COMP90043: Cryptography and security

Week 9: Workshop-10

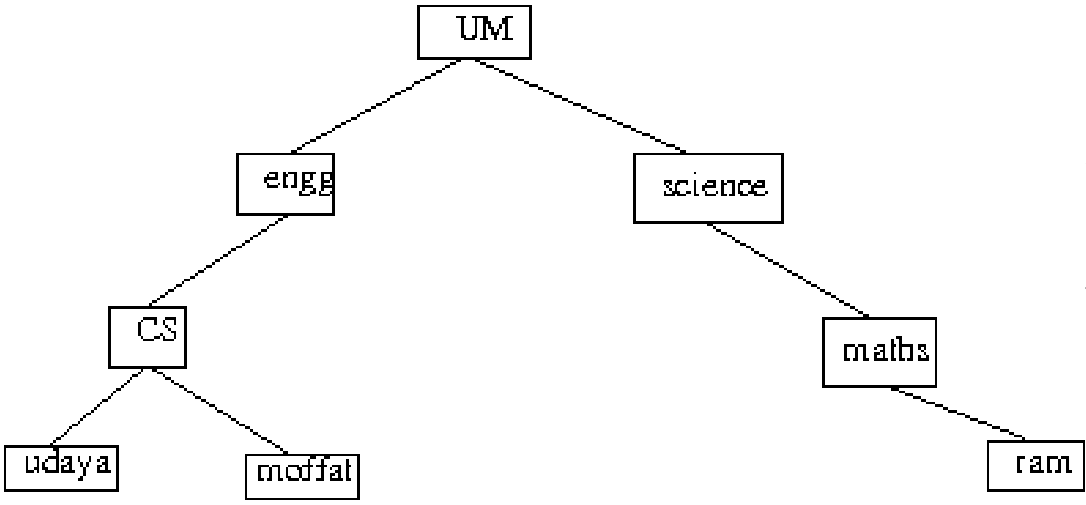
Public Key Distribution

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

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

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

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>>.



Forward Certificates: Certificates of X generated by other CAs.

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

Q5. How a X.509 certificate is revoked?

Q6. Explain how certificates can be used to protect against MITM attacks.

Q7. 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.