Security Lab using CMD

Prepared by: Misganaw A

Email: ethiomisgie@gmail.com/mail@ethioptec.com

You Tube: @ethioptech or ethioptech

You can also practice this lab using Linux (Ubuntu) OS. The difference is *Windows CMD* uses *pkeyutl* while *Linux* uses *rsautl*

Common commands

cd

Used to change the directory. cd **Desktop/security**. This command will enable as to access a security folder in Desktop.

cd ..

used to back to the previous directory. suppose we are in **Desktop/security**. When we use **cd ..** command, we will back to Desktop directory

mkdir

Used to create new directory. Eg, **mkdir** security. This command will create a directory called security

dir

Used to view the content of a given directory

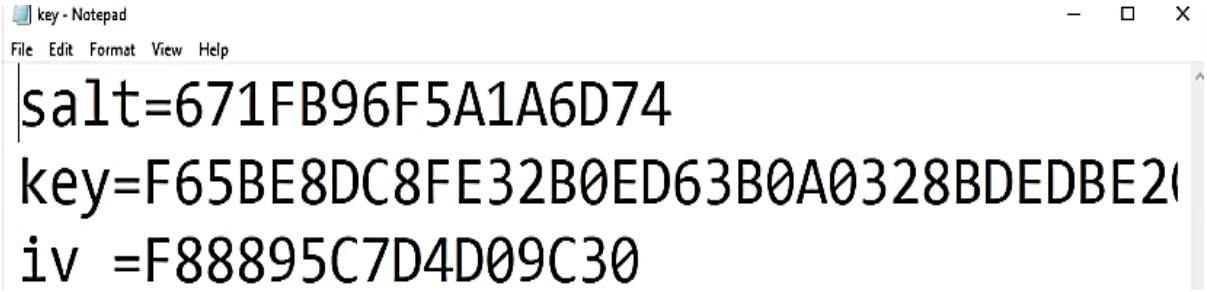
Lab 1: Creating Symmetric key

Objectives

- To create Symmetric key using Openssl on windows CMD
- To encrypt and decrypt the message using Symmetric key.

openssl enc -des3 -p

The created key could be look like the following.



- After getting the symmetric key copy in a note pad file as **.txt** file
- To open the notepad, write the command **notepad** on the CMD. This command will open notepad. Then you should copy the created key on the opened notepad and save it as **key.txt**.
- To show the created notepad file, write **notepad key.txt** on the CMD and it will open the notepad file in which your copied key is saved.
- Before starting encryption using the symmetric key, you should have a message to be encrypted. So, create the message.
- To create a message, write **notepad** on CMD and you will get notepad opened. Write the message and save it as **plaintext.txt.**
- After creating the message, use the created symmetric key to encrypt the message. To encrypt, write the following command on CMD.

openssl enc -des3 -in plaintext.txt -out encryptedtext.txt -k "key" -iv "iv".

- Write **notepad "**file name that will save encrypted message**".txt** on CMD to show the encrypted message.
- To decrypt the encrypted message, use the symmetric key and write the following command on CMD.

openssl enc -des3 -d -in encryptedtext.txt -out decryptedtext.txt -k "key" -iv "iv".

Lab 2: Create private and public key

Objectives

- To create private and public key using **Openssl** on windows CMD
- To encrypt and decrypt the message using public key and private key respectively.

Creating private key

Write the following command on CMD.

openssl genrsa -out prvtkey.pem 1024

Remember that you can give any name for the private key. Eg. **Prvtkey** or **prk** or **pr** etc.

To view the public key, you can use the following command on CMD

openssl rsa -in privat_key.pem -text -noout

Create public key

Write the following command on CMD.

openssl rsa -in prvtkey.pem -pubout -out pubkey.pem

Remember that you can give any name for the private key. Eg. **Pkey** or **pubk** or **puk** etc.

