CSS322 – Quiz 3

Security and Cryptography, Semester 2, 2011

Prepared by Steven Gordon on 26 March 2012
CSS322Y11S2Q03, Steve/Courses/2011/S2/CSS322/Assessment/Quiz3.tex, r2236

Question 1 [2 marks]

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

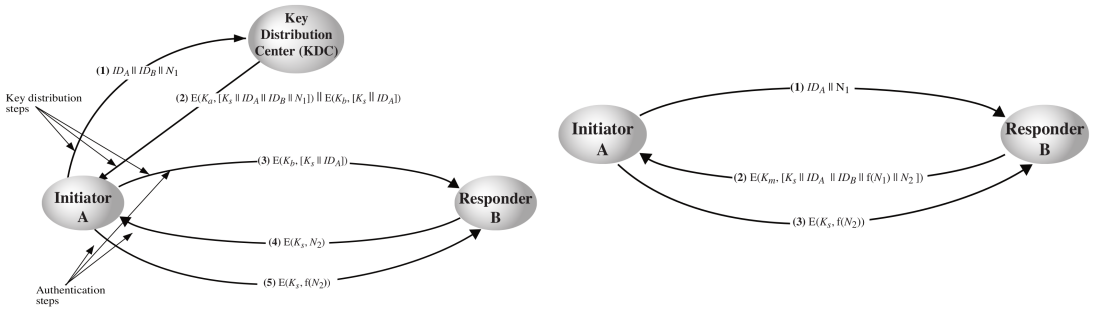
- Username, u
- Users selected password, p
- Salt, s
- Secret key known by you (the database admin), k
- Symmetric encryption function, E()
- Hash function, H()

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

Answer. *You must store the username. Rather than storing the password, the password should be combined with a random salt and hash of the two is stored. The user supplies their username and password. To check if it is correct, the system must know the salt and hence the salt should also be stored in the database. Therefore you should store:* $(u, s, H(p||s))$.

Question 2 [2 marks]

Consider the two schemes below:



If there were [100 | 100 | 40 | 40] users in the system and the scheme on the [right | left | left | right] was used, then how many master keys must be manually exchanged?

Answer. *With the scheme on the left (centralised distribution using the KDC), each user must manually exchange master keys with the KDC. With n users there are n keys exchanged. With the scheme on the right (decentralised distribution), each pair of users must manually exchange a master key. With n users there are $n(n-1)/2$ users and therefore $n(n-1)/2$ keys exchanged.*

- *Centralised (left), 100 users: 100 keys*
- *Centralised (left), 40 users: 40 keys*
- *Decentralised (right), 100 users: 4950 keys*
- *Decentralised (right), 40 users: 780 keys*

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 | a–z, 0–9 | a–z, A–Z, 0–9 | a–z, A–Z], password length [7 | 9 | 6 | 5]. Complete the equation to give the entropy, E, of the scheme (you don't have to calculate the final answer):

E = _____

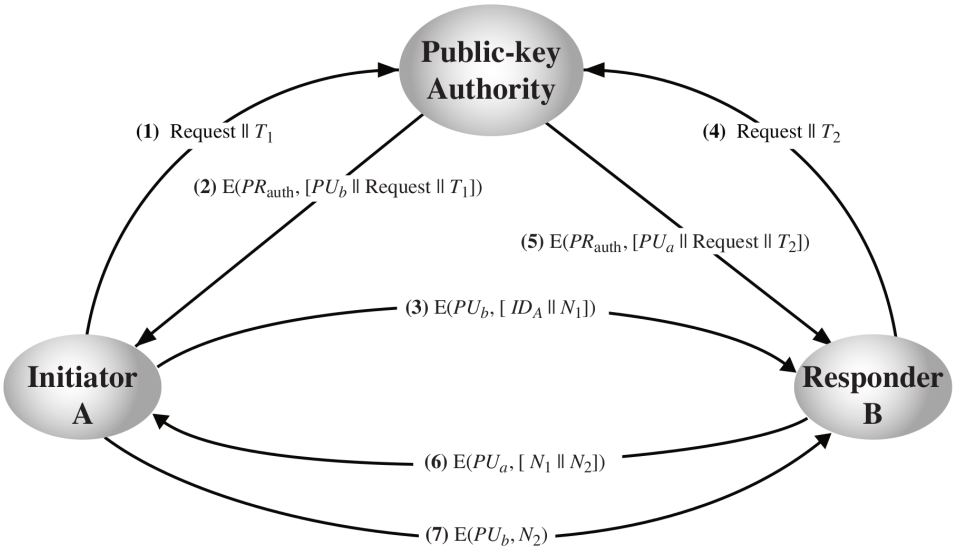
Answer. *The entropy is the number of bits needed to represent all possible passwords allowed by the scheme. With c characters in the set and a password of length n, there are c^n possible passwords. Therefore there are $E = log_2(c^n)$ bits needed.*

- *a–z, 0–9; : $E = log_2(36^7)$*
- *a–z, 0–9; : $E = log_2(36^9)$*
- *a–z, A–Z, 0–9; : $E = log_2(62^6)$*
- *a–z, A–Z : $E = log_2(52^5)$*

Question 4 [4 marks]

Consider the scheme in the figure below.

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



Answer. *Each user should know its own Public/Private key pair, and the Public key of the authority. The authority knows its own Public/Private key pair and the Public keys of the users:*

- *A:* PU_a, PR_a, PU_{auth}
- *B:* PU_b, PR_b, PU_{auth}
- *Authority:* $PU_{auth}, PR_{auth}, PU_a, PU_b$

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

Answer. *Each user learns the Public key of the other user. The authority does not learn any new keys.*

- *A:* $PU_a, PR_a, PU_{auth}, PU_b$
- *B:* $PU_b, PR_b, PU_{auth}, PU_a$
- *Authority:* $PU_{auth}, PR_{auth}, PU_a, PU_b$