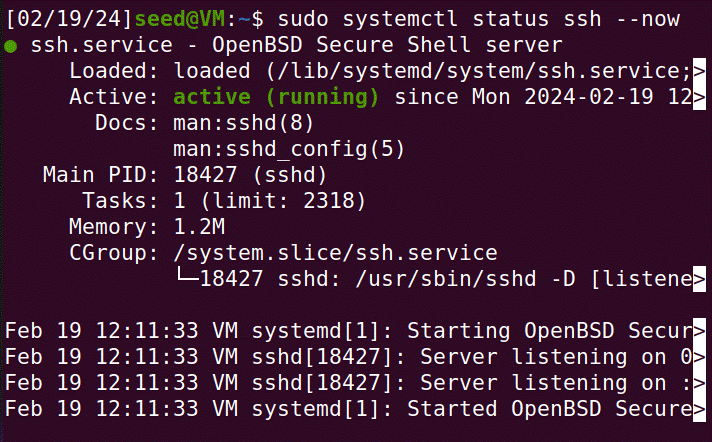
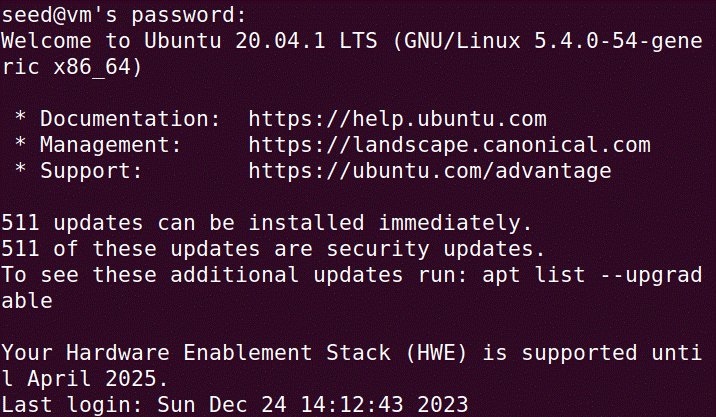
Lab1

1. **Lab Set-up**

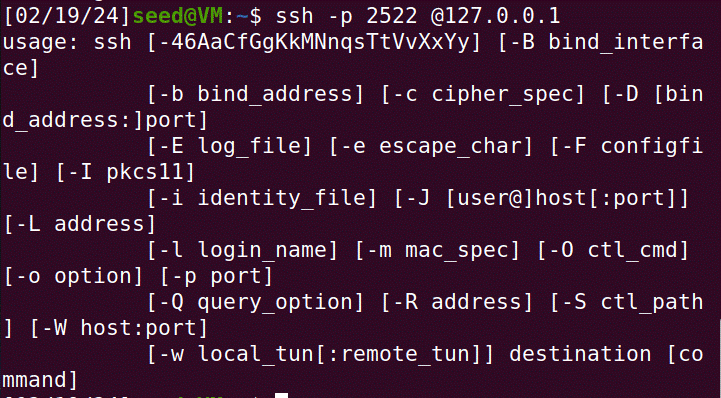
Based on the requirements, I have successfully set up VM and SSH to use it in the Windows teriminal.



**Figure 1.1. the systemctl status**

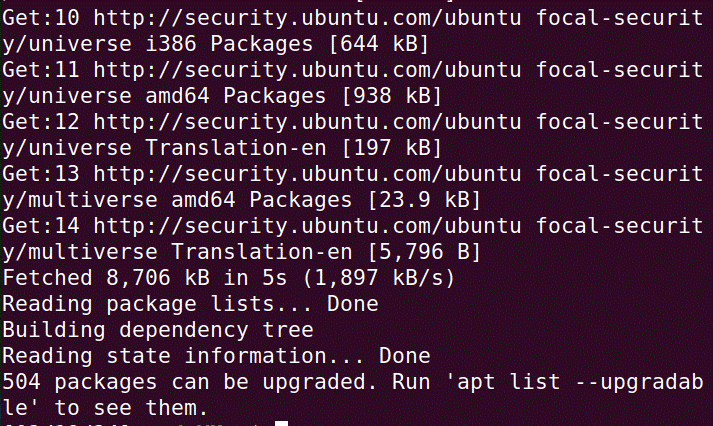
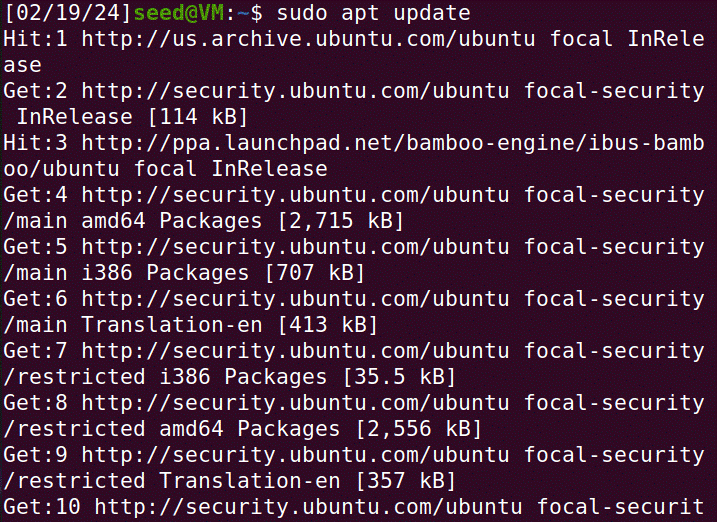


