# COMP90043 Cryptography and Security
# Semester 2, 2020, Workshop Week 9 Solutions

## Key Management and Distribution

1. Discuss four methods which are used in distributing public keys.

   Public announcement
   Publicly available directory
   Public-key authority
   Public-key certificates

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

   (a) The authority maintains a directory with a name, public key entry for each participant.

   (b) 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.

   (c) 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.

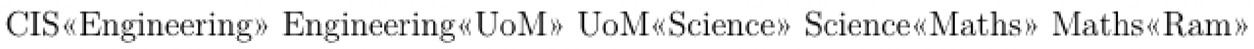
   (d) Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper.

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

3. 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.
   Forward Certificates: Certificates of X generated by other CAs.
   Reverse Certificates: Certificates generated by X that are the certificates of other CAs.

4. Consider the following



CIS«Engineering» Engineering«UoM» UoM«Science» Science«Maths» Maths«Ram»

## Key Management and Distribution

-

If a message must be broken up into blocks and sent as a sequence of encrypted blocks, a unique value of $k$ should be used for each block. If $k$ is used for more than one block, knowledge of one block $M_1$ of the message enables the user to compute other blocks as follows. Let

$$C_{1,1} = \alpha^k \bmod q;\ C_{2,1} = KM_1 \bmod q$$
$$C_{1,2} = \alpha^k \bmod q;\ C_{2,2} = KM_2 \bmod q$$

Then,

$$\frac{C_{2,1}}{C_{2,2}} = \frac{KM_1 \bmod q}{KM_2 \bmod q} = \frac{M_1 \bmod q}{M_2 \bmod q}$$

If $M_1$ is known, then $M_2$ is easily computed as

$$M_2 = (C_{2,1})^{-1}\, C_{2,2}\, M_1 \bmod q$$