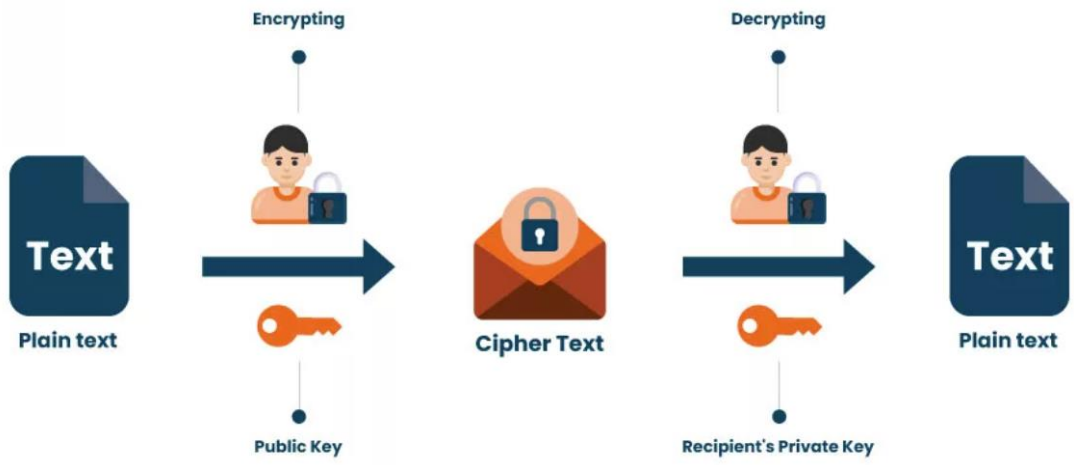
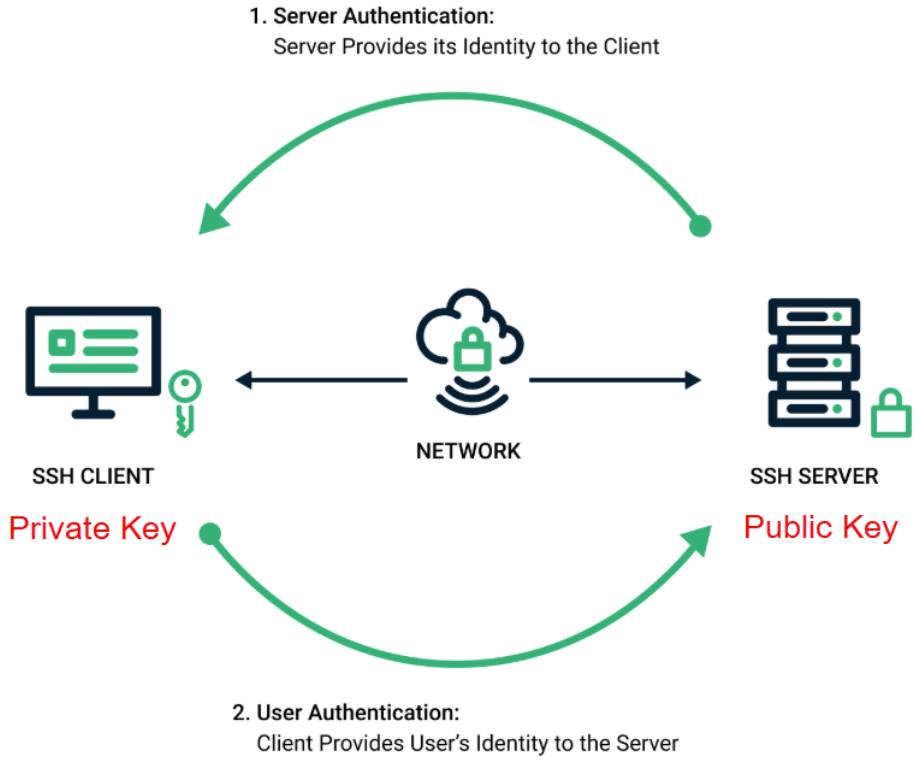
# PuTTYgen

