Programming Assignment 3
CS 478/513 Computer Security, due 4/18, before class

This project is divided into some smaller related sub-projects for your convenience. Please keep in mind that without completing the previous parts, you can not work on the rest of the project since they are highly related.

Project Overview

The basic idea of this project is getting to know digital certificates and RSA in real world implementations. You need to start with a digital certificate, downloaded from a certificate authority, which provides you the public/private key set. Then you have to use these keys for asymmetric key cryptography algorithm, RSA. In the end, you need to use the session key for symmetric key cryptography such as AES or Triple-DES. Throughout this project you need to read more about the C++ OpenSSL cryptographic library and use the built in functions and structures.

First Deliverable

You need to create an account in CAcert website. After that, you need to generate a digital certificate for yourself and store the generated certificate (if there are problems with this, you can also create an openssl certificate).
Having the certificate, you need to use OpenSSL library to extract your public key from the certificate and store it in "pem" format as pubkey.pem. For the private key, you have to download the PKCS12 format of your certificate from your browser and convert it to a readable format. After this conversion, you should be able to open the certificate in text editor and extract the private key. Store your private key in another file as privkey.pem. For using OpenSSL, you have to install the library on your machine. All the required documentation for working with OpenSSL is available at its website.

CAcert:https://www.cacert.org/index.php?id=1
OpenSSL:http://www.openssl.org

At the end of this part, you need to submit your pubkey.pem, privekey.pem and a short, half to one page report in pdf format in which you explain how did you extract these keys using OpenSSL library. Put your files and code in a file called “yourname-part1.tar”.

Second Deliverable

In the second part of this project, you need to use your public and private keys, extracted from your digital certificate in the first part to perform RSA cryptography. Hence, we provide a third party public key, named as pubkey.pem, and a message encrypted with the third party private key. You need to write a program that can perform the following steps:

1. Takes the encrypted message, the third party public key and your private key as the command line parameters in the mentioned order.

2. The program then, should use the third party public key to decrypt the encrypted message and store the message in a text file as symmetric.txt . This would be your symmetric key.

3. Then, it needs to use the decrypted message as a symmetric key to encrypt a text file with one of the symmetric key cryptography algorithms (AES, DES or 3DES; this would be a good place to use the DES algorithm you implemented in Prog. Assign 2) You either can write the code for this part or use the openssl command with system function. In the text file, you should mention your name and your banner ID. You also should explain which symmetric key algorithm you used in addition to the project evaluation.

4. After that, you have to sign the file content, already encrypted in step 3, with your private key, and store the result in a file.

You need to name your program as the project2_encryption.cpp.
Then, you should write the second program which does the decryption. The second program should work as follow:

1. Takes the file that is generated in the last step of previous program, the appropriate public key, for signature verification, and the symmetric key file, symmetric.txt, in the mentioned order.

2. Verify the signed file with the public key.

3. After this verification, it needs to do the final decryption step by using the content of symmetric.txt file and return the text file, containing your information and evaluation, in plaintext. Again, you can write the code for this part or you can use the openssl command with system function.

Name this file as project2_decryption.cpp.
For submission, you need to submit all the following items in one tar folder called "yourname-progassign3.tar" (you can use $tar - cvf foldername.tar foldername$)

- Output of part 1 ("yourname-part1.tar").
- Both programs
- The provided third party public key, publickey.pem
- The symmetric key file which you named it as symmetric.txt

- Your pub.pem and priv.pem keys that you get in first part of the project and used it here.
- The encrypted file which you encrypt it in step 4 of the first program (This would be one of the input file for second program).
- You also have to provide a readme file which explain the compilation and running command with necessary information. If you do not submit readme file or we can not compile and run your programs with provided command, you will get zero for this project.

Please follow the instruction for each step, follow the naming scheme that is given.
Remember that your programs should take three command line parameters explained in step 1 of each program.
Provide meaningful prompt for the user.
You will lose some point for missing any of the aforementioned items.