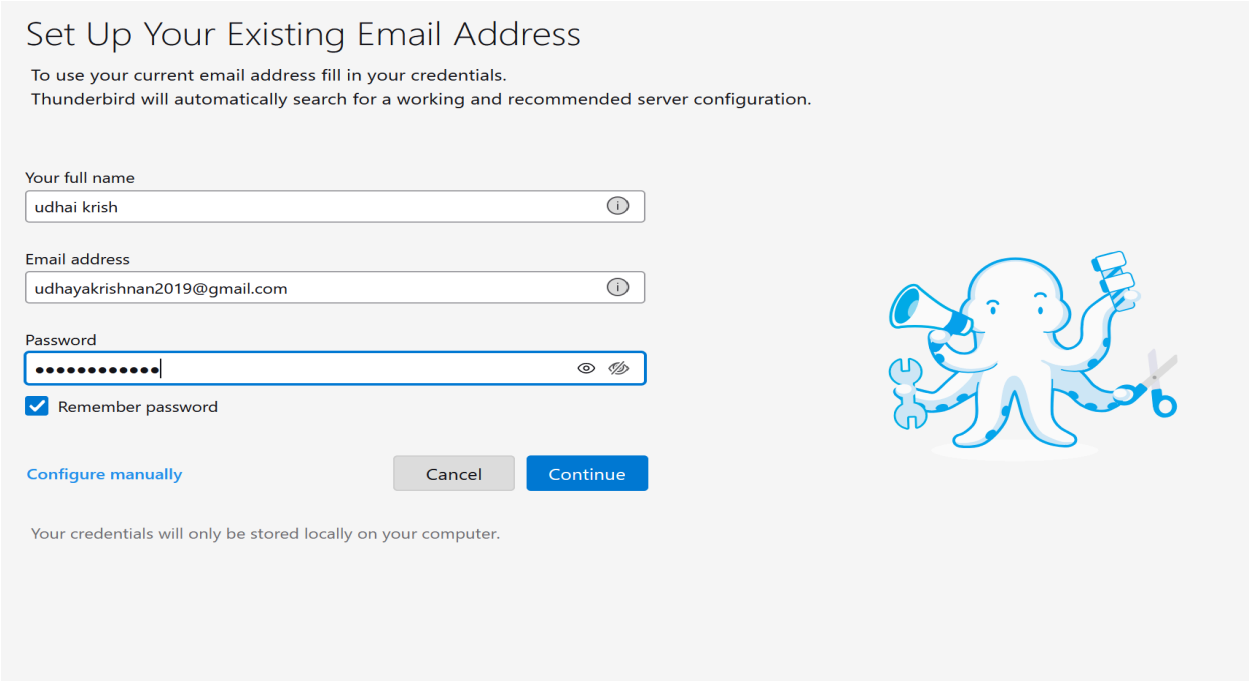
Exporting public and private keys for receiver