## ทฤษฎีที่เกี่ยวข้อง

- Asymmetric Cryptography (Private/Public Key)




- SSH Authentication

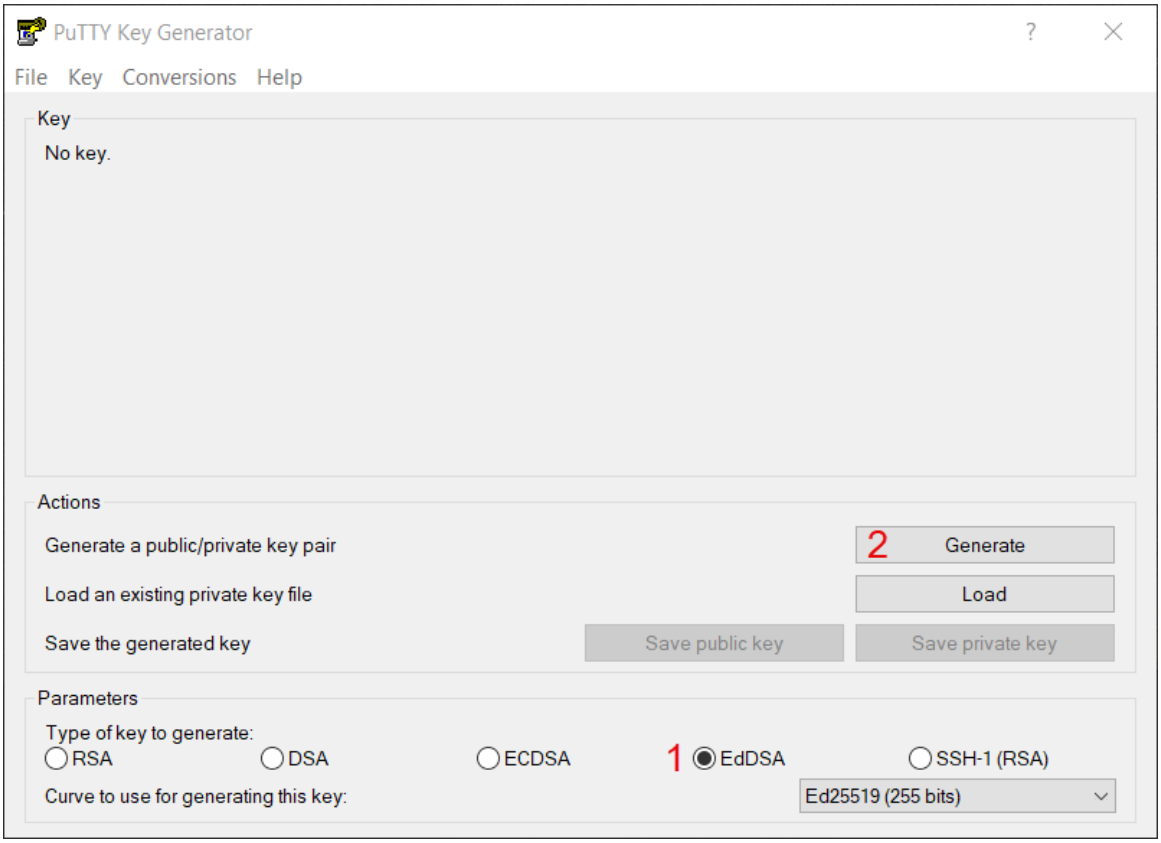


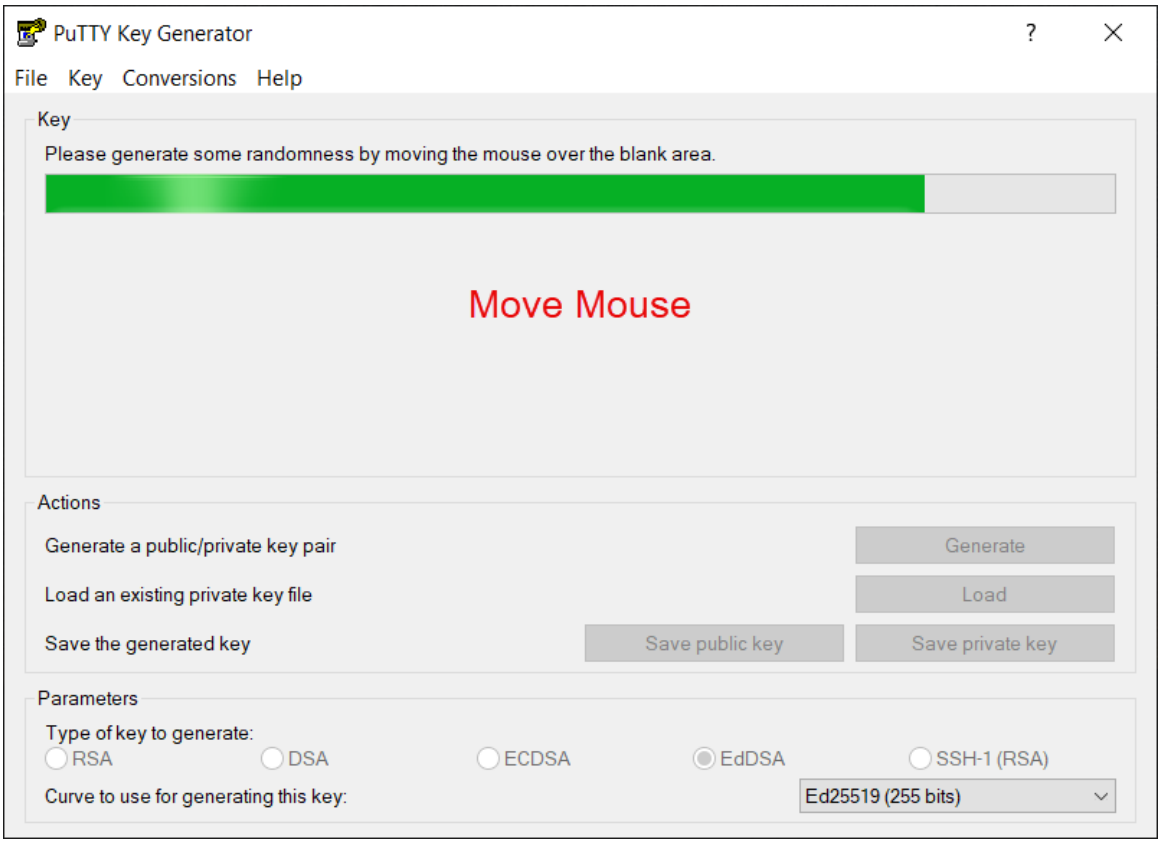
## Private key

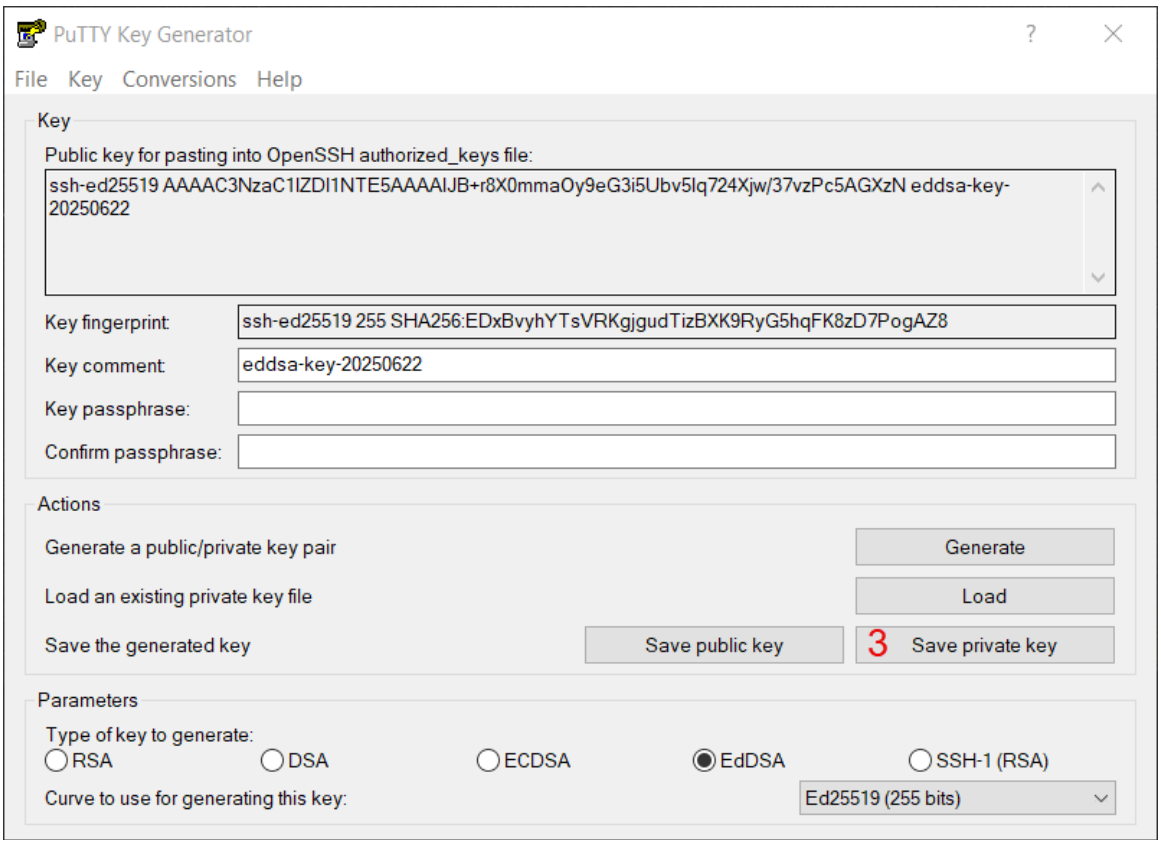
1. เปิดโปรแกรม PuTTYGen

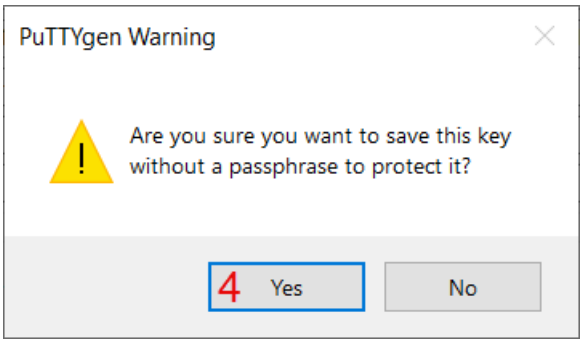
