Cairo
University

Faculty of Computers
and Information

Network Security
CS 495

2nd Term 2008-2009
Assignment #1

Assignment #1 (2 points)

Due on: Mar. 23
Please submit on FCI Moodle

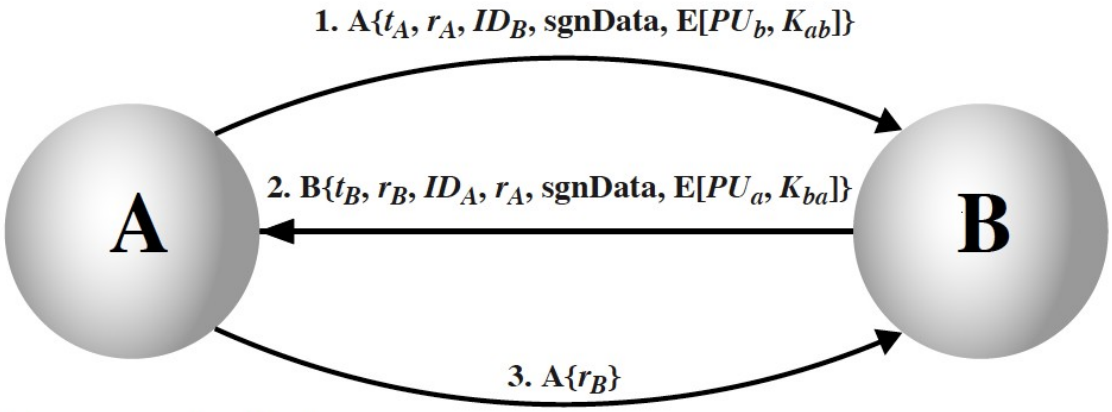
Question 1 [1 pt.]. Student Tahseen decides to implement an online game server, so that he can play friendly games with his friends across campus. The game works as follows: the server assigns five numbers selected at random from between 0 and 100 to each player. The numbers are known to their owner but must remain secret to the other players.

Then, each player makes three guesses of the numbers assigned to the other players and sends his guesses to the server. Finally, the server broadcasts each player's cards, and the player who has made the most correct guesses wins. The process is then repeated until Tahseen and his friends get tired of playing.

For security, Tahseen decides to use some encryption. Player *i* keeps a long-lived secret key K_i, which the server also knows. The server sends each of the five numbers of player *i* encrypted with K_i. When the numbers are broadcast at the end of each round, the server sends them in the clear to all players.

(a) Explain one attack that can be executed by a passive malicious player who is able to eavesdrop on the network. (*Hint: think of building some sort of a database*)
(b) Suggest a fix to this problem.

Question 2 [1 pt.]. The original three-way authentication procedure for X.509 illustrated in the following figure contains a security flaw.


1. $A\{t_A, r_A, ID_B$, sgnData, $E[PU_b, K_{ab}]\}$
2. $B\{t_B, r_B, ID_A, r_A$, sgnData, $E[PU_a, K_{ba}]\}$
A
B
3. $A\{r_B\}$

(c) Three-way authentication

The essence of the protocol is as follows:

A -> B:	$A\{t_A, r_A, ID_B\}$
B -> A:	$B\{t_B, r_B, ID_A, r_A\}$
A -> B:	$A\{r_B\}$

The text of X.509 states that checking timestamps t_A and t_B is optional for three-way authentication. But consider the following example: Suppose A and B have used the preceding protocol on some previous occasion, and that opponent C has intercepted the preceding three messages. In addition, suppose that timestamps are not used and are all set to 0. Finally, suppose C wishes to impersonate A to B. C initially sends the first captured message to B:

C -> B:	$A\{0, r_A, ID_B\}$

B responds, thinking it is talking to A but is actually talking to C:

B -> C: $\mathrm{B}\{0, r'_B, ID_A, r_A\}$

C meanwhile causes A to initiate authentication with C by some means. As a result, A sends C the following:

A -> C: $\mathrm{A}\{0, r'_A, ID_C\}$

C responds to A using the same nonce provided to C by B.

C -> A: $\mathrm{C}\{0,r'_B, ID_A, r'_A\}$

A responds with

A -> C: $\mathrm{A}\{r'_B\}$

This is exactly what C needs to convince B that it is talking to A, so C now repeats the incoming message back out to B.

C -> B: $\mathrm{A}\{r'_B\}$

So B will believe it is talking to A whereas it is actually talking to C. Suggest a simple solution to this problem that does not involve the use of timestamps and describe why your fix prevents the impersonation attack described above.