To view the public key, you can use the following command on CMD

openssl rsa -pubin -in public_key.pem -text -noout

Encrypt and decrypt using public and private key

Encrypt using public key

Use the following command on CMD

openssl pkeyutl -encrypt -in plaintext.txt -pubin -inkey publickey.pem -out encryptedtext.txt

Decrypt using private key

Write the following command on CMD

openssl pkeyutl -decrypt -in decrypted.txt -inkey privatekey.pem -out decrypted.txt

Lab 3: Digital signature

Objective

- To create a hashed character or figure print from a memo or text using well known hashing algorithm.
- To digitally sign the figure print and create message digest or digital signature to be sent with the memo or message.
- To decrypt the digital signature or message digest using sender's public key.
- To create figure print from the received memo or message using the same hashing algorithm used by the sender and compare the figure print with the decrypted one.
    - Create private and public key as shown in Laboratory practice 2
    - Create a memo or message which used to create or generate fingerprint or hashed character.
    - You may say the file name plainhash.txt. in side the file you may give the memo "Hi. This is the text to create message digest"
    - Use hash algorithm such as MD5 SHA1 or SHA256 to create figure print from a created memo.

Creating fingerprint

Write the following command on CMD

openssl dgst -hash_algorithm -out filename_to_store_fingurprint input_file_that_has_memo

eg, *openssl dgst -sha1 -out fingurprint1.txt plaindgst.txt*

creating digest (digital signature)

openssl pkeyutl –sign –in fingerprint –inkey privatekey.pem –out signature

write the following command on CMD to verify or decrypt the **encrypted finger print**

openssl pkeyutl -verify -in Fingerprint file -sigfile encrypted_fingerprint_file (signature) -inkey pubkey.pem -pubin

eg. ***openssl pkeyutl -verify -in fingerprint.txt -sigfile signature -inkey pubkey.pem -pubin***

After getting the decrypted signature, make comparison by hashing the memo plaindgst.txt using the same hashing algorithm (sha1).

Lab 4: Create Digital certificate

Objectives

- To create private and public keys of two different organization and one root CA
- To create self-signed digital certificate for root CA
- To analyse how two parties or organizations are requesting for digital certificate.
- To analyse how root CA issues digital certificate for different organizations based on their request.

Create certificate for Root CA- self signed certificate

Create root private key

openssl genrsa -out rootprkey.pem 1024

Create root public key

openssl rsa -in rootprkey.pem -pubout -out rootpkey.pem

Request for certificate

write the following command on CMD to request for root certificate

***openssl req -new -x509 -days 365 -key rootprkey.pem -out rootCA.crt*.** Then press enter.

- Provide country name:
- Provide state or province name:
- Provide locality name or city:
- Provide organization name:
- Provide organization unit name or section (branch):
- Provide common name or name of director:
- Provide email address:
- Finally, you will get root CA certificate

Requesting digital certificate from 3rd party (CA)

Let if there are two organization A and B who needs get digital certificates from root CA, first they should create private and public key and request root CA for certification.

Organization or party A

Private key

openssl genrsa -out Aprkey.pem 1024

Public key

openssl rsa -in Aprkey.pem -pubout -out Apubkey.pem

Request for certification

***openssl req -new -key Aprkey.pem -out Acsr.csr*.** then press enter.

- Provide country name:
- Provide state or province name:
- Provide locality name or city:

- Provide organization name:
- Provide organization unit name or section (branch):
- Provide common name or name of director:
- Provide email address:
- Password:
- An optional company name:

Now the **organization or party A** requested **root CA** for certification

Root CA issue certificate for Party A

Write the following command on CMD

openssl x509 -req -days 365 -in Acsr.csr -CA rootCA.crt -CAkey rootprkey.pem -set_serial 01 -out Acert.crt

Organization or party B

the procedure for party B request and certifications are the same as party A except the name. you may give the following naming for party B.

- private key: **Bprkey.pem**
- public key: **Bpubkey.pem**
- certificate service request: **Bcsr.csr**
- certificate: **Bcert.crt.**