JOHN PATRICK S. LA-ANAN CS253 PROJECT

**NOTES:**

Operating System Used: Windows 7

* Added OpenSSL bin folder in the *Path* environment variable

OpenSSL Version: OpenSSL 1.1.0 from (https://www.openssl.org/source/openssl-1.1.0e.tar.gz)

Script running: Used Docker command line (to be able to execute Linux commands) to run the scripts in the *scripts.txt* file

**1. OPENSSL**

**Download and install OpenSSL, if you do not have it yet. https://www.openssl.org**

STEP 1: Install OpenSSL and get its version.



**2. SYMMETRIC ENCRYPTION**

**Study the OpenSSL Library and use it to perform symmetric AES encryption on the 512x512 Color (24-bit) Lena image (http://www.ece.rice.edu/~wakin/images/lena512color.tiff)**

**Use both ECB and CBC mode, for AES-128.**

1. **AES-128 ECB**

STEP 1: Encrypt the file using *enc* with option *aes-128-ecb* to generate *lena512color\_enc.tiff* file. The key used *253021617*.



STEP 2: [1], [2] A TIFF file begins with an 8-byte information about its header. To generate the encrypted image file, the first 8 bytes of the original Lena image file should be extracted and append the last 786,564 bytes of the encrypted file (*lena512color\_enc.tiff*). The 786,564 is the size of the Lena image file (*786,572 bytes*) less the 8 bytes of header information.

Get the header information and save to *lena\_encrypted.tiff*



STEP 3: Get the last 786,564 bytes of the encrypted file and append to *lena\_encrypted.tiff*



1. **AES-128 CBC**

STEP 1: Encrypt the file using *enc* with option *aes-128-cbc* to generate *lena512color\_enc.tiff* file. The key used *253021617* and the initialization vector *iv* is *716120352*.



STEP 2: [1], [2] A TIFF file begins with an 8-byte information about its header. To generate the encrypted image file, the first 8 bytes of the original Lena image file should be extracted and append the last 786,564 bytes of the encrypted file (*lena512color\_enc.tiff*). The 786,564 is the size of the Lena image file (*786,572 bytes*) less the 8 bytes of header information.

Get the header information and save to *lena\_encrypted.tiff*



STEP 3: Get the last 786,564 bytes of the encrypted file and append to *lena\_encrypted.tiff*



**3. HASHING**

**Using OpenSSL, hash the same Lena 512x512 image using the following hash functions: SHA-1, SHA-256, SHA-512. Again, fully document the process and the results of the hash.**

1. **SHA-1**

STEP 1: Generate hash and then output to sha1.pem.



sha1.pem file contains the hash:



1. **SHA-256**

STEP 1: Generate hash and then output to sha256.pem.



sha256.pem file contains the hash:

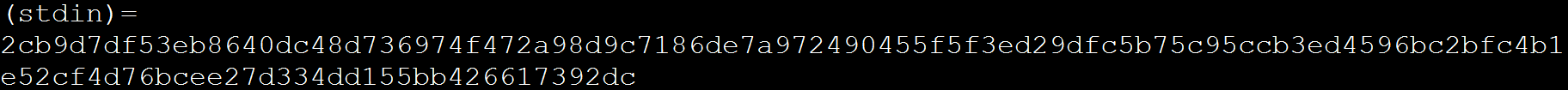


1. **SHA-512**

STEP 1: Generate hash and then output to sha512.pem.



sha512.pem file contains the hash:



**4. PUBLIC KEY ENCRYPTION**

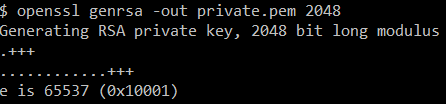
1. **Using OpenSSL, perform an RSA encryption on the Lena 512x512 image, using RSA-2048**

To perform RSA encryption, *rsautl* is used. However, it cannot be used for large files. The following error is displayed:



To do the RSA encryption for large files, the key first will be encrypted using *rsautl* and then encrypt the file using AES.

STEP 1: Generate the private key keys using *genrsa*.



STEP 2: Generate the public key using the generated private key.



STEP 3: Generate a 256-bit random key



STEP 4: Encrypt the 256-bit key using the public key.



STEP 5: Encrypt the Lena image file using AES 256 CBC.



**DECRYPTION:**

STEP 1: Decrypt the key using *rsautl*.



STEP 2: Decrypt file using the decrypted key



1. **Using OpenSSL, generate an ECDSA signature on the same Lena image. If you need to use a hash function, use SHA-256**

STEP 1: Generate a random key using *ecparam* to be the private key. The curve used is *secp256k1*, SECG curve over a 256-bit prime field. (*openssl ecparam –list\_curves*).



STEP 2: Generate the public key using the private key generated in Step 1



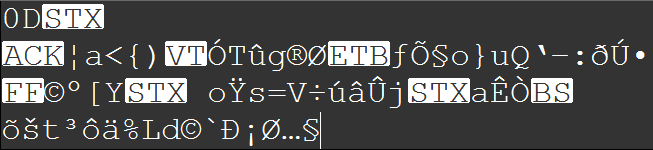
STEP 3: Sign the Lena image file using the generated private and public key.



It will generate the file lena.der



Containing the following file (view using Notepad++)



**REFERENCES:**

[1] https://tools.ietf.org/html/rfc2306 (Last accessed May 22, 2017)

[2] http://paulbourke.net/dataformats/tiff/ (Last accessed May 22, 2017)