Tutorial Session 3

1. Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme?
2. Using the two keys (memory words) cryptographic and network security, encrypt the following message: Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends. Decrypt the cipher text and Comment on when it would be appropriate to use this technique and what its advantages are.
3. List three approaches to message authentication.
4. How can public-key encryption be used to distribute a secret key?
5. Alice wants to send a secure message to Bob using RSA encryption. They have agreed on the public key (e, n), where e = 5 and n = 77. Bob's private key (d) is 29.
    i. Calculate the ciphertext (C) when Alice encrypts her message M using Bob's public key (e, n).
    ii. Now, Bob receives the ciphertext (C) and decrypts it using his private key (d). Calculate the original message (M) sent by Alice.