**Figure 1.2. The user interface of SSH into the VM**

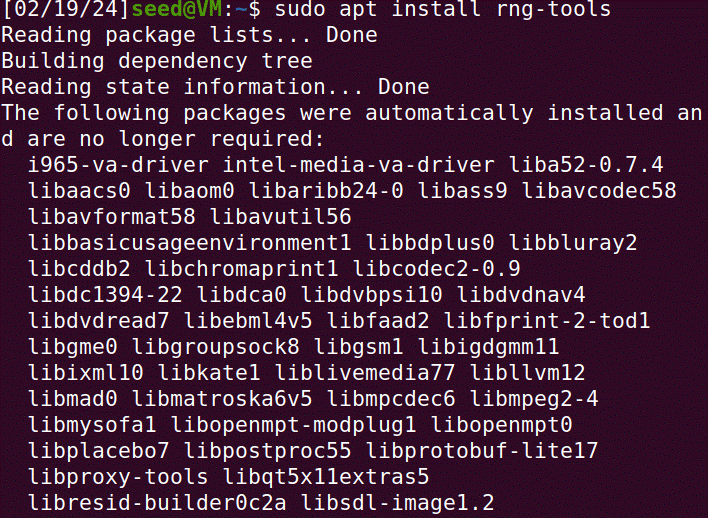


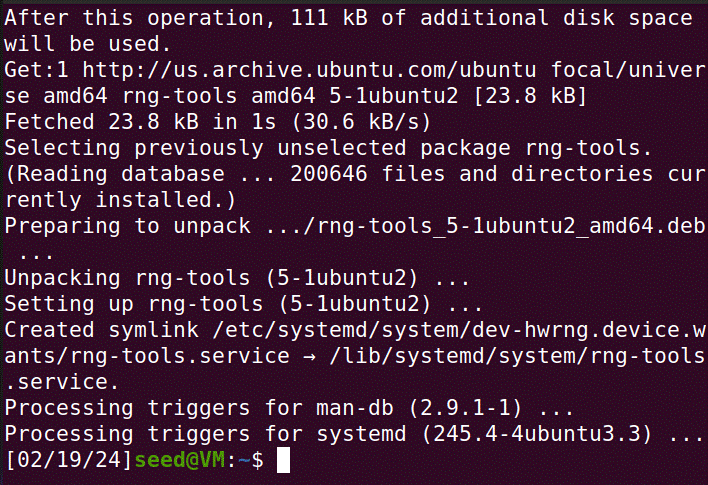
**Figure 1.3. The user interface of SSH NAT access to VM**

