Network Security

Project 1.3

Encrypted Socket Programming

Instructor: Shiuhpyng Shieh

TA：E-Lin Ho, Jui-Chien Jao

1. Project Description

In this project, you need to implement a socket program to communicate with the server at **140.113.194.88:45000** through a secure channel using both RSA cryptosystem and AES in CBC mode encryption.

The communication protocol, illustrated in Fig. 1, shall be implemented in your client socket program.

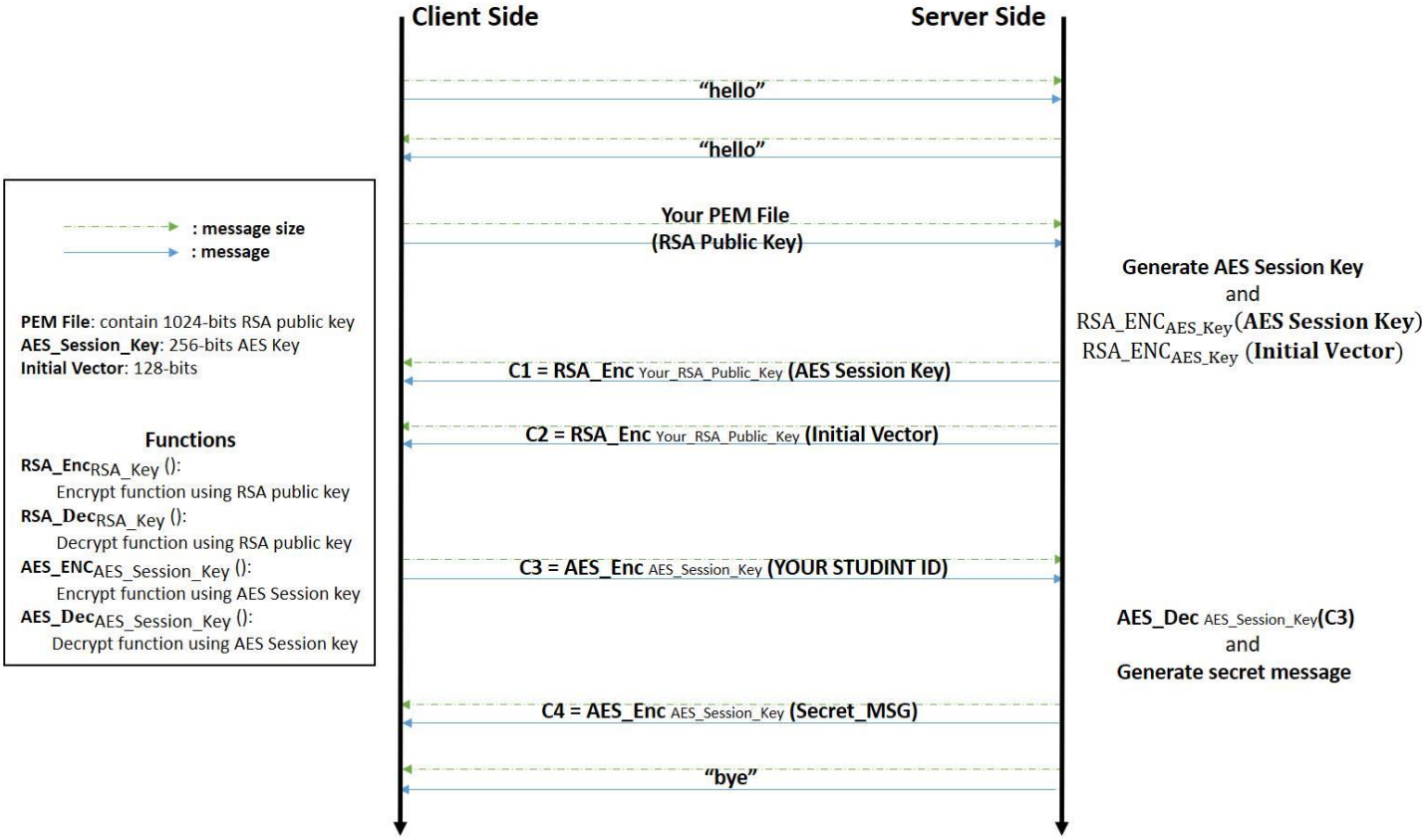

Fig. 1 The protocol of Encrypted Socket Programming.

As shown in Fig. 1, every message content should be sent after the total number of bytes of it. A "hello" message sent from the client starts a new conversation. After the server sends a "hello" message back to the client, the communication protocol is defined as follows: Firstly, the client sends RSA public key in PEM file format to

the server. The key can further encrypt and decrypt messages, thus securely sending messages. Secondly, the server encrypts both **AES Session Key** and **Initial Vector of CBC mode encryption** by **client's RSA public key**, and delivers them to the client respectively.

Next, the client uses AES Session Key and Initial Vector to do AES encryption on your student ID, and sends the encrypted data to the server. Finally, the server decrypts the message, produces a corresponding magic number, encrypts the magic number by the same AES session key and delivers it to the client. The magic number is uniquely generated from the student ID, so the result of every student are different from each other.

The magic number will be in the form of ***XXXXX***, surrounded by three preceding and three succeeding '*'. The last "bye" message in plaintext terminates the conversation.

Reminder:

- **For the implementation of RSA and AES cryptosystem, the use of the OpenSSL library supporting C/C++ and Java is recommended.**
- **Padding Method of RSA cryptosystem is EME-OAEP defined in PKCS #1 v2.0 with SHA-1, MGF1 and an empty encoding parameter.**
- **AES-256 is used in this project and the initial vector of CBC mode is 128-bit.**

2. Deliverables

Each student must work individually and submit a .zip file, named by "<YOUR_STUDENT_ID>.zip" containing:

a) The source code of your socket program.

b) A report includes:

- The magic number you receive from the server.
- The instructions for compiling your source code.

3. Reference

Openssl: https://www.openssl.org/

Any anomaly connection such DDoS will be traced for penalty.

Deadline : 2016/10/30 (Sun.) 23:59:59