Openssl alice bob

1. Make directory

* mkdir alice
* mkdir bob
* ls
* cd alice

1. confidentiality creating random key

* man rand
* openssl rand -hex 16
* openssl rand -hex 16
* openssl rand -out symm.key -hex 16
* ls
* cat symm.key

1. creating file with dummy data

* cat > plain.txt
* CNN isa is going on
* Cat plain.txt

1. Encrypting the content

* Man enc
* Openssl enc -list
* Openssl enc -aes -128-cbc -in cipher.txt -out cipher.txt -kfile symm.key

1. Creating 2048 bit RAS private key

* Openssl genrsa -out alicepritv.key 2048
* Ls
* Cat alicepritv.key

1. Extracking public key from alicepritv.key and storing in file alicepub.key

* Openssl rsa -in alicepritv.key -pubout > alicepub.key
* Ls
* Cat alicepub.key

1. Repeating 5 and 6 for bob

* Cd ../bob
* Openssl genrsa -out bobpriv.key 2048
* Ls
* Cat bobpriv.key
* Openssl rsa -in bobpriv.key -pubout > bobpub.key
* Ls
* Cat bobpub.key

1. Both exchange public key

* Cp bobpub.key ../alice/bobpub.key
* Ls ../alice/
* Cd ../alice
* Cp alicepub.key ../bob/alicepub.key
* Ls ../bob/

1. Alice send cipher text to bob

* Cp cipher.txt ../bob/cipher.txt
* Cd ../bob
* ls

1. alice encrypts symm.key using public key of bob

* openssl rsautl -encrypt -in symm.key -out symm.enc.key -inkey bobpub.key -pubin
* ls
* cat symm.enc.key

1. bob secrypts symm.enc.key and store in symm.dec.key

* cp symm.enc.key ../bob/symm.enc.key
* cd ../bob
* ls
* openssl rsautl -decrypt -in symm.enc.key -out symm.dec.key -inkey bobpriv.key
* ls
* cat symm.dec.key

1. bob decrypt using symm.dec.key and stores output

* ls
* cat symm.dec.key
* openssl enc -d -aes-128-cbc -in cipher.txt -out cipher.dec.txt -kfile symm.dec.key
* ls
* cat cipher.dec.txt
* cd ../alice
* ls
* cat plain.txt

integrity check

1. compute sha-512 hash on plain.txt

* man dgst
* openssl dgst -out hash.txt -sha512 plain.txt
* ls
* cat hash.txt

1. verifying the hash

* openssl dgst -out hashcheck.txt -sha512 plain.txt
* diff hashcheck.txt hash.txt

1. making changes to plain.txt

* cat plain.txt
* vi plain.txt
* cat plain.txt
* openssl dgst -out hashcheck.txt -sha512 plain.txt
* diff hashcheck.txt hash.txt

authentication check

1. computing MAC on plain txt

* openssl dgst -out plain.mac -hmac -sha512 plain.txt
* cat plain.txt
* ls
* openssl dgst -sha512 -sign alicepertiv.key -out alicemacsign.sign plain.txt

1. verifying MAC

* openssl dgst -sha512 -verify alicepub.key -signature alicemacsign.sign plain.txt

digital signature

1. alice create sha-512

* openssl dgst -out hash.sign -sign alicepriv.key -sha512 plain.txt
* ls
* cat hash.sign

1. alice send plain.txt and hash.sign to bob

* cp plain.txt ../bob/plain.txt
* cp hash.sign ../bob/hash.sign
* cd ../bob
* ls

1. bob verifies

* openssl dgst -sha512 -verify ../alice/alicepub.key -signature hash.sign plain.txt