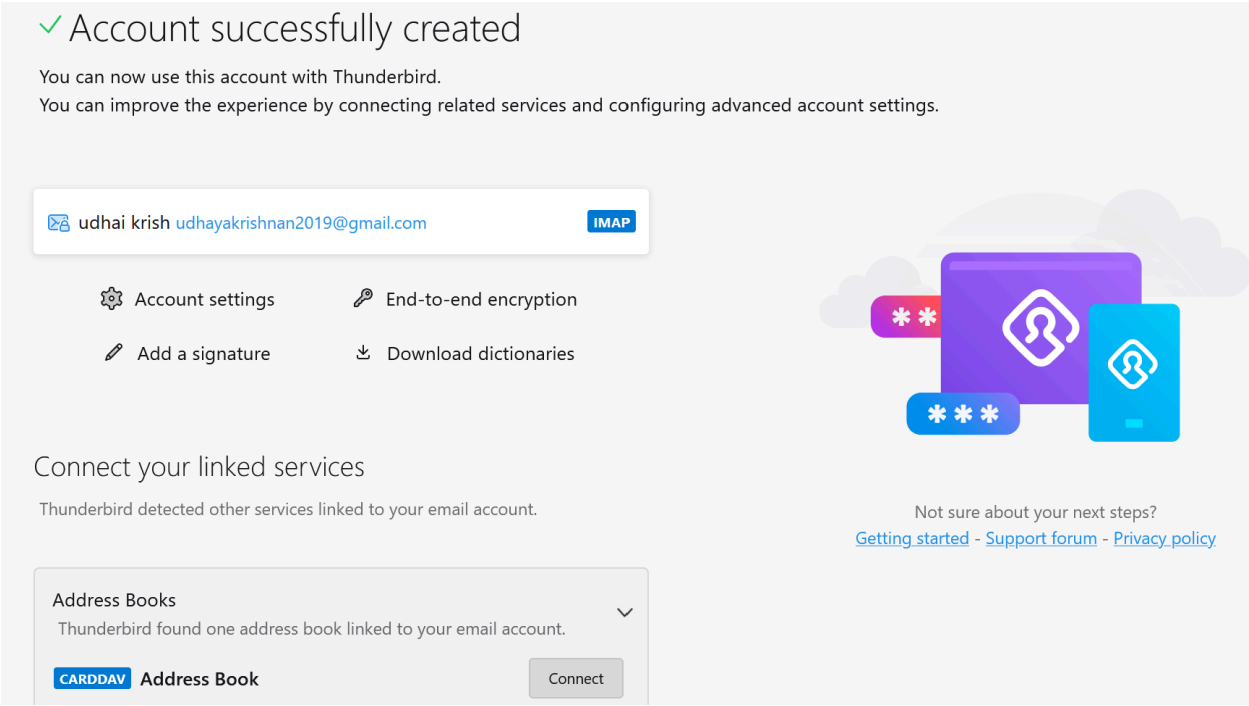


Pair of public and private keys for sender and receiver

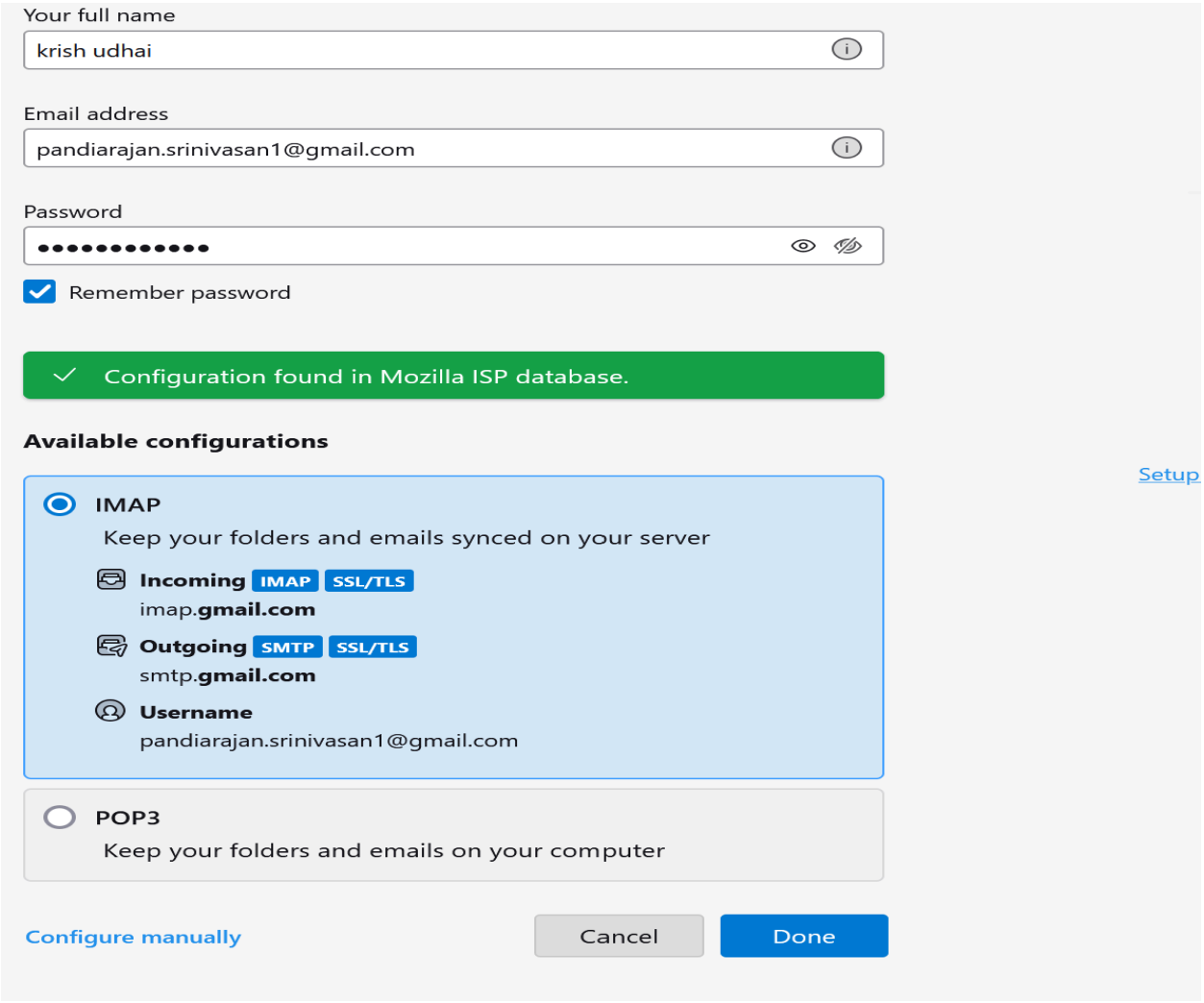
Configuring Email Accounts

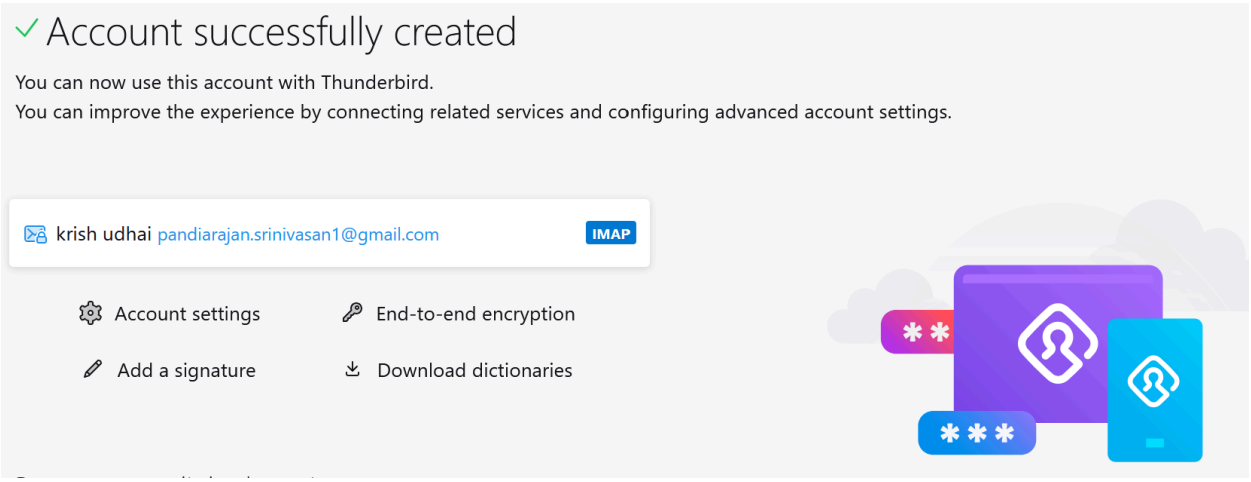
Configuring Sender Mail Account in Thunderbird



