Track B
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. (60 points) Tcpcrypt is a TCP extension designed to make end-to-end encryption of TCP traffic the default, not the exception. To facilitate adoption tcpcrypt provides backwards compatibility with legacy TCP stacks and middle boxes. The paper, "The case for ubiquitous transport-level encryption", is available for you to go through all the details. You can also go to http://tcpcrypt.org/ and find more information about Tcpcrypt. Read the paper and answer the following questions:
    a. (20 points) Tcpcrypt is a transport layer security protocol. As we discussed in the class, TLS is also a transport layer security protocol. Compare the differences between Tcpcrypt and TLS protocol (list at list three differences)
    b. (20 points) What is the design consideration of Tcpcrypt protocol? Why is it necessary?
    c. (20 points) Tcpcrypt was originally proposed in 2010. What are the major challenges to adopt Tcpcrypt?

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)

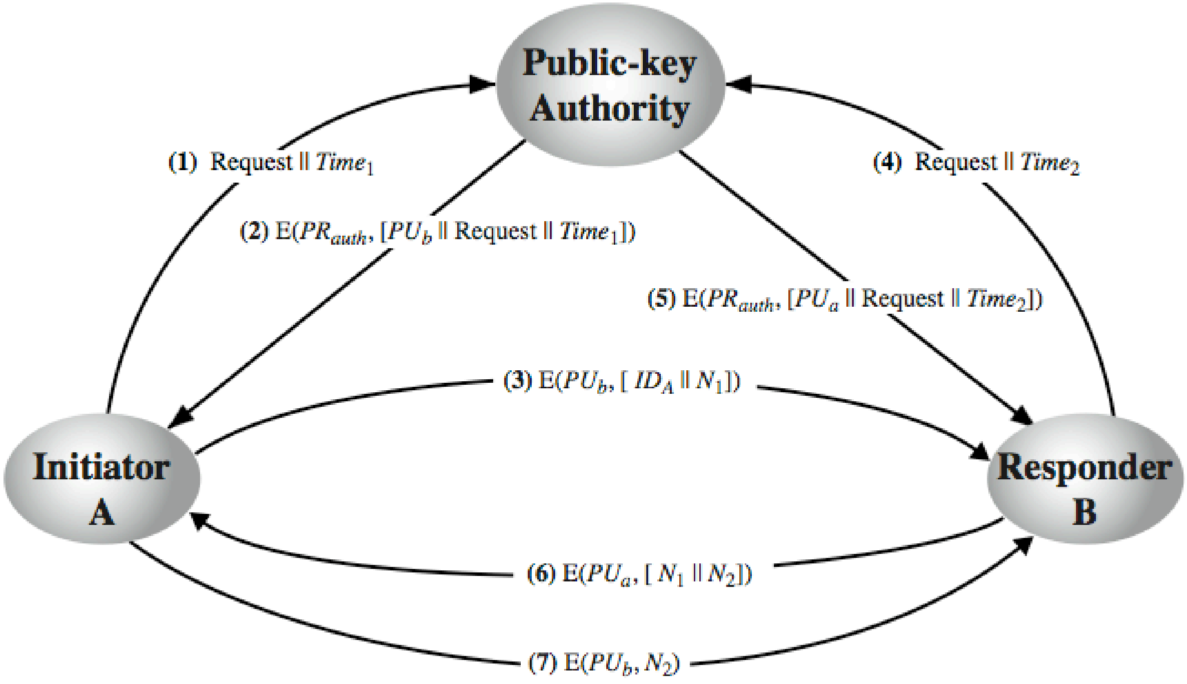
Public-key Authority
(1) Request || $Time_1$
(2) $E(PR_{auth}, [PU_b \| Request \| Time_1])$
(4) Request || $Time_2$
(5) $E(PR_{auth}, [PU_a \| Request \| Time_2])$
(3) $E(PU_b, [ID_A \| N_1])$
Initiator A
Responder B
(6) $E(PU_a, [N_1 \| N_2])$
(7) $E(PU_b, N_2)$

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?