COMP90043: Cryptography and security

Week 9: Workshop-9

Part1: Symmetric Key Key distribution

Q1 This is a variation of the protocol discussed in the class symmetric key description involving n users and a KDC. Here every user decides to generate random number themselves for the communication they seek to start.

The steps are as follows:

1. A generates a random number R and sends to the KDC his name A, destination B, and E(Ka, R).

2. KDC responds by sending E(Kb, R) to A.

3. A sends E(R, M) together with E(Kb, R) to B.

4. B knows Kb, thus decrypts E(Kb, R), to get R and will subsequently use R to decrypt

E(R, M) to get M.

Is this secure?

PS: Assume all other assumptions made in the protocol. All users share a master key with KDC, all communications can be observed by the users.

Q2.

Consider the following protocol, designed to let A and B decide on a fresh, shared session key K=AB. We assume that they already share a long-term key K_{AB}.

1. A → B: A, N_A.

2. B → A:E(K_{AB}, [N_A, K'_{AB}])

3. A → B:E(K'_{AB}, N_A)

a. We first try to understand the protocol designer's reasoning:

— Why would A and B believe after the protocol ran that they share K'_{AB} with the

other party?

—Why would they believe that this shared key K'_{AB} is fresh?

In both cases, you should explain both the reasons of both A and B, so your answer should complete the sentences

A believes that she shares K'_{AB} with B since…

B believes that he shares K'_{AB} with A since…

A believes that K'_{AB} is fresh since…

B believes that K'_{AB} is fresh since…

b. Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that she has only been communicating with C). Thus, in particular, the belief in (a) is false.

c. Propose a modification of the protocol that prevents this attack.

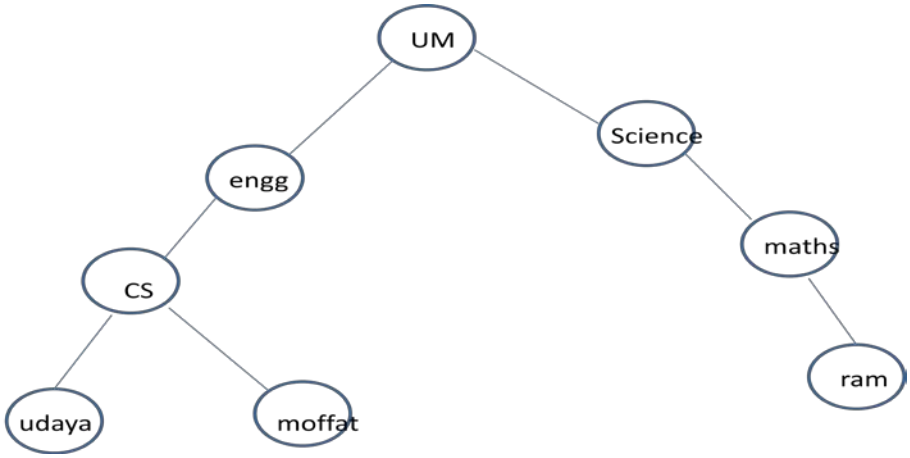
Part2: Public Key Distribution

Q4 .Discuss four methods which are used to distribute public keys?

Q5. What are the essential ingredients of a public-key directory?

Q6. What is a chain of certificates? What are forward and reverse certificates?

Q7 For the following hierarchy, what is the chain of certificates that user "moffat" needs to obtain in order to establish a certificate path to "ram"? You can use X.509 conventions for the certificate chain discussed in the book, for example the certificate for "moffat" by CA "CS" is represented as CS<<moffat>>.



Forward Certificates: Certificates of X generated by other CAs.

Reverse Certificates: Certificates generated by X that are the certificates of other CAs.

Q8. How a X.509 certificate is revoked?

Q9. Find at least one intermediate certification authority's certificate and one trusted root certification authority's certificate on your computer (e.g. in the browser). Print screenshots of both the general and details tab for each certificate.

Homework Questions:

1. What are the core components of a PKI? Briefly describe each component.

2. Explain the problems with key management and how it affects symmetric cryptography.