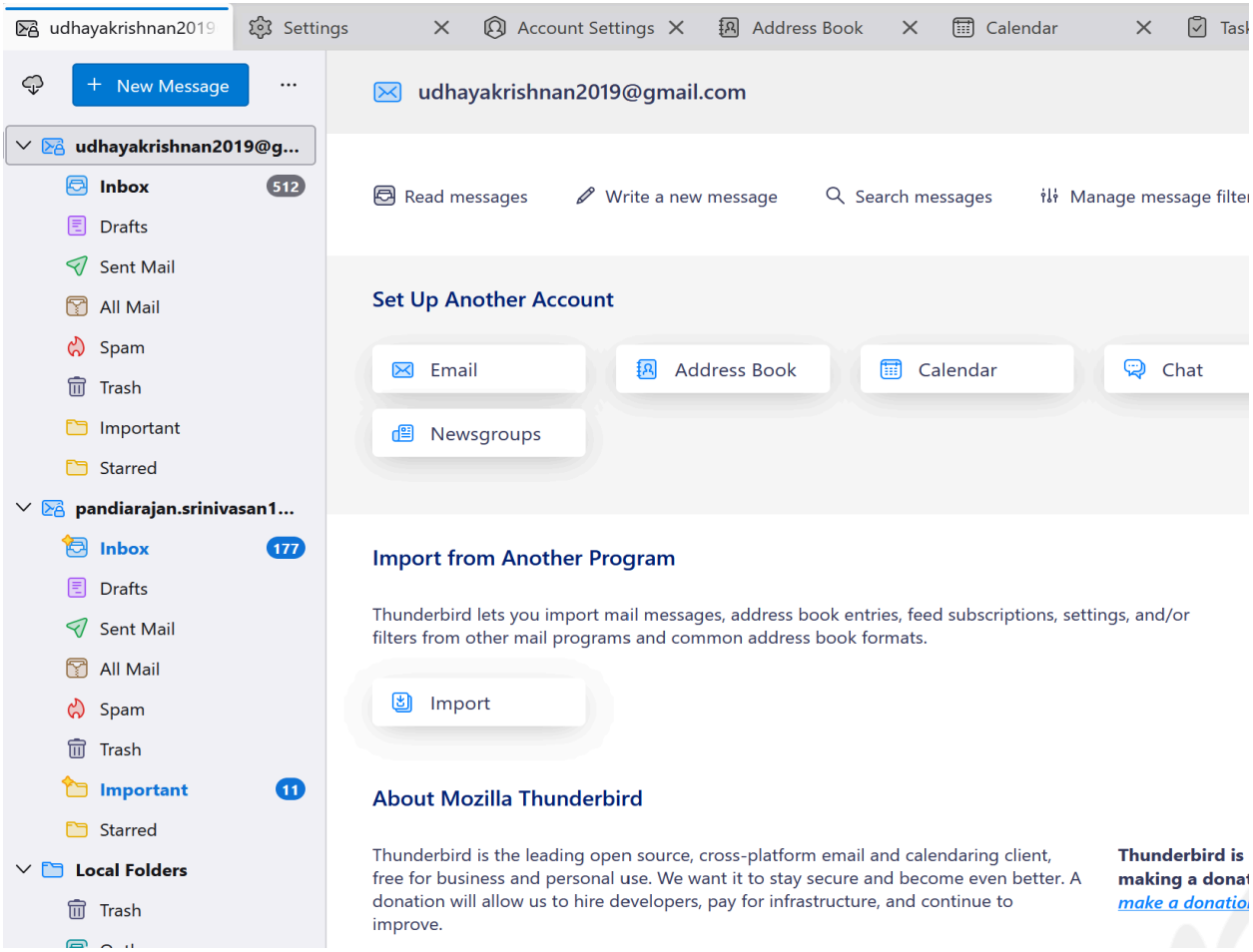


Configuring Receiver Mail Account in ThunderBird





Both Accounts Configured Successfully

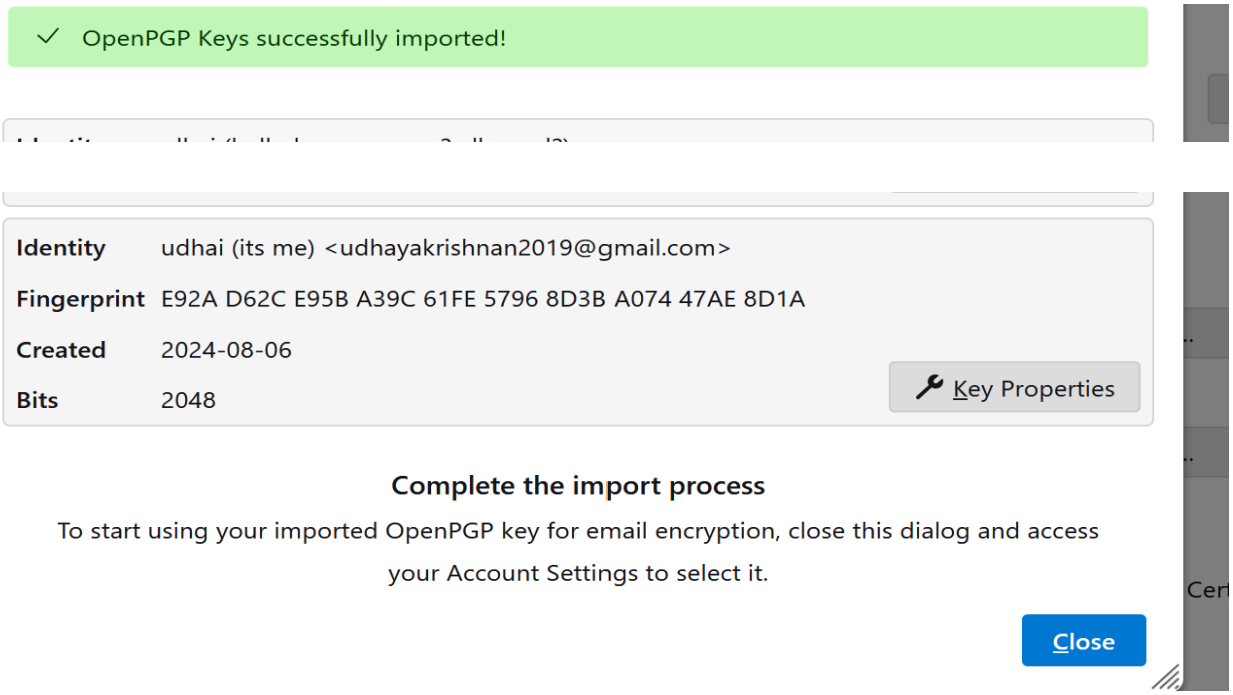


Exchanging Public Keys

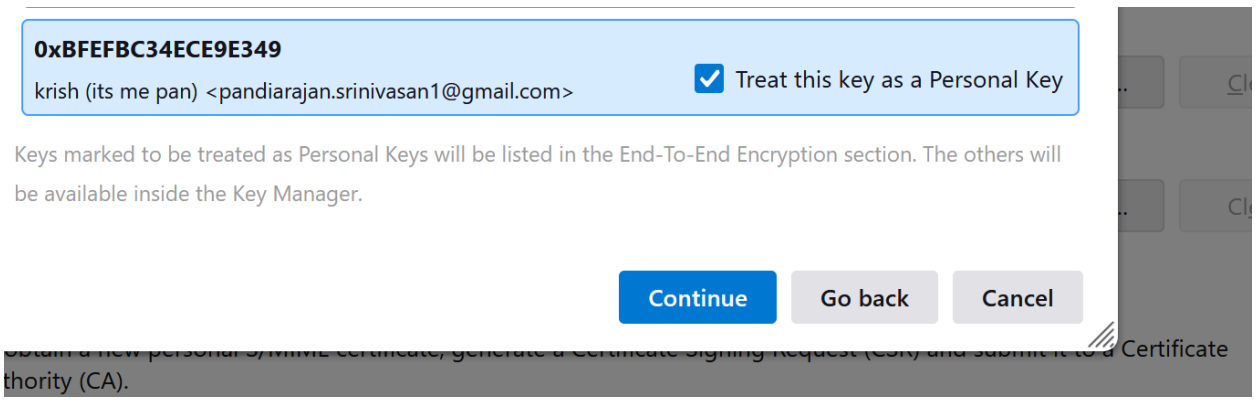
Exchanging public keys between two email accounts is a critical step in setting up secure email communication using encryption. The process ensures that each party can encrypt messages to be sent securely to the other party, and only the corresponding recipient can decrypt and read them.

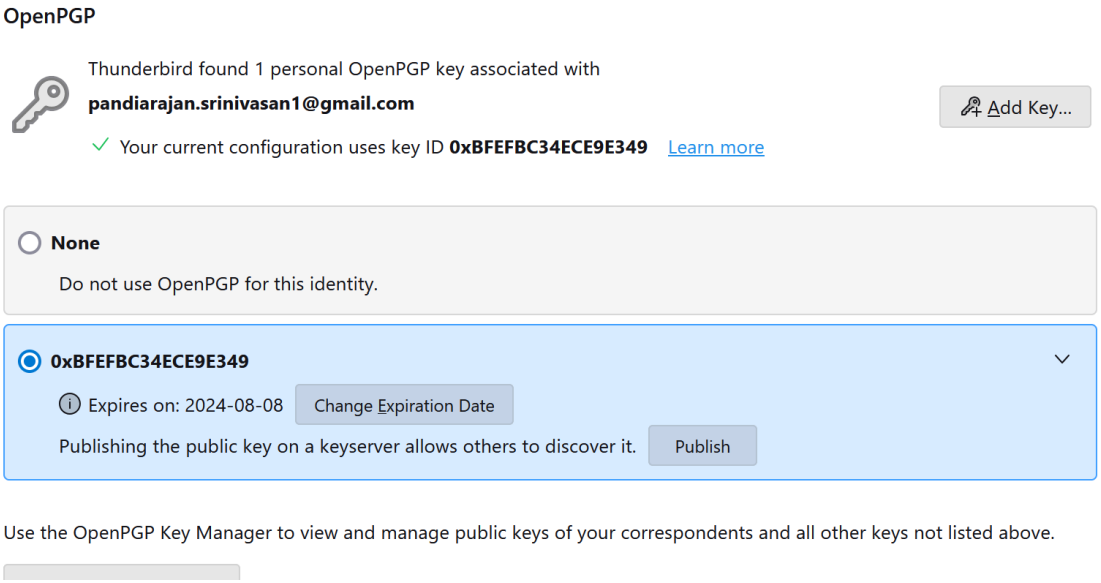
Sending the keys over the mail securely and importing the same in Thunderbird to configure with the sender and receiver accounts

