FIT1047

SUPPLEMENTARY WORKSHEET -02

WEEK 07

1. Explain the symmetric cryptography algorithm, with example.

2. Explain the Asymmetric cryptography algorithm, with example.

3. What is the difference between asymmetric and symmetric encryption?

In asymmetric encryption, it uses a pair of keys - private and public key, while in symmetric encryption, it uses only one key for each pair of users.

Hence, in asymmetric, the total number of keys increases linearly (as only 2 keys are needed for each users). On the other hand, the total number of keys in symmetric increases exponentially (as for every 2 users, there exists one key).

In asymmetric, the recipient's public key is used to encrypt the sender's message and the recipient will use its private key to decrypt the message. While in symmetric, the same key is used for encryption and decryption. Hence, asymmetric is usually known to have higher confidentiality than symmetric encryption.

FIT1047

SUPPLEMENTARY WORKSHEET -02

WEEK 07

4. How many keys are required for secure communication between ***10*** users?

a. Using asymmetric cryptography

For every user there is a:
- public key
- private key

10 users will have total 20 keys (10 for private and 10 for public)

b. Using symmetric cryptography

There is one key for every communication between every two users (as same key is used for encryption and decryption).

If there are 2 users, total key is 1.
If there are 3 users, total keys is 3 (each pair of users would need 1)

Hence, the total keys can be found with combination, nC2.

10 users means 10C2.

Total keys would be 90 / 2 = 45 keys

[Prepared by Haidar Al-Khalidi]