1. **Update and Install Software**



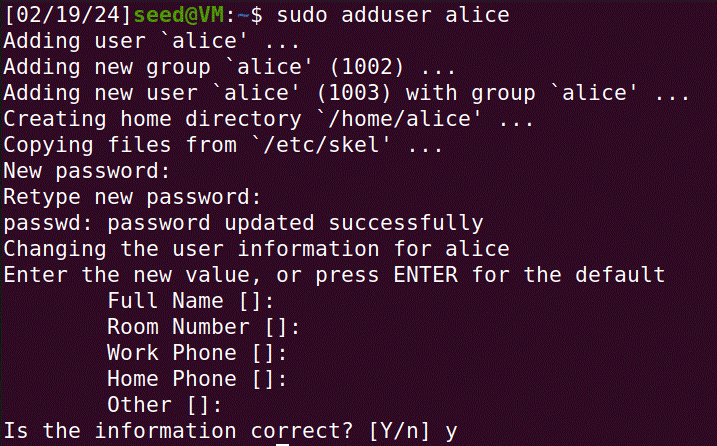
**Figure 2.1. Sudo apt update**

**

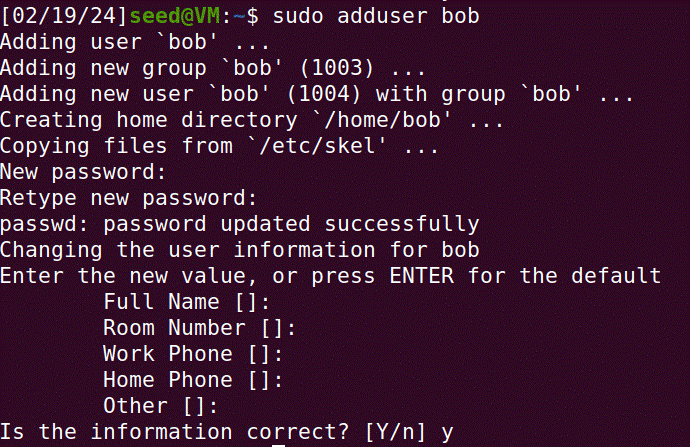
**

**Figure 2.2. Sudo apt install rng-tools**

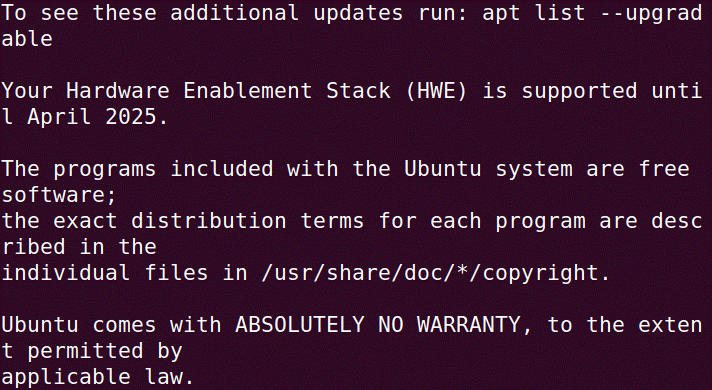
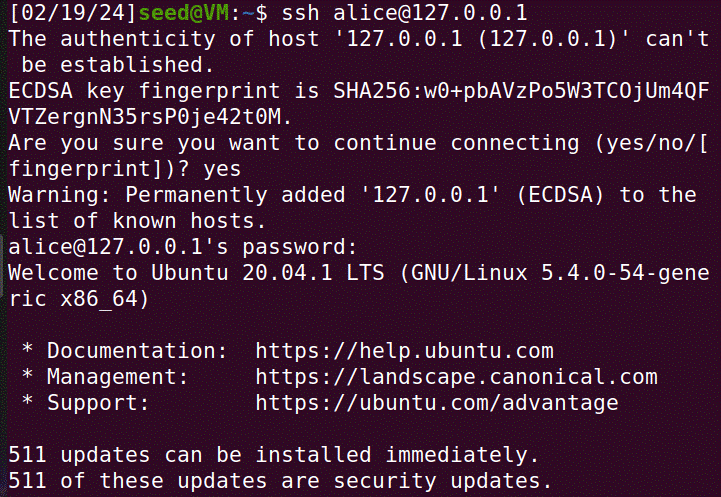
1. **Create user account**

****

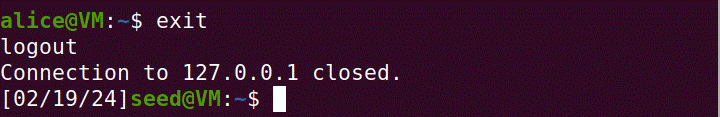
**Figure 3.1. Creating Alice account on the VM**

****

**Figure 3.2. Creating Bob account on the VM**



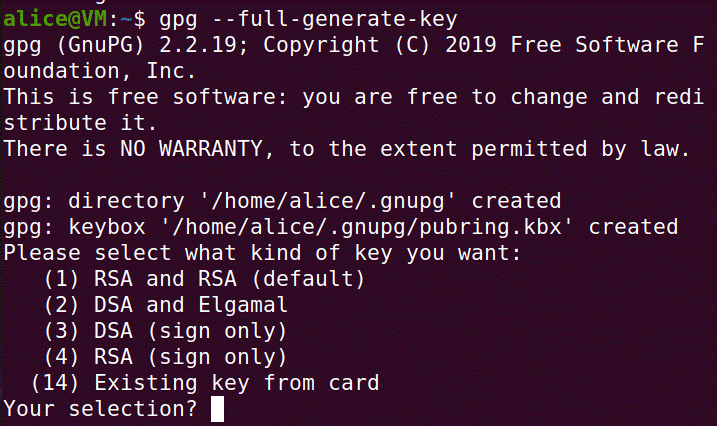
**Figure 3.3. switch to alice account on the VM**