Importing the key-pair for the sender

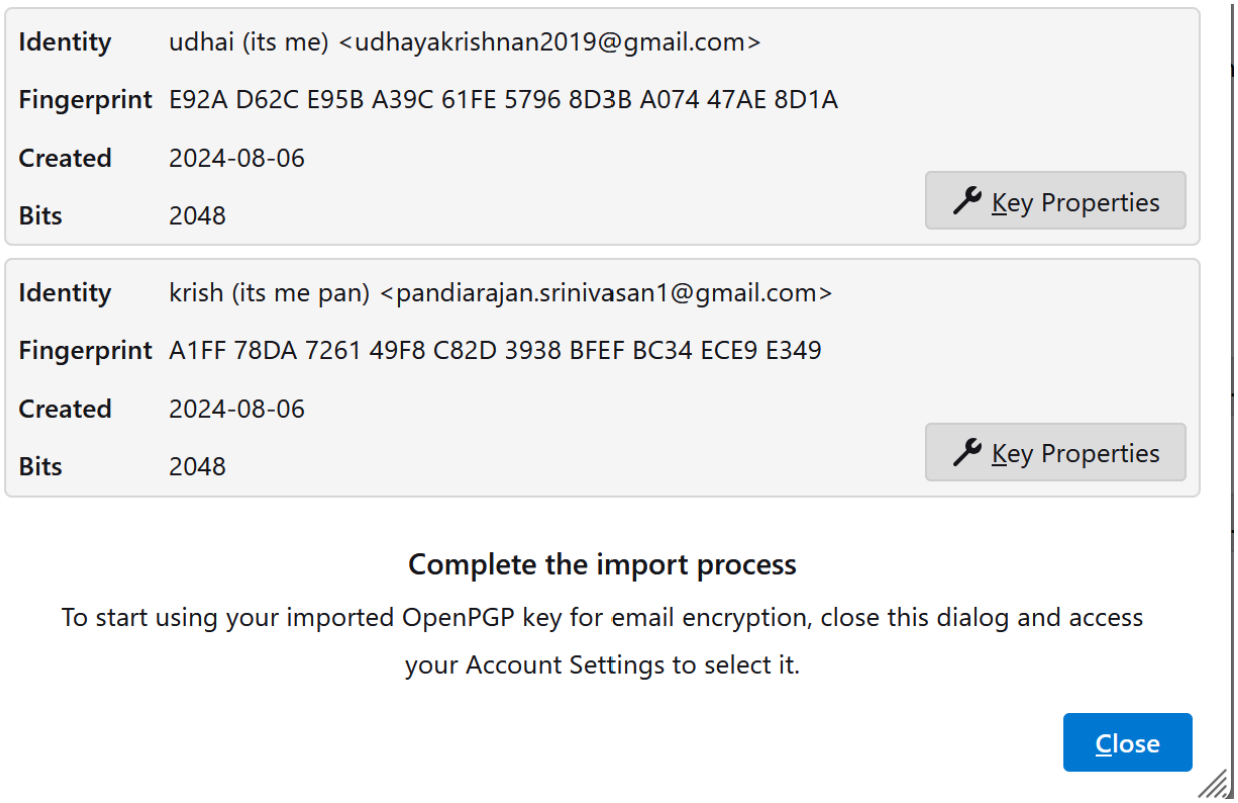


Importing the key-pair for the receiver



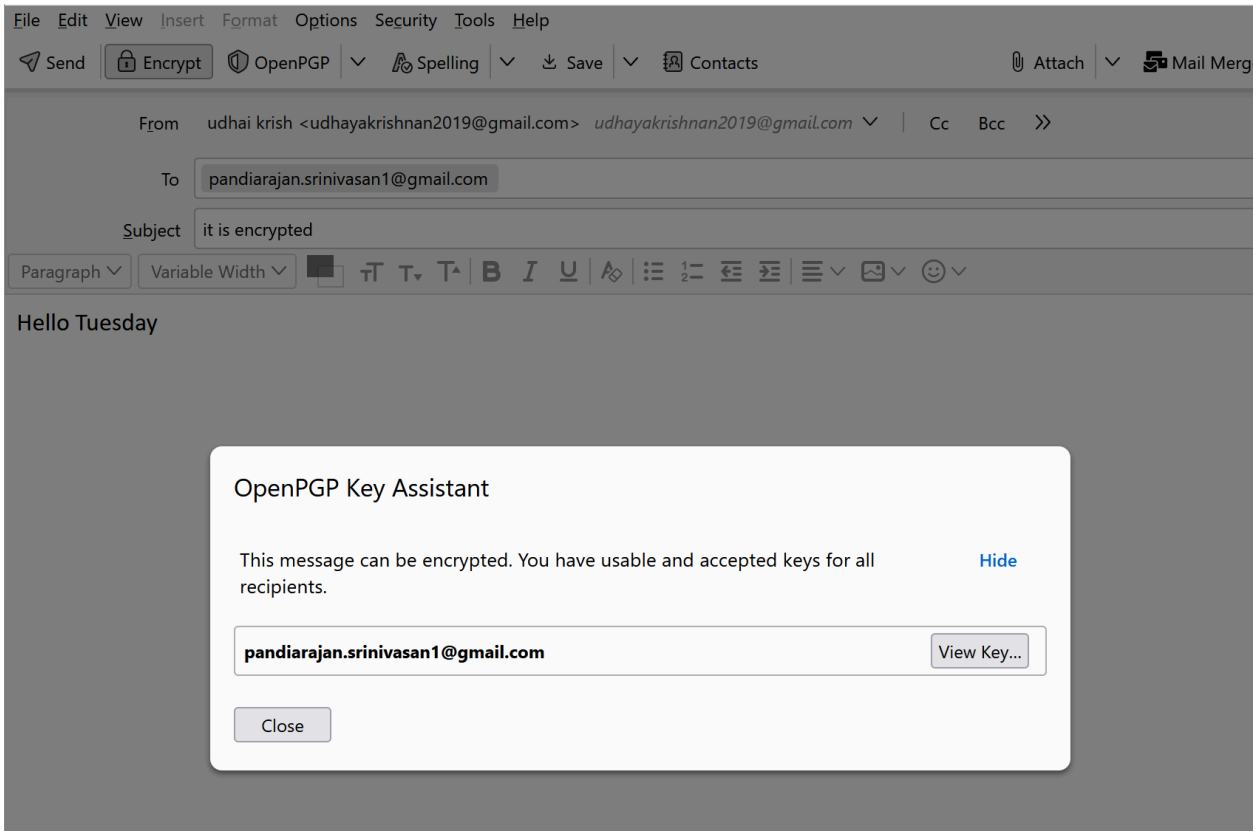


Both key pairs were configured successfully.

