SSH KEY GENERATION

```
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

- -t Type of encryption algorithm to use for SSH key pair.
- -b Bit Size of the generated key
- -C add comment to the generated key pair.

Upon running the prompt you will be prompted to enter file in which to save the key, the default is (/home /user /.ssh /id_rsa)

Then a passphrase to protect the private key. If empty the private key will be unencrypted and less secure.

Public key will be saved in file named id_rsa.pub
Private key will be saved in file name id_rsa

The terminal will then print the fingerprint & Randomart

Fingerprint

Fingerprint is a short, unique identifier for the public key. It’s a cryptographic hash (usually SHA256) of the key’s content

When connecting to a server, you can compare the fingerprint of the server's public key with the one you have recorded. This helps ensure you're connecting to the correct server and that the key hasn't been tampered with
You can use the fingerprint to easily identify a specific key among multiple keys.

Randomart

Randomart - A visual representation of the key's fingerprint. It's an ASCII art image generated from the hash of the public key.

Comparing the randomart images of two keys is often easier and less error-prone than comparing long strings of hexadecimal characters in the fingerprint.
The unique patterns in the randomart image can help you quickly recognize a specific key.

While the randomart image is helpful for visual verification, it's not as cryptographically secure as the fingerprint itself. Always prioritize using the fingerprint for secure key verification.