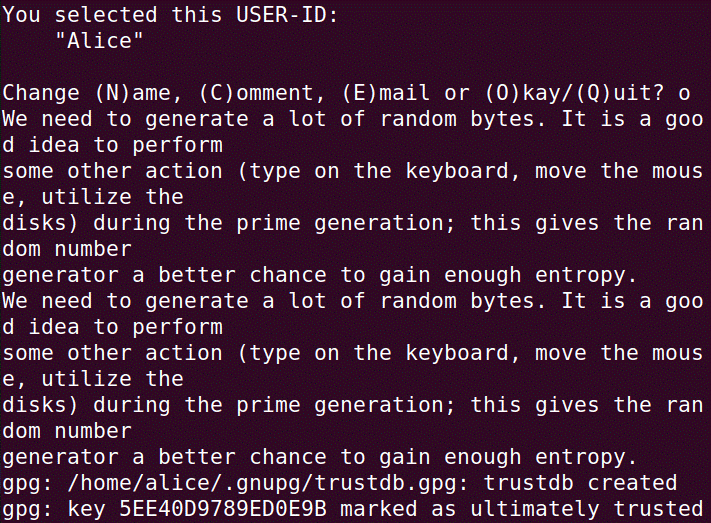


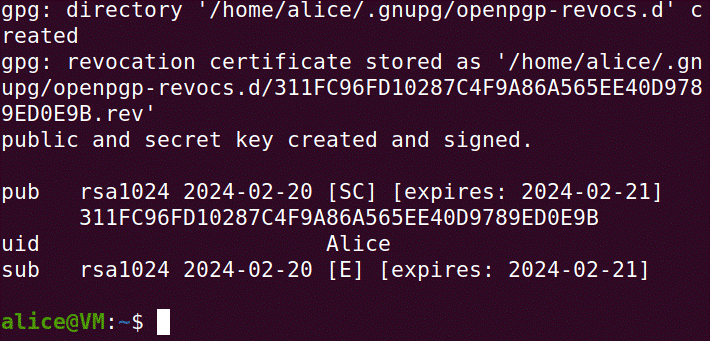
**Figure 3.3. log out alice account on the VM**

1. **The GNU Privacy**

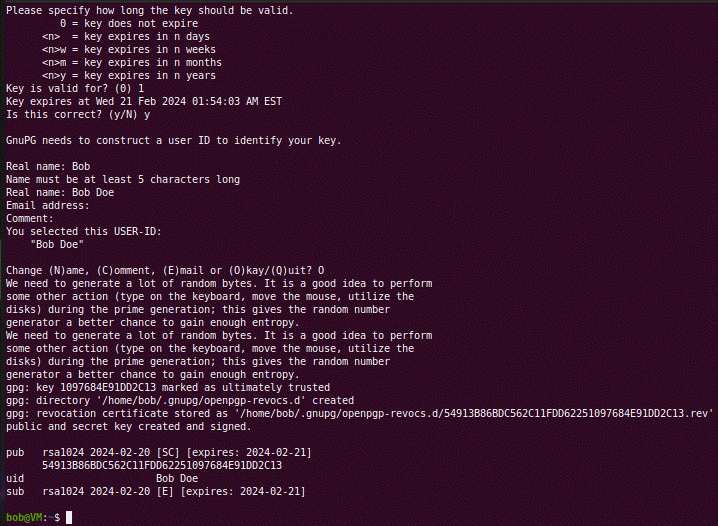
**1. Generating a new keypair**







**Figure 4.1.1. GPG key generation for Alice**

****

**Figure 4.1.2. GPG key generation for Bob**

**Question 1**: What is the meaning of the first RSA and the second RSA in the option of keypair?

The public and private keys are generated using RSA, which produces hashes that are greater than those produced by any traditional technique. Encrypting data and verifying the system are also faster.

**Question 2:** What is the keysizes that are available for RSA? Between longer key or shorter key, which key provides better security?

For RSA, the allowable key sizes range from 512 to 4096. The longer the key, the harder it is to crack as the number of bits increases.

**Question 3:** What does USER-ID for the keypair consist of?

USER-ID for the keypair consist of real name, email address and comment.

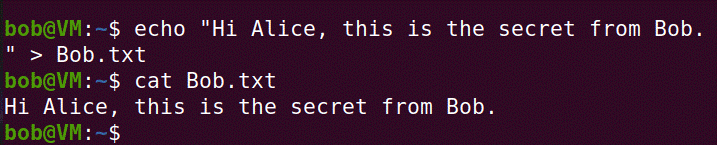
**Question 4:** What is the use of passphrase in the key generating process?

It's employed to raise the private level of a private key that must be kept secret when a user gains access to it.

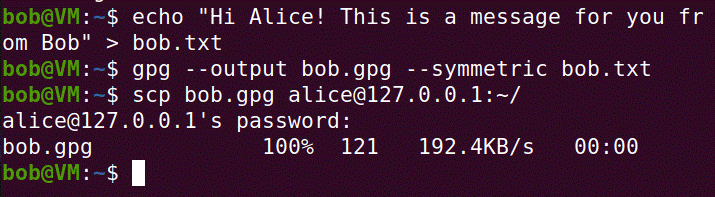
**Question 5:** What is the key id for the public key?