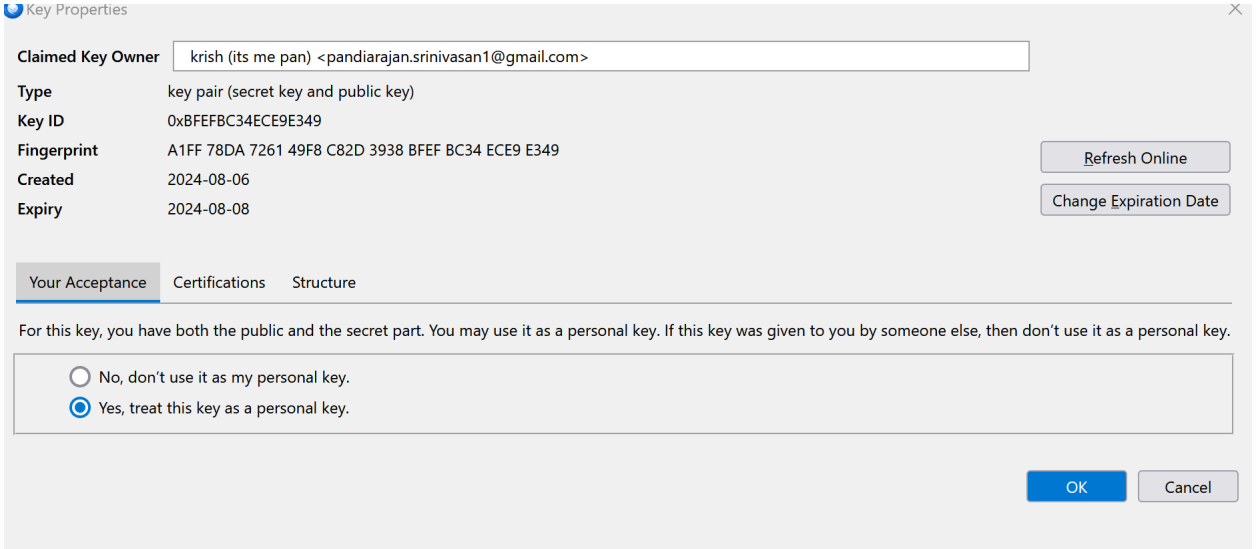


Sending Encrypted Email and Verification of Encrypted Email

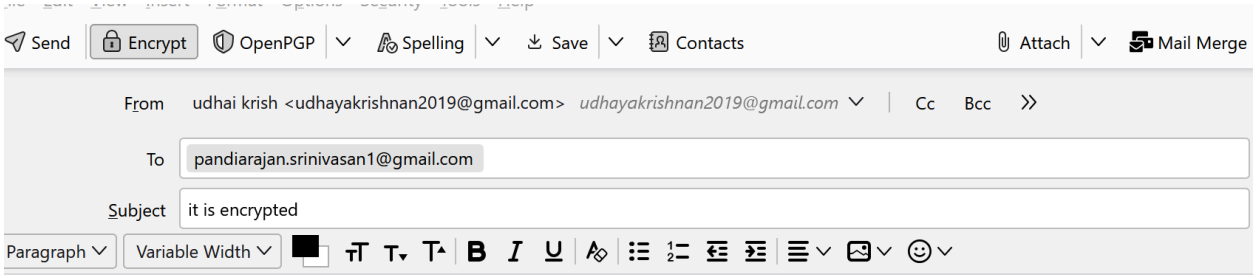
Composing Mail



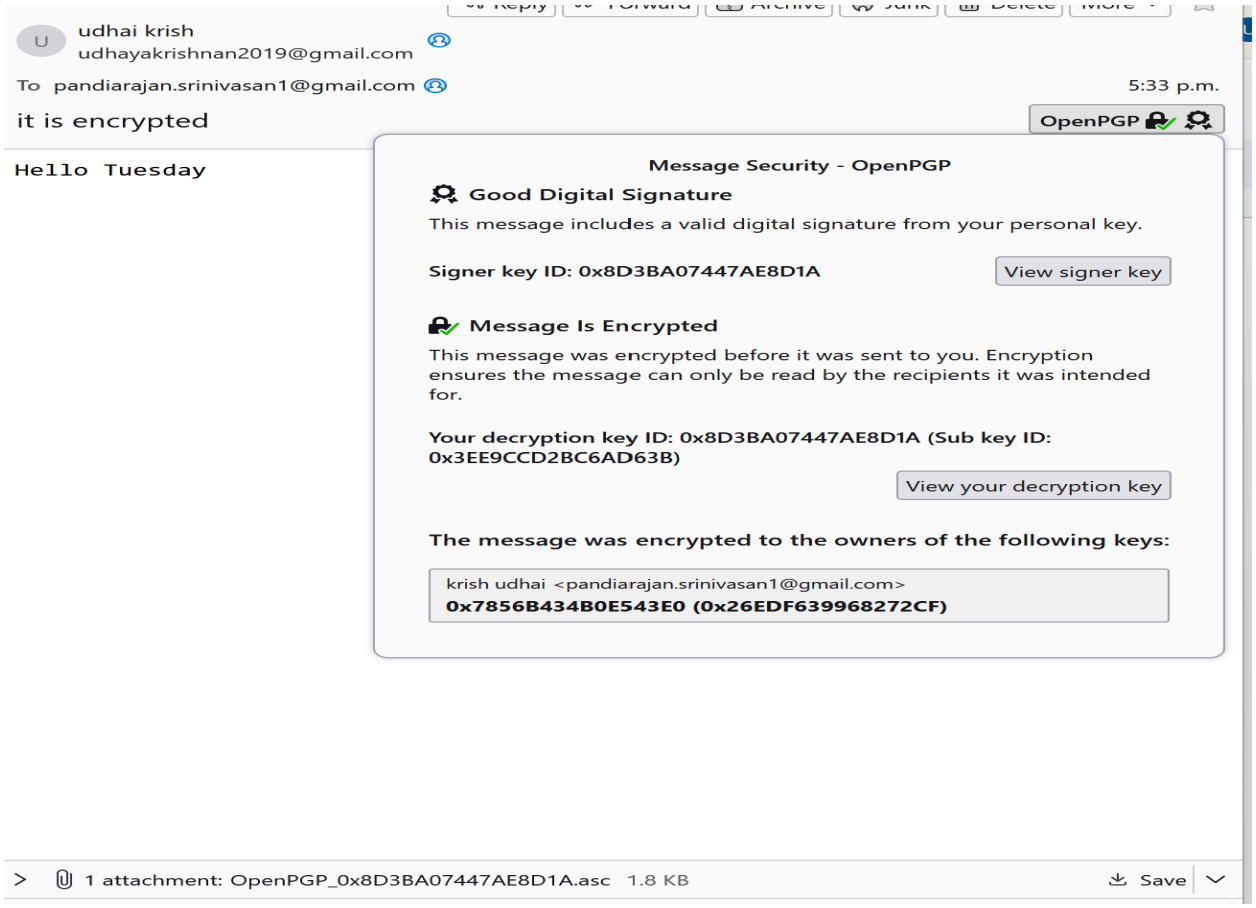
Select the key from OpenPGP option

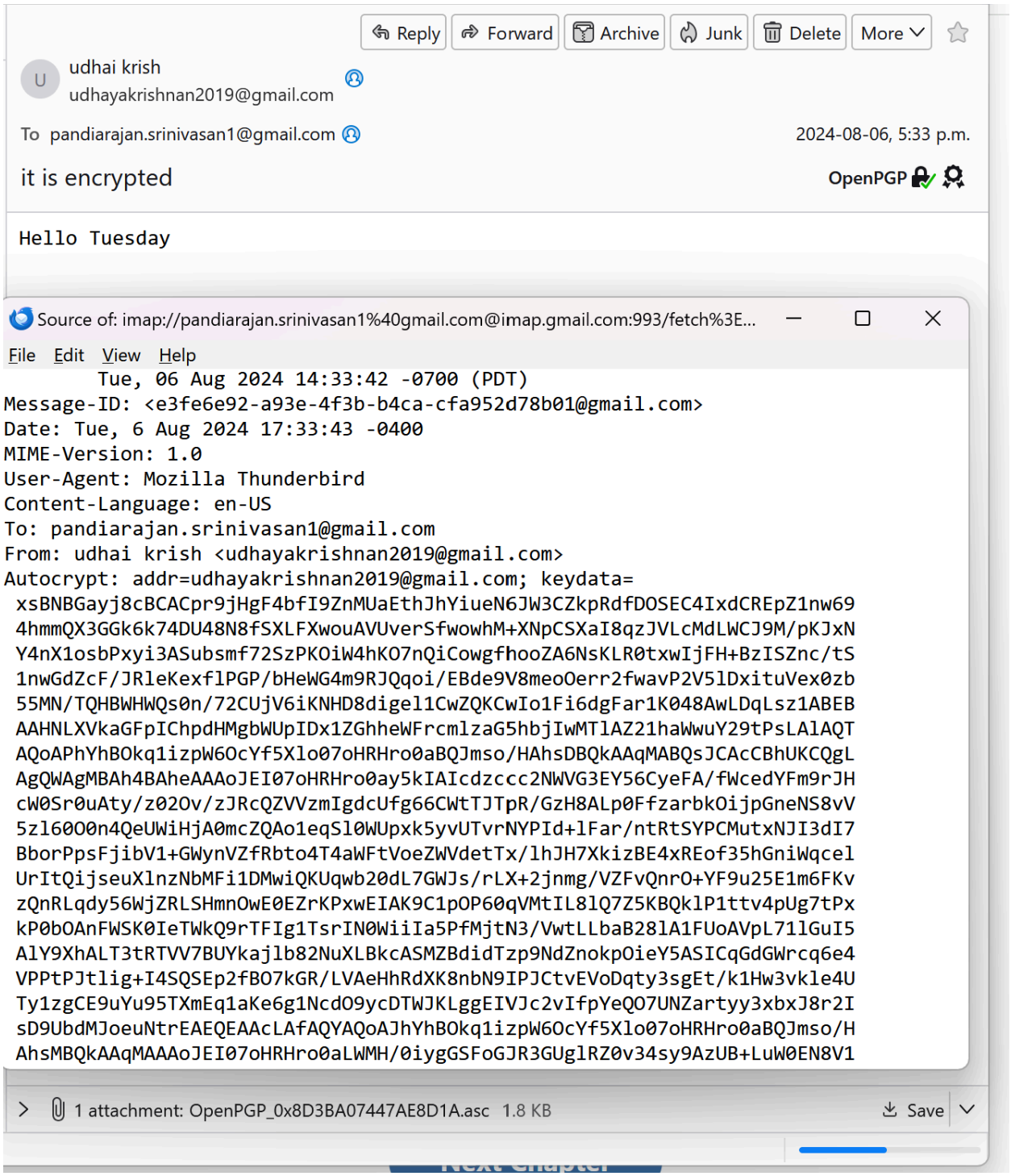


Sending Encrypted Message with the key-pair selected

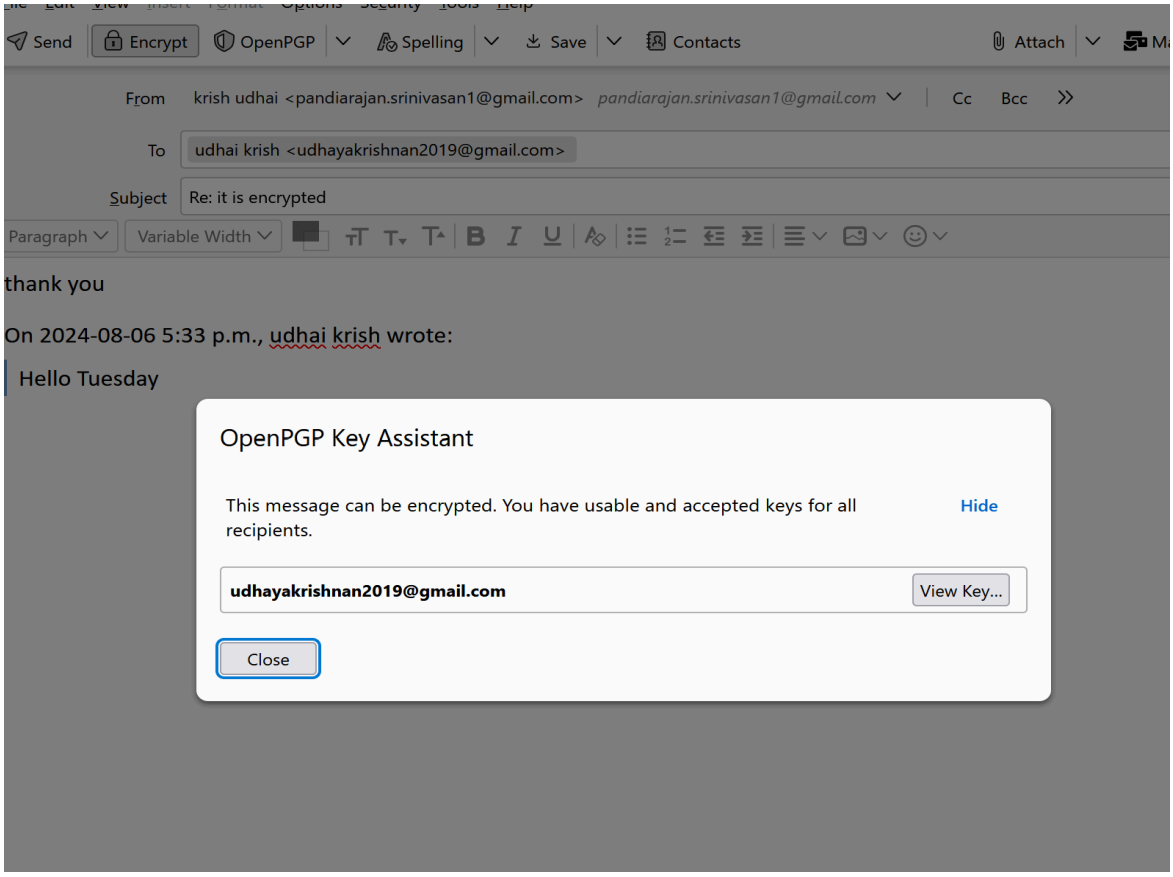


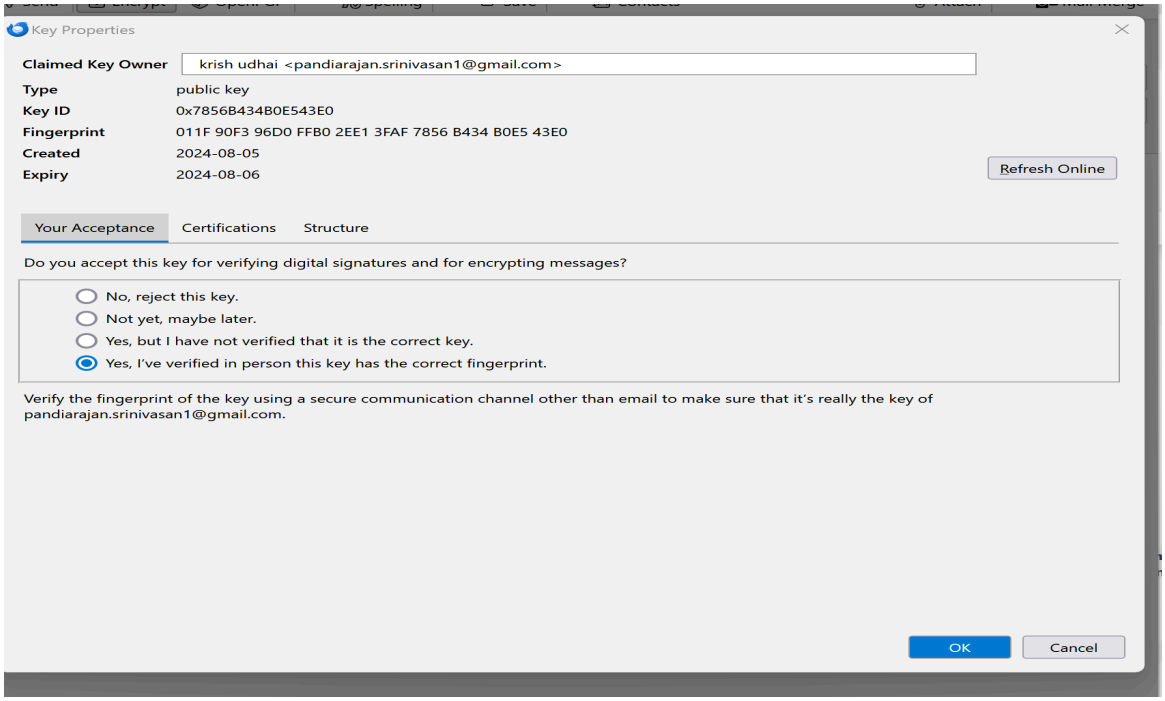
The Encrypted mail received with and Decrypted with the keys shared



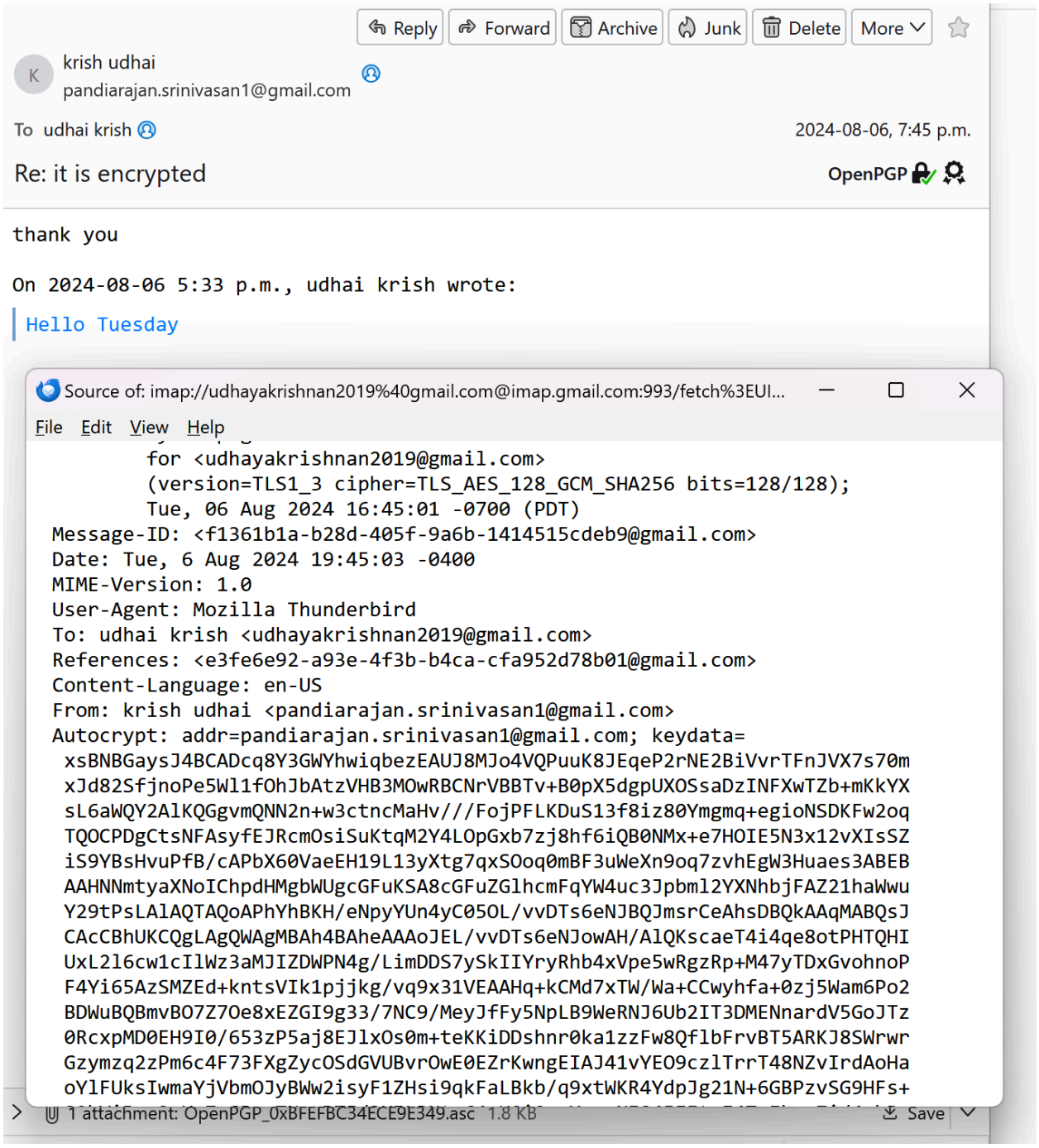

Reply
Forward
Archive
Junk
Delete
More
udhai krish
udhayakrishnan2019@gmail.com
To pandiarajan.srinivasan1@gmail.com
2024-08-06, 5:33 p.m.
it is encrypted
OpenPGP
Hello Tuesday
Source of: imap://pandiarajan.srinivasan1%40gmail.com@imap.gmail.com:993/fetch%3E...
File Edit View Help
Tue, 06 Aug 2024 14:33:42 -0700 (PDT)
