CSS322 – Quiz 3

Name: ______________________ ID: ______________ Marks: _____ (10)

Question 1 [2 marks]

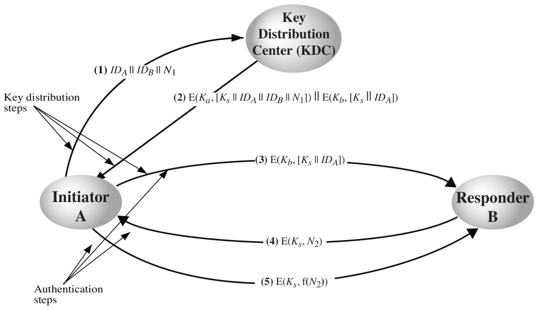
You are designing a database to store user details. You have the following information available:

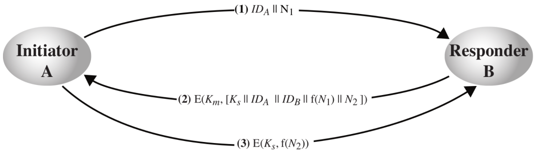
- Username, u
- Users selected password, p
- Salt, s
- Secret key known by you (the database admin), k
- Symmetric encryption function, E()
- Hash function, H()

List the best set of data to be stored in the database. Use equations/operations where appropriate.

Question 2 [2 marks]

Consider the two schemes below:


Key Distribution Center (KDC)
(1) $ID_A \| ID_B \| N_1$
Key distribution steps
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$
(3) $E(K_b, [K_s \| ID_A])$
Initiator A
Responder B
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps



If there were 40 users in the system and the scheme on the right was used, then how many master keys must be manually exchanged?

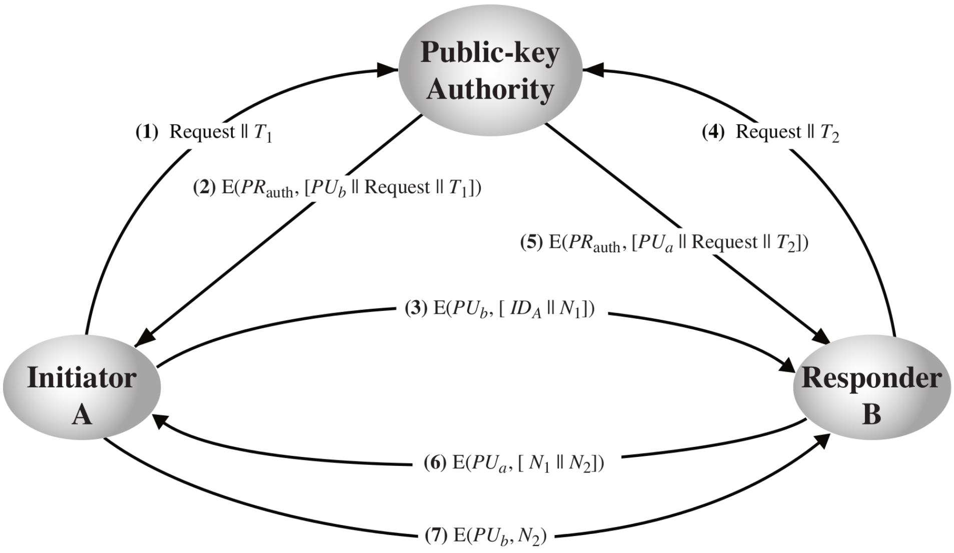
Question 3 [2 marks]

You develop a web site that requires a user to choose a password. The password scheme is: character set a–z, A–Z, password length 5. Complete the equation to give the entropy, E, of the scheme (you don't have to calculate the final answer):

E = ____________________

Question 4 [4 marks]

Consider the scheme in the figure below.


Public-key Authority
Initiator A
Responder B
(1) Request ‖ T_1
(2) E(PR_{auth}, [PU_b ‖ Request ‖ T_1])
(4) Request ‖ T_2
(5) E(PR_{auth}, [PU_a ‖ Request ‖ T_2])
(3) E(PU_b, [ID_A ‖ N_1])
(6) E(PU_a, [N_1 ‖ N_2])
(7) E(PU_b, N_2)

(a) List all keys assumed to be known by the authority before the scheme starts (i.e. before message (1) is sent).

(b) List all keys known by A after the scheme is finished (i.e. after message (7) is sent).