When keeping several public keys on a server or keychain, it is utilized to identify the true public key. It might be considered the public key's reference.

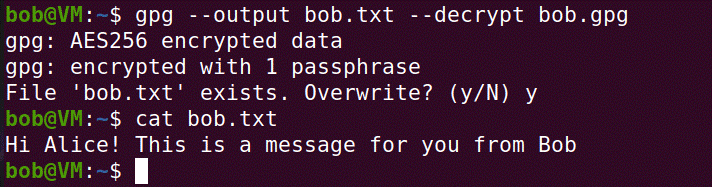
**2. Creating secret texts**



**3. Encrypting the secret using symmetric encryption**

****

**Figure 4.3.1: Encrypting the secret and send the message to alice**

****

**Figure 4.3.2: Decrypting the secret and send the message to alice**

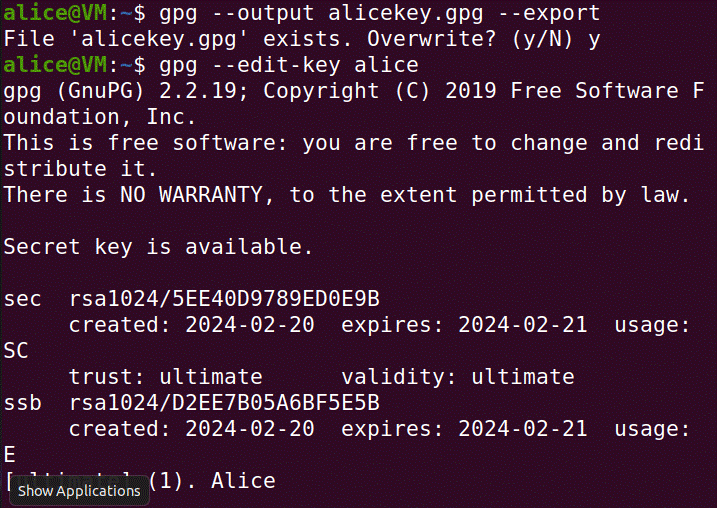
**Question 6:** How is the symmetric key generated?

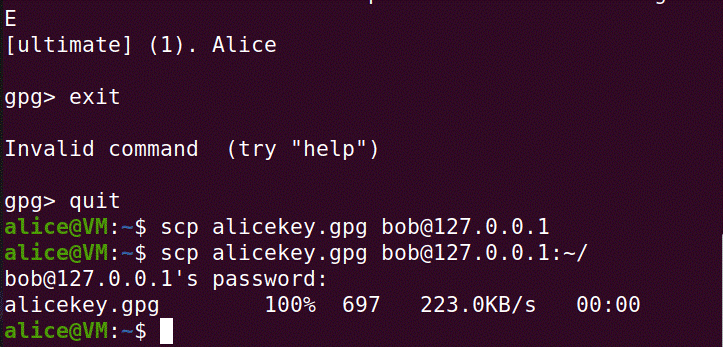
It is produced when a person encrypts a file with a passphrase that is distinct from the passphrase associated with their own private key.

**Question 7:** Change to Alice’s account and decrypt the message sent from bob.gpg. Does Alice need to know Bob’s private key to decrypt the ciphertext? What key does Alice use and where deos it come from?

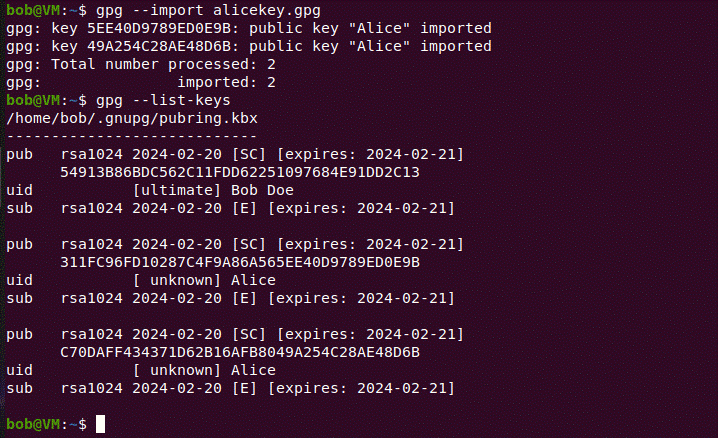
Since symmetric encryption does not require Bob's private key, Alice can decipher the ciphertext without knowing it. In order for Alice to successfully decrypt Bob's ciphertext, she needs to employ the passphrase, which originates from their first conversation or agreement.

