COMP90043: Cryptography and security

Workshop-9-Part A Solution

Q1.Discuss four methods which are used to distribute public keys?

Public announcement.

Publicly available directory.

Public-key authority.

Public-key certificates

Q2. What the essential ingredients of a public-key directory?

1. The authority maintains a directory with a {name, public key} entry for each participant.

2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.

3. A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way.

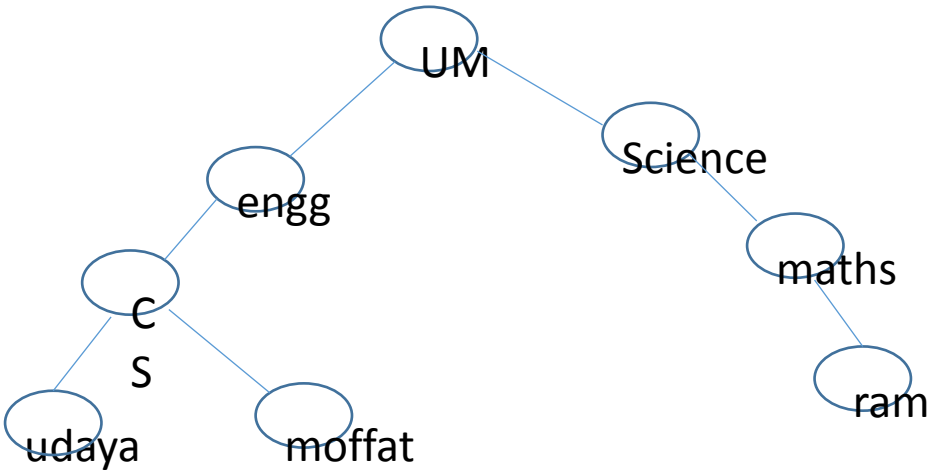
4. Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper.

5. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

Q3. What is a chain of certificates? What are forward and reverse certificates?

A chain of certificates consists of a sequence of certificates created by different certification authorities (CAs) in which each successive certificate is a certificate by one CA that certifies the public key of the next CA in the chain.

Q4 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>>.



CS<<engg>> engg <<UM>>UM<<Science>>Science<<maths>> maths<<ram>>

Maths<<Science>>Science<<UM>> UM<<engg>>engg<<cs>>cs<<moffat>

Forward Certificates: Certificates of X generated by other CAs.

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