INFA723 Homework 4

The homework assignment will be graded based on the following criteria:

- Accuracy: 1) the solution meets specific requirements in the problem description; 2) the solution produces correct results; 2) the procedures adopted in the solution are technically sound.
- Efficiency: efficiency will be one of the criteria when grading programing assignment. The solution should produce the desired results efficiently.
- Effort/neatness: the solution includes excellent effort, and all relate work is shown neatly and organized well.

Homework assignment feedback will be available through the DropBox folder on D2L.

1. This homework includes 2 labs listed as below:

   (20 points) Lab 9 Use OpenSSL to Generate a Self-Signed Certificate

   (30 points) Lab 10 Use OpenSSL to Set up a Simple SSL/TLS Server and Test a Remote Host Using SSL/TLS

The steps in each lab are documented for your learning purpose. You don't need to make screenshots for those steps.

There is a question section in the end of each lab. Please answer all the questions in each lab. The required data files for the labs have been enclosed in the labs9-10.zip file. Copy the data files to you OpenSSL testing environment to complete the labs.

Please create a single document to include all your answers and submit your work through D2L.

2. (15 points) Figure 1 shows a diagram of how to retrieve public keys using a public key authority. In steps 3, 6, and 7, two nonce N_1, N_2 are used. Explain why N_1, N_2 are used in the protocol and what security service can be ensured by using N_1, and N_2 in the protocol.
   (Hints: think about non-repudiation service in OSI model)

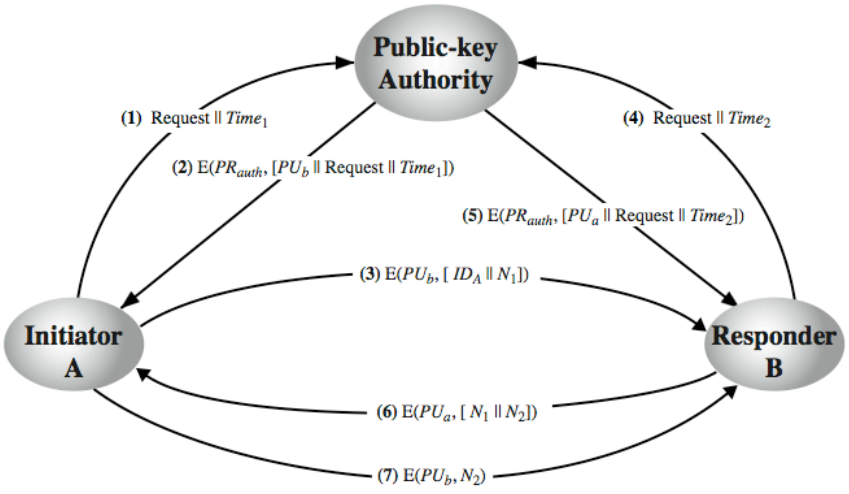

Figure 1 Retrieve Public Keys using a Public-key Authority

3. (15 points) Users A and B uses the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7.
    a. (5 points) If user A has private key $X_A = 5$, what is A's public key Y_A ?
    b. (5 points) If user B has private key $X_B = 12$, what is B's public key Y_B ?
    c. (5 points) What is the shared secret key?

    (Hints: refer to text book Figure 10.1 in Page 303)

4. (10 pints) Consider a one-way authentication technique based on asymmetric encryption:
    1. A->B: ID_A
    2. B->A: $E(PU_a , R_2)$
    3. A->B: R_2

    a) Explain the protocol;
    b) What type of attack is this protocol susceptible to?

5. (10 points) Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.
    a. SSLsplit is a tool for man-in-the-middle attacks against SSL/TLS encrypted network connections. Connections are transparently intercepted through a network address translation engine and redirected to SSLsplit. SSLsplit terminates SSL/TLS and initiates a new SSL/TLS connection to the original destination address, while logging all data transmitted.
    b. A downgrade attack is a form of cyber attack in which an attacker forces a network channel to switch to an unprotected or less secure data transmission standard. Downgrading the protocol version is one element of man-in-the-middle type attacks,

and is used to intercept encrypted traffic. An example of a downgrade attack might be redirecting a visitor from an HTTPS version of a resource to an HTTP copy.