1. **Exchanging keys**

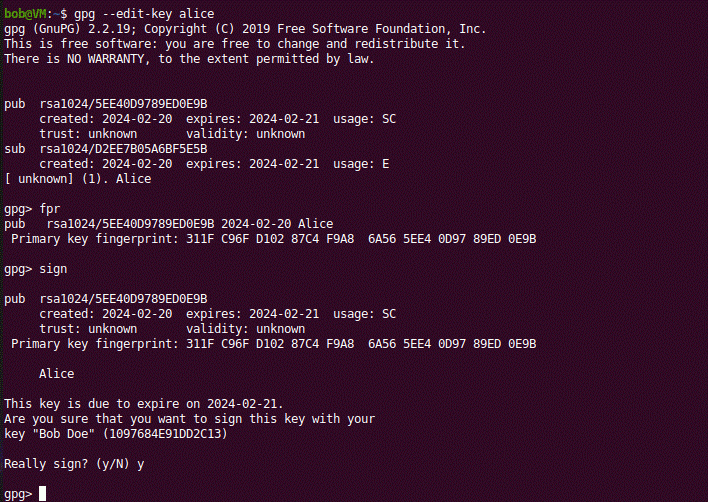
****

****

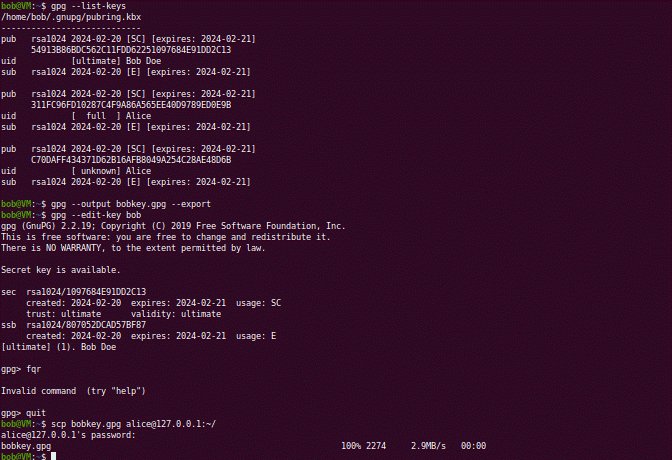
**Figure 4.4.1. Export Alice’s public key and view its fingerprint**

****

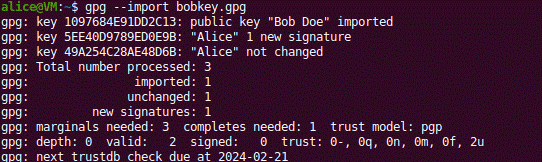
**Figure 4.4.2. Import Alice’s public key to bob keychain**

****

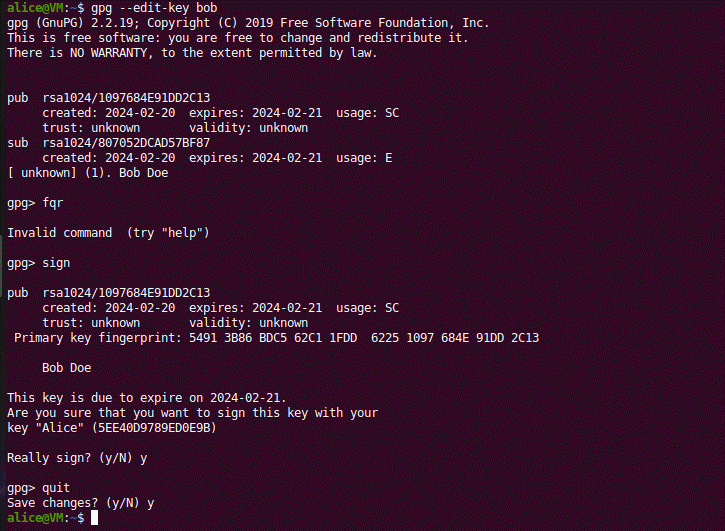
**Figure 4.4.3. Compare Alice’s public key fingerprint and sign it with Bob’s key**

****

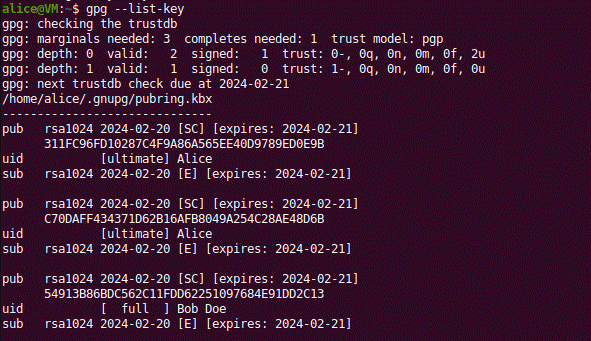
**Figure 4.4.4. Check for Bob’s keychain again and do the exchange of his key**

