**OpenSSL [ genpkey, pkey, pkeyutl ]**

**Introduction**

OpenSSL is a powerful toolkit widely used for implementing cryptographic functions and securing communications. It provides command-line tools and libraries for cryptographic operations such as generating keys, certificates, encrypting/decrypting data, and creating secure network connections

**Generating Private Key**

The genpkey command in OpenSSL is used to generate private keys for various cryptographic algorithms. It's a versatile command that supports multiple algorithms such as RSA, EC, DH, and Ed25519.

*openssl genpkey -algorithm <algorithm> -out <output\_file\_name> -pkeyopt <key\_size>*

*(or)*

*openssl genpkey -algorithm RSA -out rsa\_private\_key.pem -pkeyopt rsa\_keygen\_bits:2048*

*(or)*

*openssl genpkey -algorithm EC -out ec\_private\_key.pem -pkeyopt ec\_paramgen\_curve:P-256*

*(or)*

*openssl genpkey -algorithm DH -out dh\_private\_key.pem*

**Note**

To generate private key for DH algorithm we need to first create dhparam file which can be done using

*openssl dhparam -out dhparams.pem 2048*

**Generating Public Key**

The pkey command in OpenSSL is used for manipulating and processing public and private keys. It allows you to perform various cryptographic operations with keys, such as generating, converting, or performing operations like encryption, signing, and verifying signatures.

*openssl pkey -in <private\_key> -pubout -out <output\_public\_key\_file\_name>*

*(or)*

*openssl pkey -in rsa\_private\_key.pem -pubout -out rsa\_public\_key.pem*

**Encrypting Data**

The openssl pkeyutl command is used to perform cryptographic operations such as encryption, decryption, signing, and verification using public and private keys. It supports a variety of algorithms, including RSA, EC (Elliptic Curve), and others.

*openssl pkeyutl -encrypt -in <file\_to\_encrypt> -pubin -inkey <input\_public\_key> -out <output\_file\_name>*

*(or)*

*openssl pkeyutl -encrypt -in message.txt -pubin -inkey rsa\_public\_key.pem -out encrypted\_message.bin*

**Note**

-pubin option indicates encryption using the public key.

**Decrypting Data**

To decrypt the data pkeyutl is used with following options.

*openssl pkeyutl -decrypt -in <file\_to\_decrypt> -inkey <input\_private\_key> -out <output\_file\_name>*

*(or)*

*openssl pkeyutl -decrypt -in encrypted\_message.bin -inkey rsa\_private\_key.pem -out decrypted\_message.txt*