Message-ID: <e3fe6e92-a93e-4f3b-b4ca-cfa952d78b01@gmail.com>
Date: Tue, 6 Aug 2024 17:33:43 -0400
MIME-Version: 1.0
User-Agent: Mozilla Thunderbird
Content-Language: en-US
To: pandiarajan.srinivasan1@gmail.com
From: udhai krish <udhayakrishnan2019@gmail.com>
Autocrypt: addr=udhayakrishnan2019@gmail.com; keydata=
xsBNBGayj8cBCACpr9jHgF4bfI9ZnMUaEthJhYiueN6JW3CZkpRdfDOSEC4IxdCREpZ1nw69
4hmmQX3GGk6k74DU48N8fSXLFXwouAVUverSfwowhM+XNpCSXaI8qzJVLcMdLWCJ9M/pKJxN
Y4nX1osbPxyi3ASubsmf72SzPKOiW4hKO7nQiCowgfhooZA6NsKLR0txwIjFH+BzISZnc/tS
1nwGdZcF/JRleKexflPGP/bHeWG4m9RJQqoi/EBde9V8meoOerr2fwavP2V5lDxituVex0zb
55MN/TQHBWHWQs0n/72CUjV6iKNHD8digel1CwZQKCwIo1Fi6dgFar1K048AwLDqLsz1ABEB
AAHNLXVkaGFpIChpdHMgbWUpIDx1ZGhheWFrcmlzaG5hbjIwMTlAZ21haWwuY29tPsLAlAQT
AQoAPhYhBOkq1izpW6OcYf5Xlo07oHRHro0aBQJmso/HAhsDBQkAAqMABQsJCAcCBhUKCQgL
AgQWAgMBAh4BAheAAAoJEI07oHRHro0ay5kIAIcdzccc2NWVG3EY56CyeFA/fWcedYFm9rJH