****

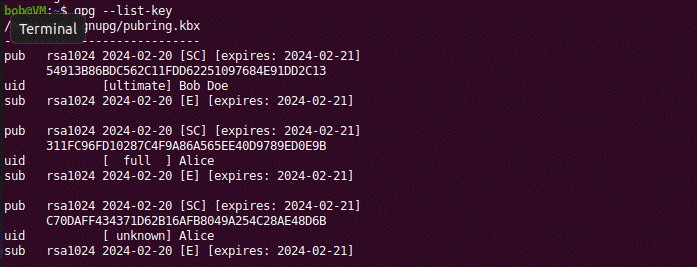
**Figure 4.4.5. Import** **Bob’s public key on Alice's account**

****

**Figure 4.4.6. sign** **Bob’s public key on Alice's account**

****

**Figure 4.4.6. check keychain of alice**

****

**Figure 4.4.6. check keychain of bob**

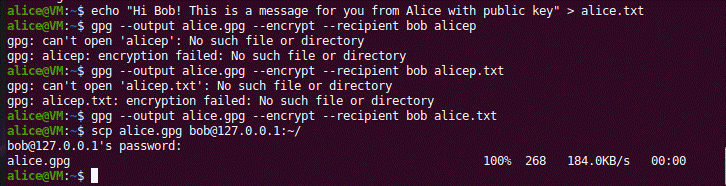
**Question 8:** What are the type of keys are exported and imported?

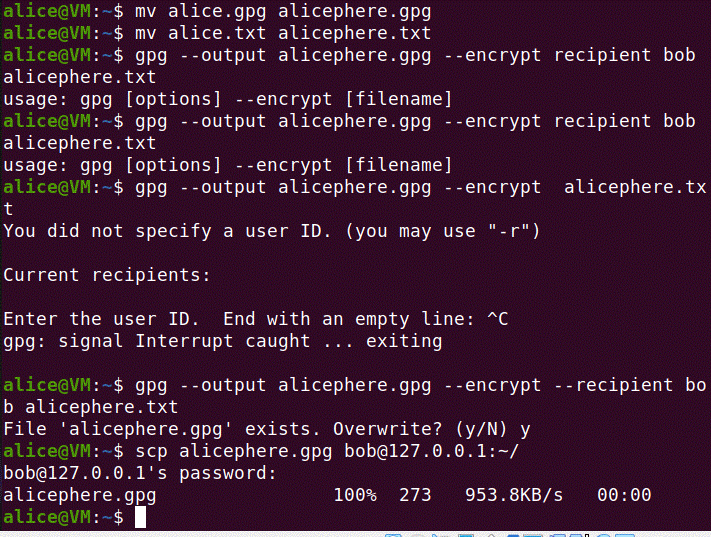
It is the public keys of one and their partner that are exported and imported.

**Question 9:** When import a key into your keyring, you sign the key. What is the implication of signing for that key?

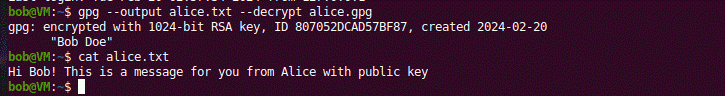
It indicates that whomever signs the key with their private key is certain that the one making the claim indeed owns the key. By signing it, you are indicating that you understand who is truly behind it and that you trust this public key.

