

# CSS322 – Quiz 3

Name: \_\_\_\_\_ ID: \_\_\_\_\_ Marks: \_\_\_\_\_ (10)

## Question 1 [2 marks]

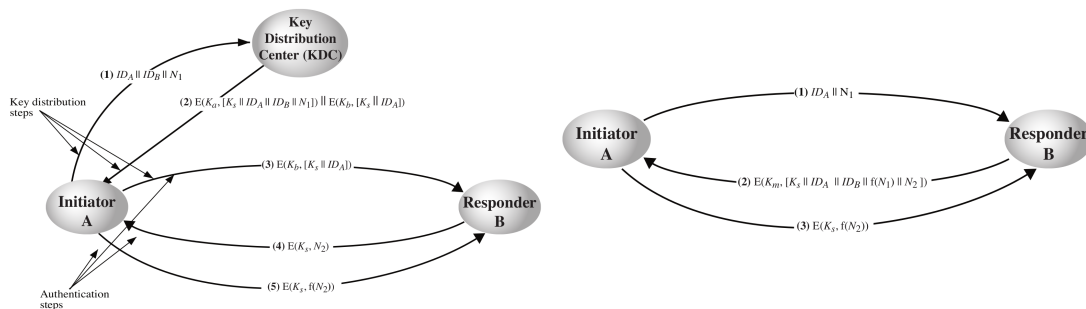
You are designing a database to store user details. You have the following information available:

- 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:



If there were 100 users in the system and the scheme on the left was used, then how many master keys must be manually exchanged?

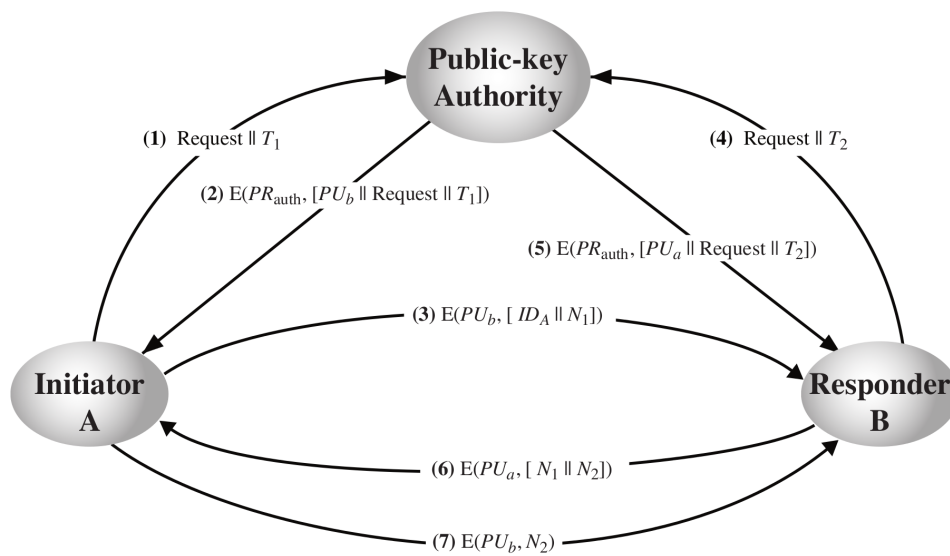
**Question 3** [2 marks]

You develop a web site that requires a user to choose a password. The password scheme is: character set a–z, 0–9, password length 9. Complete the equation to give the entropy,  $E$ , of the scheme (you don't have to calculate the final answer):

$E = \underline{\hspace{4cm}}$

**Question 4** [4 marks]

Consider the scheme in the figure below.



(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 B after the scheme is finished (i.e. after message (7) is sent).