Encrypt a text file with a PGP Public Key

GROUP 23

Soumyadeep Basu, Kumar Utkarsh, Rohit Haolader, Raushan Raj, Suryasen Singh

V Semester BTech, Department of Information Technology,

Indian Institute of Information Technology, Allahabad, India.

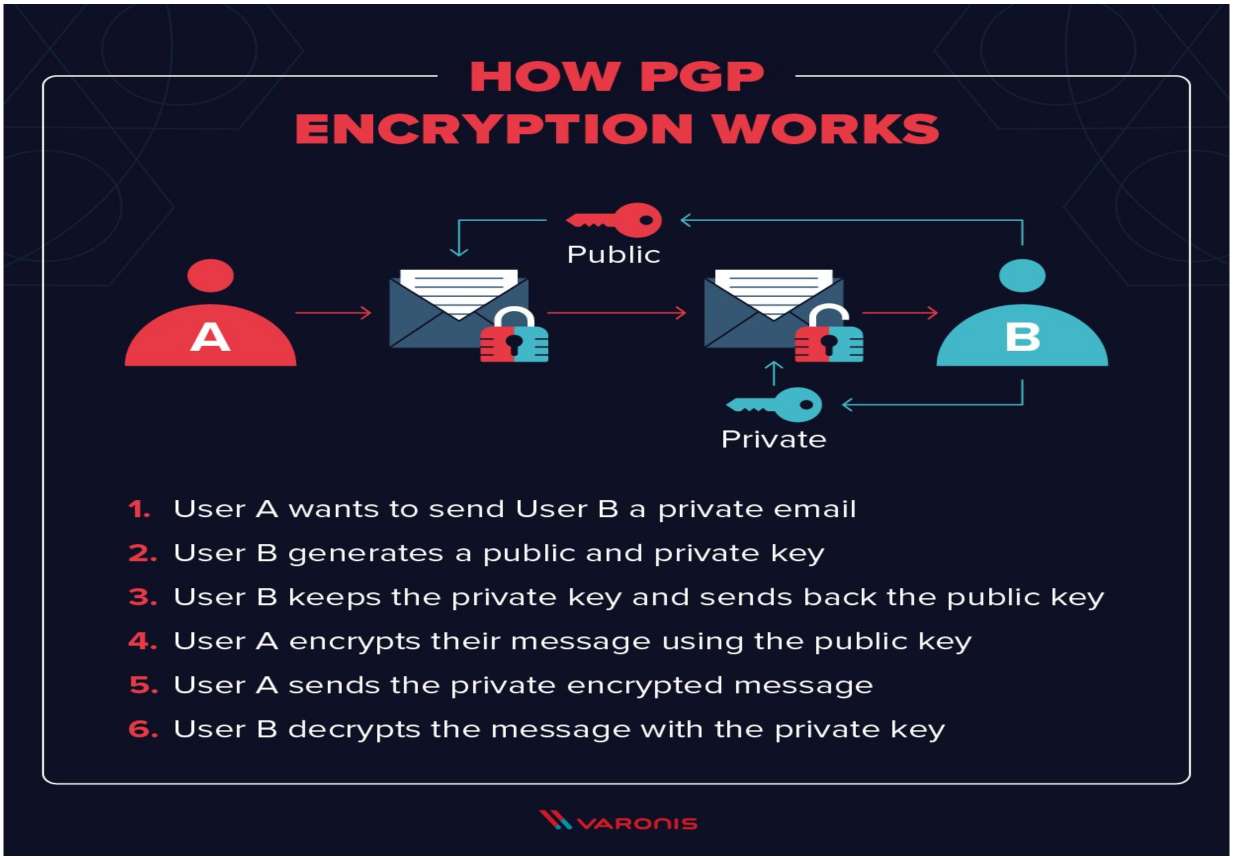
Necessity to encrypt a text file with a PGP Public Key

It will help us to make sure that sensitive data like our bank accounts, passwords and/or confidential documents will be available only to the designated people.

We encrypt this information and then we can safely store it locally, in the cloud or send via email.

How does the encryption process work?

- First of all we need to create PGP key-pair
- It's called a key-pair because there is a pair of keys - private and public
- When a file is encrypted (locked) with a Public key it's considered safe (unauthorized people will not be able to unlock it and read the contents). File can be encrypted with multiple public keys (presuming multiple people are allowed to access the file)
- If Alice wants to encrypt file so that only Bob can decrypt it she needs to ask Bob to send his public key and select only this key when encrypting file
- One of the matching Private keys is required to decrypt (unlock) the file. Passphrase is required to use private key
- To avoid jeopardizing the whole security idea NEVER share your private key with other people and DO NOT send private key over the internet



HOW PGP ENCRYPTION WORKS

1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

Starting with OpenPGP

PGP stands for Pretty Good Privacy. Prefix "Open" means that this is an open standard, many applications support it.

OpenPGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures.

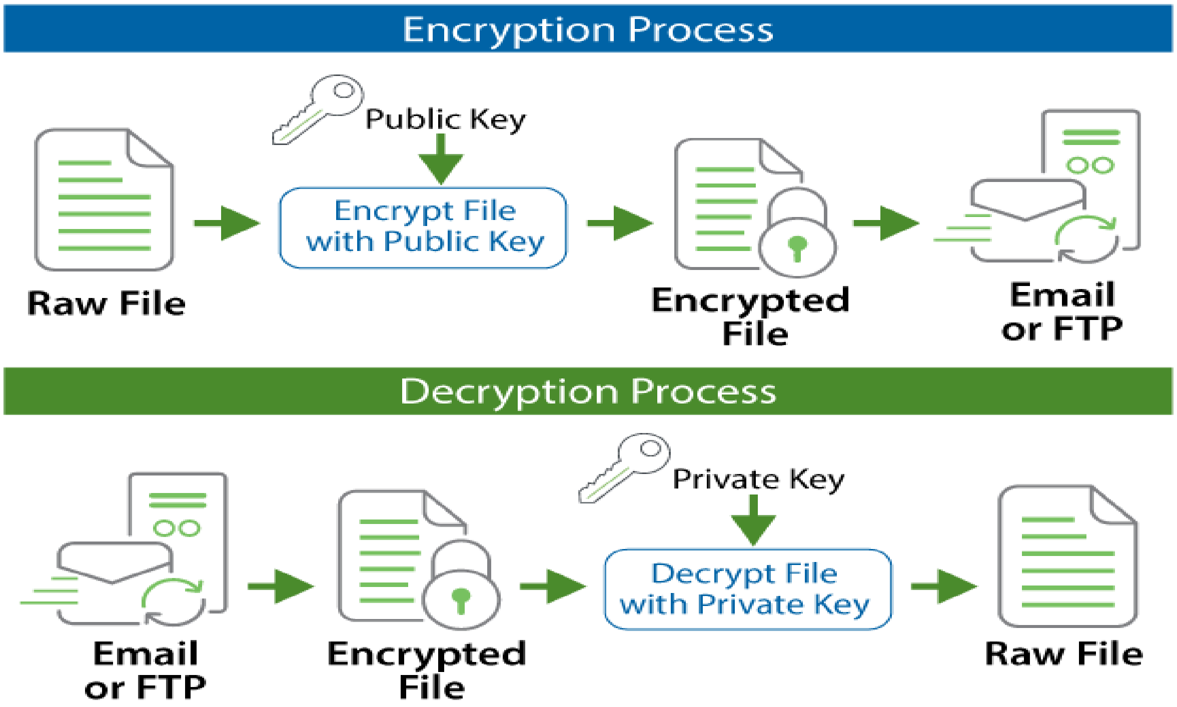
How to Encrypt Files with Open PGP

Open PGP's file encryption tool enables us to both store sensitive information and transmit that information across insecure networks, such as the internet or email, so that it cannot be read by anyone except the intended recipient.

A public key is used to encrypt a file and verify a signature. A private key is used by the owner to decrypt and to add a digital signature to files.

The major steps required to encrypt files with Open PGP:-

1. Get your trading partner’s public key to encrypt the file.
2. Import your trading partner’s public key into a Key Vault.
3. Use your file transfer tool to create a Project to encrypt the file. Sign the file with your private key if required.
4. Confirm that the project was set up correctly before executing.



PGP Key Management

Keys are protected and organized into Key Vaults for security access controls. Access the Key Management System through the Encryption menu.

Protecting a File with PGP Encryption

To get started, we first encrypt a file that we can send to our trading partner. We will need our trading partner's public key to encrypt the file. Oour trading partner will use their private key to decrypt the file once it is received.

Signing a File

Digital signatures allow your trading partner to ensure that you are the true originator of the files. You only need to sign a file if your trading partner requires that you sign your files with your private key. This will embed a digital signature into those files, and your trading partner will use your public key to authenticate your identity when decrypting the files.

1. To add a signature, expand the Secret Key panel and select the Add a Secret Key option.
2. On the Key Name field, select your private key and enter the Password of the key. If you do not have a private key, you can create one in the Key Vault.

Precautions while encryption

- You should always verify the hash of the file with the recipient or sign it with your private key, so the other person knows it actually came from you.
- If there is a man-in-the-middle, then he/she could substitute the other person's public key for his/her own and then you're screwed. Always verify the other person's public key (take a hash and read it to each other over the phone).

-------------------------------THE END-----------------------------------