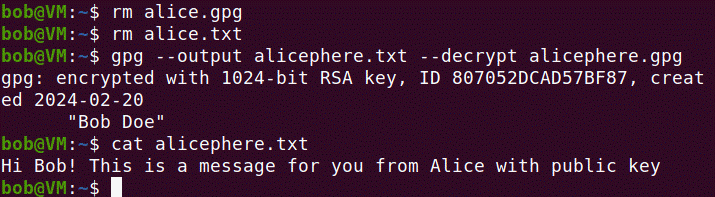
1. **Encrypt using a public key**

****

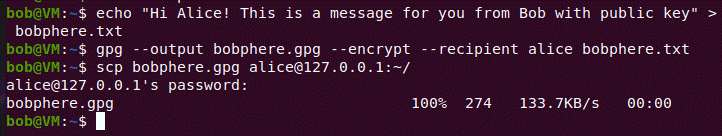
****

**Figure 4.5.1. Alice creates the message, encrypts it, and sends it to Bob's account**

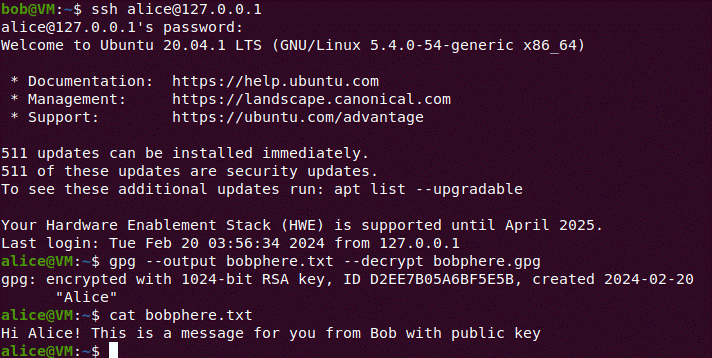
****

****

**Figure 4.5.2. Bob decrypt the cipheretxt .txt**

****

**Figure 4.5.3. Bob creates the message, encrypts it, and sends it to Alice’s account**

****

**Figure 4.5.2. Bob decrypt the cipheretxt .txt**

**Question 10:** Which key does Alice use to encrypt? Can Alice use her own public key?

Bob's public key is used by Alice to encrypt the text message. Bob's private key may not be used to decrypt it; Alice can still use her public key.

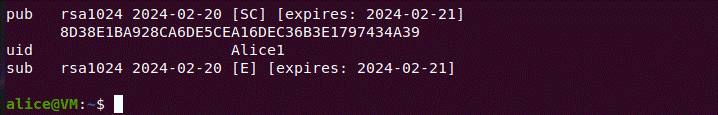
**Question 11:** Which key does Bob use to decrypt?

Bob decrypts Alice's message with his private key.

**Question 12:** GPG use hybrid cipher for encryption/decryption. What is is? What are the keys involved in hybrid cipher and what are they used for?

A hybrid cypher is one in which the session key and the delivered message are automatically combined into a single package and encrypted using public key and symmetric cyphers, respectively. The recipient uses his private key to decipher the session key, after which he uses that session key to unlock the message.

1. **Distributing keys**

****

**Figure 4.6.1. Alice1 ‘s public key, userId and subkey**

****

**Figure 4.6.1. Alice1 ‘s public key to the server, specifiying the ID(0X+ 8 digits in public key)**

**A computer screen shot of a computer

Description automatically generated**

**Figure 4.6.3. Find that key with the ID and import the public key “Alice1” to Bob’s account**

**A screenshot of a computer program

Description automatically generated**

**A computer screen shot of a computer

Description automatically generated**

**Figure 4.6.4. Sign the key on Bob’s account**

**A computer screen shot of a computer

Description automatically generated**

**Figure 4.6.4. Make sure the key is working on Bob‘s keychain**

**A computer screen with white text

Description automatically generated**

**Figure 4.6.1. Bob 1 ‘s public key, userId and subkey and Bob 1 ‘s public key to the server, specifiying the ID(0X+ 8 digits in public key)**

**A screen shot of a computer

Description automatically generated**

**Figure 4.6.6. Find that key with the ID and import it to Alice’s account**

**A screenshot of a computer program

Description automatically generated**

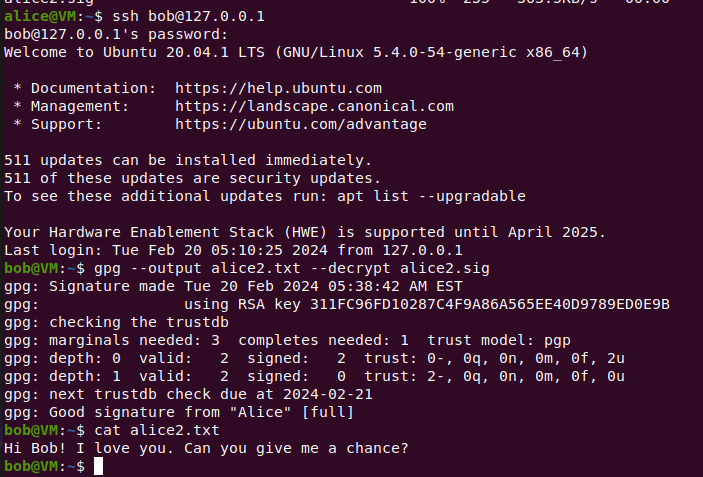
**Figure 4.6.7. Make sure the key is working on Alice‘s keychain**

1. **Digitally sign documents**

**A screenshot of a computer screen

Description automatically generated**

**Figure 4.7.1. Alices creates a new message, sign with hẻ private key, and send it to Bob**

****

**Figure 4.7.2. swith to the Bob account, and decrypt it and cat alice2.txt**

Question 13: Which key does Alice use to sign?

Alice signs the message with her secret key.

Question 14: Which key does Bob use to decrypt?

Bob must decrypt the ciphertext and obtain both the message and the signature status using Alice's public key.

Question 15: Can Alice sign without encrypting the message?

Without encryption, Alice can still sign the message, but she is unsure if its contents are kept private. If someone does not have Alice's public key, they can view the message but cannot confirm whether it originates from Alice.