| openssl help openssl enc help |
| --- |

--------------------------AES-------------------------------------------

encrypt:

| openssl aes-256-cbc -e/-a (-nosalt) -in secret-file -out secret-file.enc |
| --- |

decrypt:

| openssl aes-256-cbc <-d, -d -base64> -in secret-file -out secret-file.enc |
| --- |

example:

| openssl aes-256-cbc <-d, -d -base64> -in secret-file -out secret-file.enc |
| --- |

AES KEY 128,192, 256 bits

------------------------------RSA--------------------------------------

| openssl genrsa help |
| --- |

// GENERATE RSA PAIR

| openssl genrsa -des3 -out private.pem 2048 |
| --- |

// This command generates the private.pem file. In order to find the public key from the private key, run

| openssl rsa -in private.pem -pubout -out public.pem  openssl rsa -in private.pem -out privatekey.pem // afaireis to passphrase  openssl genrsa -out private.pem 2048 //xwris passphrase  openssl rsa -noout -text -in private.pem // to see the parametrous |
| --- |

-----for signature-----

| openssl rsautl -sign -inkey private.pem -in sender.txt > filename.txt // encrypt with private key  openssl rsautl -verify -inkey public.pem -pubin -in sender\_enc\_prv // decrypt |
| --- |

OR

| openssl rsautl -verify -inkey private.pem -in sender\_enc\_prv // decrypt |
| --- |

// STILL USES THE PUBLIC KEY BECAUSE IT’S INCLUDED IN PRIVATE.PEM

-----for encryption/decryption-----

| openssl rsautl -encrypt -inkey private.pem -in rcv.txt -out rcvpub.enc // encrypt with PUBLIC KEY |
| --- |

OR

| openssl rsautl -encrypt -inkey public.pem -pubin -in rcv.txt -out rcvpub.enc2// encrypt  openssl rsautl -decrypt -inkey private.pem -in rcvpub.enc -out rcvtext.dec // decrypt with PRIVATE KEY |
| --- |

----------------------------------HASH------------------------------------------

| echo "Hello World" | openssl dgst -sha256  openssl dgst -sha256 ./random.data  openssl md5 |
| --- |

----------------------------------------------------------------------------------