`puttygen.exe`

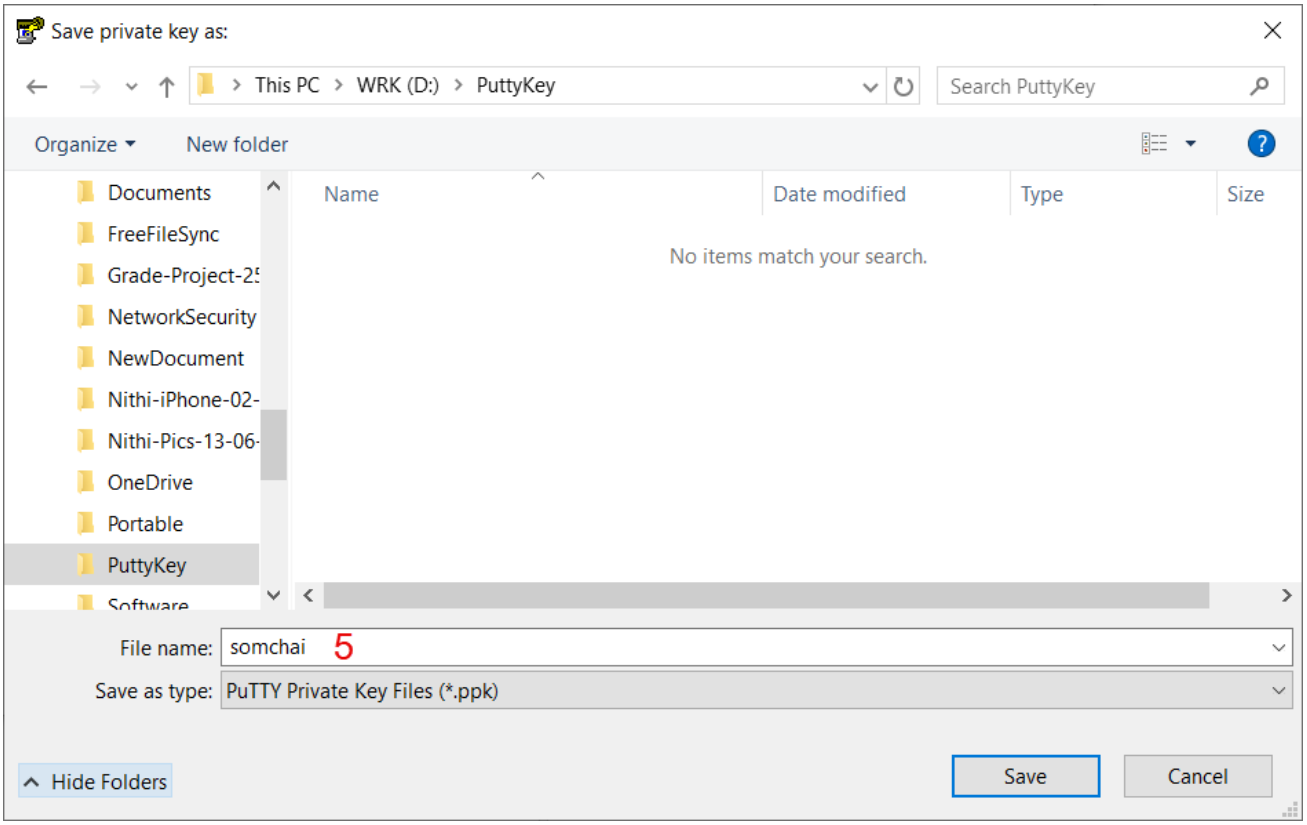
2. สร้างรหัสแบบ EdDSA algorithm




PuTTY Key Generator
File Key Conversions Help
Key
Please generate some randomness by moving the mouse over the blank area.
Move Mouse
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Curve to use for generating this key:
Ed25519 (255 bits)


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJB+r8X0mmaOy9eG3i5Ubv5lq724Xjw/37vzPc5AGXzN eddsa-key-20250622
Key fingerprint:
ssh-ed25519 255 SHA256:EDxBvyhYTsVRKgjgudTizBXK9RyG5hqFK8zD7PogAZ8
Key comment:
eddsa-key-20250622
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
3
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)
Curve to use for generating this key:
Ed25519 (255 bits)




- ขั้นตอนที่ 4 ไม่ใส่ Passphrase (รหัสผ่านสำหรับใช้งาน Private Key)

```
Using username "somchai"
Authenticating with public key "eddsa-key-20240626"
```