cW0Sr0uAty/z02Ov/zJRcQZVVzmIgdcUfg66CWtTJTpR/GzH8ALp0FfzarbkOijpGneNS8vV
5zl60O0n4QeUWiHjA0mcZQAo1eqSl0WUpxk5yvUTvrNYPId+lFar/ntRtSYPCMutxNJI3dI7
BborPpsFjibV1+GWynVZfRbto4T4aWFtVoeZWVdetTx/lhJH7XkizBE4xREof35hGniWqcel
UrItQijseuXlnzNbMFi1DMwiQKUqwb20dL7GWJs/rLX+2jnmg/VZFvQnrO+YF9u25E1m6FKv
zQnRLqdy56WjZRLSHmnOwE0EZrKPxwEIAK9C1pOP60qVMtIL8lQ7Z5KBQklP1ttv4pUg7tPx
kP0bOAnFWSK0IeTWkQ9rTFIg1TsrIN0WiiIa5PfMjtN3/VwtLLbaB28lA1FUoAVpL71lGuI5
AlY9XhALT3tRTVV7BUYkajlb82NuXLBkcASMZBdidTzp9NdZnokpOieY5ASICqGdGWrcq6e4
VPPtPJtlig+I4SQSEp2fBO7kGR/LVAeHhRdXK8nbN9IPJCtvEVoDqty3sgEt/k1Hw3vkle4U
Ty1zgCE9uYu95TXmEq1aKe6g1NcdO9ycDTWJKLggEIVJc2vIfpYeQO7UNZartyy3xbxJ8r2I
sD9UbdMJoeuNtrEAEQEAAcLAfAQYAQoAJhYhBOkq1izpW6OcYf5Xlo07oHRHro0aBQJmso/H
AhsMBQkAAqMAAAoJEI07oHRHro0aLWMH/0iygGSFoGJR3GUglRZ0v34sy9AzUB+LuW0EN8V1
1 attachment: OpenPGP_0x8D3BA07447AE8D1A.asc 1.8 KB
Save

