# Secure communication between two scomputer File Transfer Between Two Kali Linux VMs

## Configure Both Kali VMs on the Same Network

1. In VirtualBox > VM Settings > Network, choose 'Bridged Adapter'.

2. Enable the network adapter and select your physical network interface (Wi-Fi or Ethernet).

3. Boot both VMs and check IPs using `ip a`.

4. Use `ping <other-vm-ip>` to confirm connectivity.

## Set Up SSH Key-Based Authentication

1. Generate SSH Key Pair on your Kali VM:

`ssh-keygen` (accept defaults, optional passphrase).

2. Copy your public key to Hammad's VM:

`ssh-copy-id kali@<Hammad\_VM\_IP>`

3. Test SSH login:

`ssh kali@<Hammad\_VM\_IP>` → should not ask for a password.

## Encrypt Files Using GPG

There are two methods: passphrase-based (symmetric) and public-key-based (asymmetric).

## Option A: GPG Encryption Using Passphrase

1. Encrypt:

`gpg -c myfile.txt` → enter a passphrase

2. Send using SCP:

`scp myfile.txt.gpg kali@<Hammad\_VM\_IP>:~`

3. Hammad decrypts:

`gpg myfile.txt.gpg`

## Option B: GPG Encryption Using Public Key

1. Hammad generates key:

`gpg --full-generate-key`

2. Export Hammad’s public key:

`gpg --export -a "Hammad" > hammad\_pubkey.asc`

3. You import the key:

`gpg --import hammad\_pubkey.asc`

4. Optional: Trust the key via `gpg --edit-key "Hammad"` → trust → 5 → quit

5. Encrypt:

`gpg -e -r "Hammad" secret.txt`

6. Send using SCP:

`scp secret.txt.gpg kali@<Hammad\_VM\_IP>:~`

7. Hammad decrypts:

`gpg secret.txt.gpg`

## Comparison: Passphrase vs Key-Based Encryption

| Feature | Passphrase (`gpg -c`) | Public/Private Key (`gpg -r`) |

|-------------------------------|--------------------------------|----------------------------------|

| Key Distribution | Manual (share passphrase) | Encrypt with public key |

| Security Level | Medium | High |

| Multi-Recipient Support | No | Yes |

| Ease of Use | Simple | Slightly more setup |

| Portability | Easy | Needs private key to decrypt |