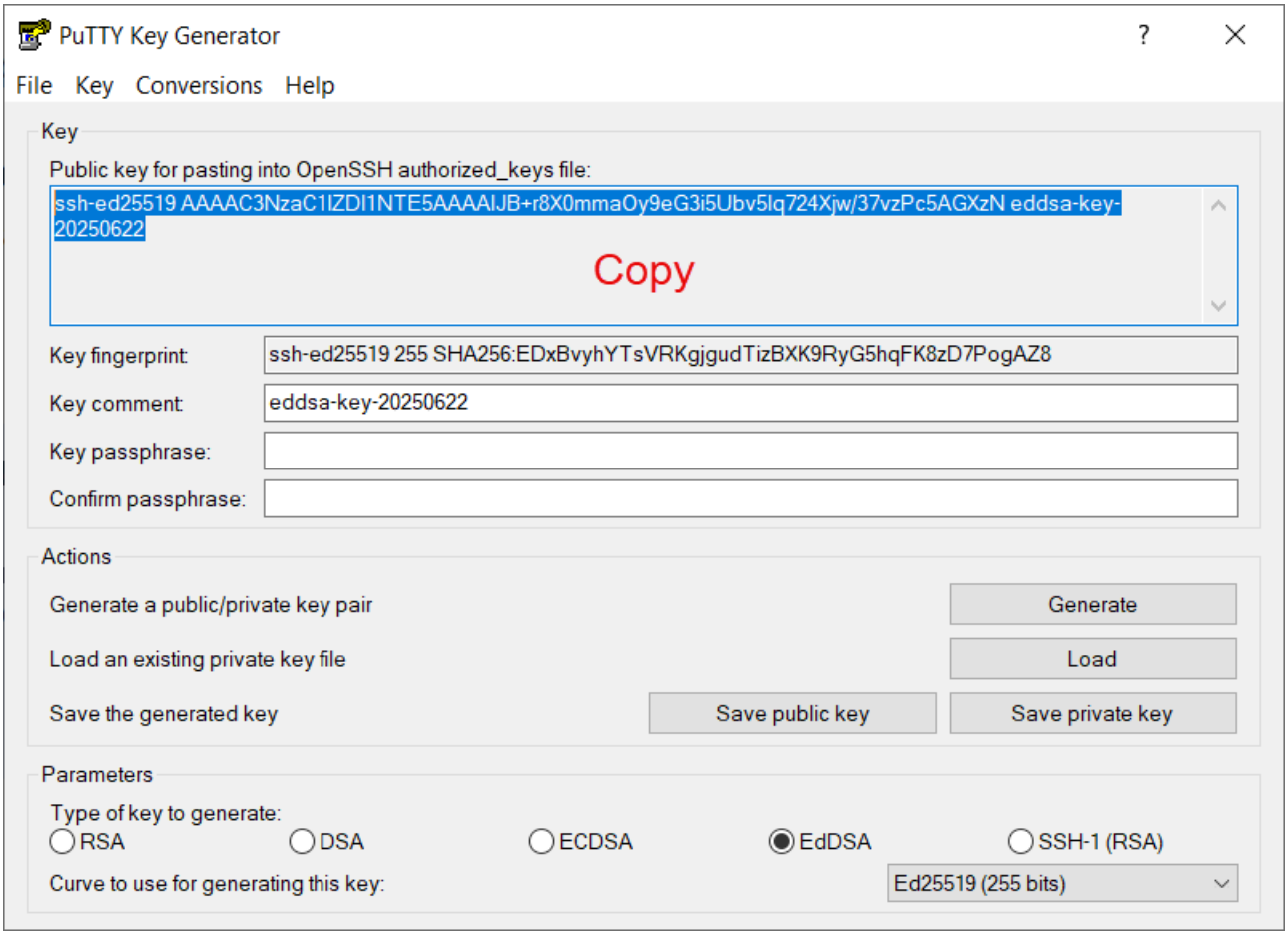
- ในกรณีที่ใส่ Passphrase เมื่อ login

```
Using username "somchai"
Authenticating with public key "eddsa-key-20240626"
Passphrase for key "eddsa-key-20240626": [hidden]
```

## Public Key

1. บันทึก public key เพื่อใช้กับ OpenSSH บนเซิร์ฟเวอร์

```
New text file > somchai.pub > Paste "ssh-ed25519 AAAAC3 ..."
```




2. สร้างไฟล์ authorized_keys เพื่อเก็บ public key บนเซิร์ฟเวอร์
    - login เข้าเซิร์ฟเวอร์ด้วย username/password
    - สร้างไดเรกทอรี (dot นำหน้า)

```
mkdir .ssh
```

    - สร้างไฟล์

```
nano .ssh/authorized_keys
```

    - วาง public key จากไฟล์ somchai.pub
    - บันทึกไฟล์

3. หากต้องการเพิ่ม public key ของคนอื่น ให้เพิ่มต่อในบรรทัดถัดไป