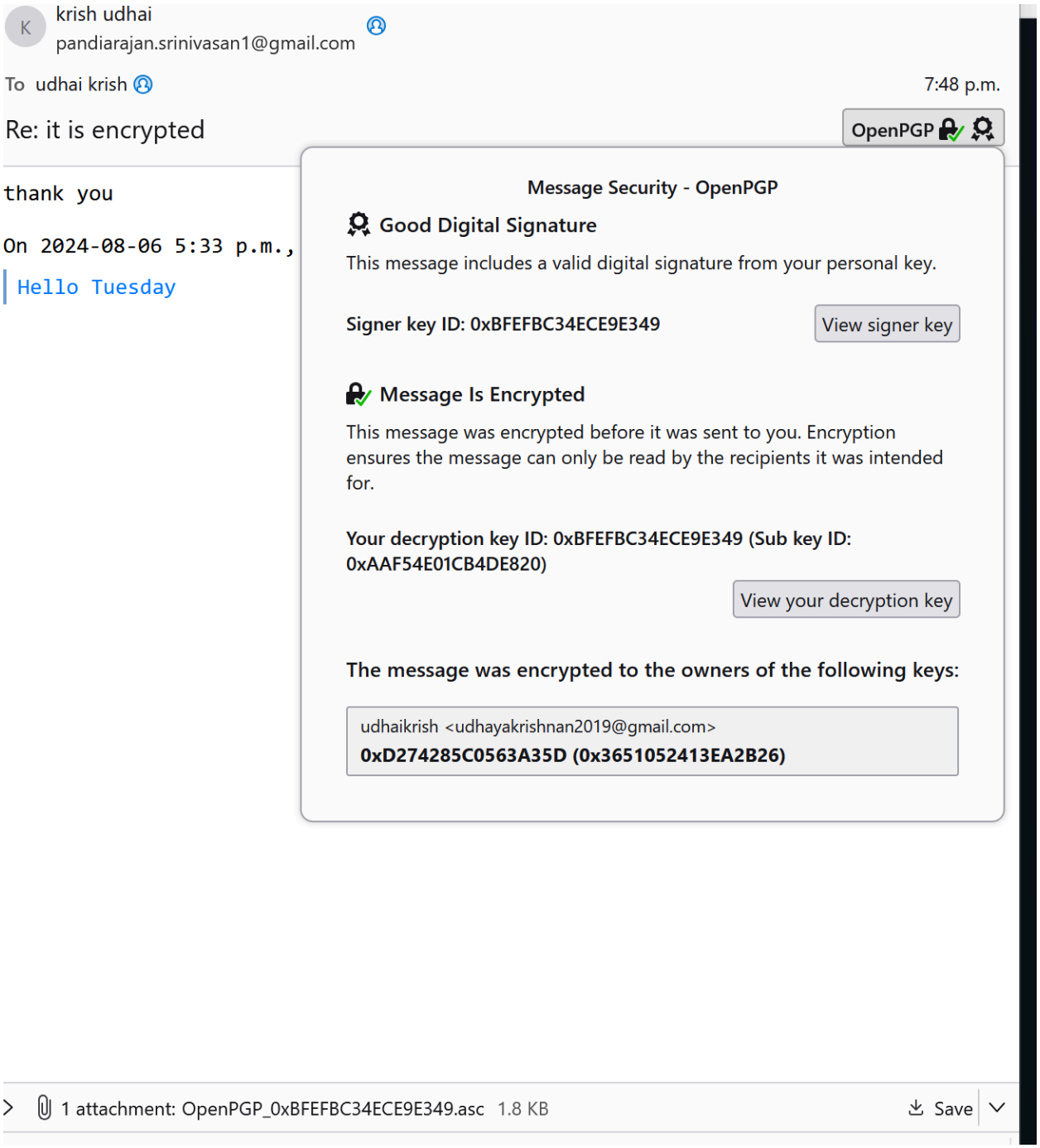
Responding the sender back with the shared public key





Decrypted Successfully at the other end




K
krish udhai
pandiarajan.srinivasan1@gmail.com
To udhai krish
7:48 p.m.
Re: it is encrypted
OpenPGP
thank you
On 2024-08-06 5:33 p.m.,
Hello Tuesday
Message Security - OpenPGP
Good Digital Signature
This message includes a valid digital signature from your personal key.
Signer key ID: 0xBFEFBC34ECE9E349
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: 0xBFEFBC34ECE9E349 (Sub key ID: 0xAAF54E01CB4DE820)
View your decryption key
The message was encrypted to the owners of the following keys:
udhaikrish <udhayakrishnan2019@gmail.com>
0xD274285C0563A35D (0x3651052413EA2B26)
1 attachment: OpenPGP_0xBFEFBC34ECE9E349.asc 1.8 KB
Save

Conclusion

Implementing email encryption using GPG, Thunderbird, and OpenPGP was insightful. It involved understanding key cryptography concepts, selecting appropriate tools, generating keys, configuring email accounts, exchanging public keys, and finally encrypting and sending emails. Each step was crucial in ensuring secure communication

Importance of Email Encryption in Securing Digital Communications

Email encryption is vital for protecting sensitive information from unauthorized access. It ensures confidentiality, integrity, and authenticity of communications, thereby safeguarding against threats such as eavesdropping, tampering, and phishing attacks. This implementation reinforces the necessity of adopting strong encryption practices to maintain privacy and security in digital communications.