Tutorial 2

Questions

- What is the difference between the public and private keys?

- If 20 people want to communicate using conventional encryption, how many keys are needed? And if they want to use public-key encryption, how many keys are needed?

- Briefly describe the *Diffie-Hellman* key exchange.

- User A and B use the *Diffie-Hellman* key exchange technique with a common prime q = 31 and a primitive root α = 3
- If user A has private key XA = 4, what is A's public key YA?
- If user B has private key XB = 2, what is B's public key YB?
- What is the shared secret key B?

- List the principal elements of a public-key encryption. Briefly explain each of them.

- What are three broad categories of applications of public-key cryptosystems?

- What is the RSA? What are its uses?

- Define Message Authentication Code

- What is a cryptographic hash function?

- What is the difference between a message authentication code and a hash function?

- What changes are required to replace an underlying hash function in HMAC?

- What security services are provided by Digital Signature?

- Perform Encryption and decryption using the RSA algorithm for the following:

p = 3, q = 11, e = 7, M = 5

p = 5, q = 11, e = 3, M = 9

p = 7, q = 11, e = 17, M = 8

Calculate d and ciphertext C

- In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35.What is the plaintext M?