OpenSSL Lab

1. Install openssl on Ubuntu Linux with the following command
   sudo apt install openssl (This will prompt for password)

2. Check the openssl version with the following command:
   openssl version

3. Download the logo.jpg file and check the size and properties of file
   ls -l logo.jpg

4. Encode the logo in base 64 with the following command:
   openssl enc -base64 -in logo.jpg -out logo.enc

5. Decode the logo.enc generated in the previous step and verify that they are the same file
   openssl base64 -d -in logo.enc -out logo_rec.jpg

6. Generate a AES key. You need two consoles for this complete. On one console using the following command

   openssl enc -d -a -md sha256 -aes-256-cbc -nosalt -p

   (This will prompt for a password)

   It will give a Key and IV.

   From another console open a file:

   gedit aes.txt&

   Copy and paste the key and IV into this file and save it.

7. Encrypt logo.jpg with AES key

   openssl enc -nosalt -aes-256-cbc -in logo.jpg -out logo.aes -base64 -K <your generated key here> -iv <your generated IV here>

8. Decrypt the logo.aes file with the following command

    openssl enc -nosalt -aes-256-cbc -d -in logo.aes -out logo_aes.jpg -base64 -K <your generated key here> -iv <your generated IV here>

9. Verify that log.jpg and logo_aes.jpg are the same file

10. Generate a RSA private key with the following command
    openssl genrsa -aes256 -out private.key 8912
    (This will take a while and prompt for a password)

    Verify the private.key file. It should have the following structure:
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: AES-256-CBC

    <Generated Key>

    -----END RSA PRIVATE KEY-----

11. Generate a RSA public key from the private key generated:
    openssl rsa -in private.key -pubout -out public.key

    Verify the public.key. It should have the following structure:
    -----BEGIN PUBLIC KEY-----
    KEY
    -----END PUBLIC KEY-----

12. Create a file sid.txt with the following command:

    gedit sid.txt&

    Put your student ID number in this file and save it

13. Encrypt the sid.txt file using RSA

    openssl rsautl -encrypt -pubin -inkey public.key -in sid.txt -out sid.rsa

14. Decrypt the sid.rsa file using openssl

    openssl rsautl -decrypt -inkey private.key -in sid.rsa -out sid_1.txt

15. Verify sid.txt is same as sid_1.txt

16. Try encrypting logo.jpg using RSA and share your experience

17. Create another RSA key for signature.

    a. Make a change to openssl config file. On the console edit the config file using the following command(this will prompt for a password):
       sudo gedit /etc/ssl/openssl.cnf

       change the line with the following text:
       RANDFILE = $ENV::HOME/.rnd
       To :
       # RANDFILE = $ENV::HOME/.rnd
       Save the file and close gedit
    b. Run the following command(change "my name" to yours):
       openssl req -nodes -x509 -sha256 -newkey rsa:4096 -keyout "$(whoami)s_sig_key.key" -out "$(whoami)s_sig_key.crt" -days 365 -subj "/C=US/ST=Vijay Anand/L=St. Louis/O=UMSL/OU=IST Dept/CN=$(whoami)s Sign Key"
       This will generate 2 files:
       Private Key: <yourname>s_ sig_key.key
       X509 certificate containing your public key: <yourname>s_ sig_key.crt (This is a self-signed certificate)
    c. Verify the contents of the certificate by running the following command:

openssl x509 -in "$(whoami)s_sig_key.crt" -text -noout > x509.txt
Open the x509.txt file and verify:
“Issuer:” is same as “Subject:”
The CA flag is TRUE:
CA:TRUE

18. Generate Signature with the following command:

    openssl dgst -sha256 -sign "$(whoami)s_sig_key.key" -out sign.txt.sha256 logo.jpg

    You can check the content of sign.txt.sha256 by running the following command. It will show some random characters

    cat sign.txt.sha256

19. Verify that the signature belongs to logo.jpg file:

    openssl dgst -sha256 -verify <(openssl x509 -in "$(whoami)s_sig_key.crt" -pubkey -noout) -signature sign.txt.sha256 logo.jpg

    You should see the following output:

    Verified OK

For this labwork submit the following(ZIP all the files):

1. openssl version
2. logo.enc
3. logo_rec.jpg
4. aes.txt
5. logo.aes
6. logo_aes.jpg
7. sid.txt
8. private.key
9. public.key
10. sid_1.txt
11. <yourname>s_ sig_key.key
12. <yourname>s_ sig_key.crt
13. x509.txt
14. sign.txt.sha256
15. Screenshot stating “Verified OK”