In asymmetric encryption there are two keys, private and public key.

A user encrypts data with private key and gives public key to user you wants to decrypt this encrypted data. If the other will have public key then only he will be able to decrypt data otherwise he will not be able to decrypt data. This is called Asymmetric Encryption.

RSA Algorithm is an example of Asymmetric key Encryption Algorithm.

OpenSSL is a software that helps you generate private and public key using RSA Algorithm.

Install Openssl for windows from website

https://wiki.openssl.org/index.php/Binaries

create a folder in windows with name rsa_keys

now go to directory where you have installed openssl

Below are some command to create rsa keys with openssl

openssl genrsa

generates rsa private key of 2048 bits

openssl genrsa -aes256

generates rsa private key of 2048 bits with aes256 encryption

above command will ask for a pass phrase or password used for aes256 encryption

openssl genrsa -aes256 -out c:\rsa_keys\private.pem

above command will generate private key of 2048 bits encrypted with aes256 encryption algorithm and will save the private key to file c:\rsa_keys\private.pem

public key is included within the private key, we can extract public key from private key.

Command to extract public key from private key is given below

openssl rsa -in c:\rsa_keys\private.pem -outform PEM -pubout -out c:\rsa_keys\public.pem

above command will take private key from file c:\rsa_keys\private.pem and extract public key from it in file c:\rsa_keys\public.pem, it will also ask for pass phrase or password entered by the user while creating private key.

openssl genrsa 4096

above command will create a private key of length 4096 bits