FIT3031-Tutorial 3

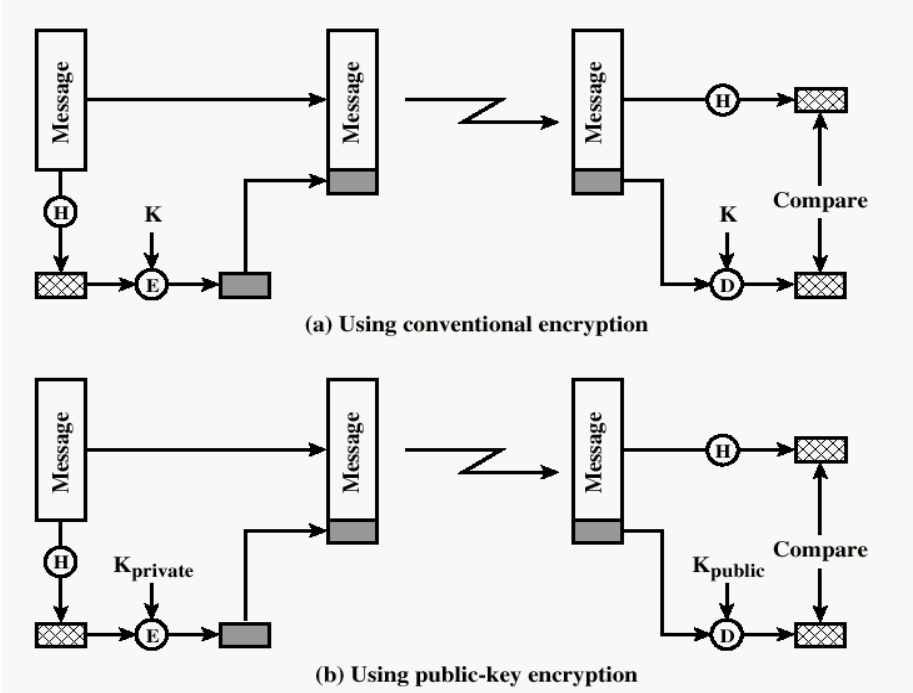
ASYMMETRIC ENCRYPTION

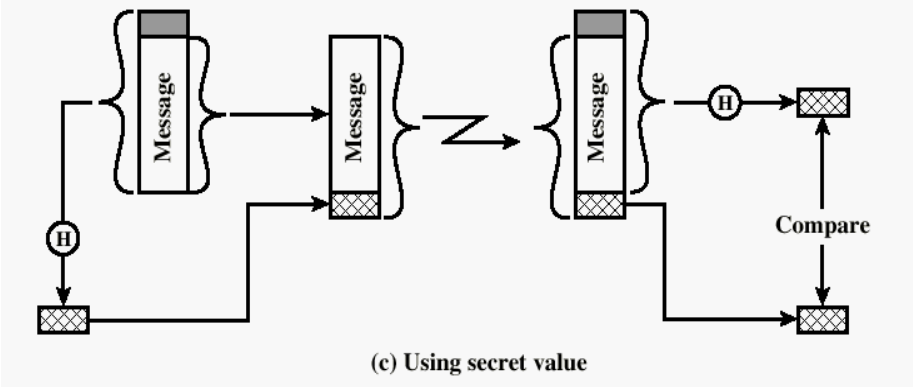
Review

Q1 What is message authentication? List three approaches to message authentication.

Q2 What is a message authentication code?

Q3 Briefly describe the three schemes illustrated in the Figures below.





Q4 What properties must a hash function have to be useful for message authentication?

Q5 What are the principle components of a public key cryptosystem?

Q6 List and briefly define three uses of a public key cryptosystem.

Q7 What is the difference between a private key and a secret key?

Q8 What are a digital signature and a digital certificate?

Q9 What is a public key certificate?

Q10 How can public key encryption be used to distribute a secret key?

Problems:

Modular Arithmetic Applications

Q1 Find the integers x such that

a. $5x \equiv 4 (\mathrm{mod}\, 3)$
b. $7x \equiv 6 (\mathrm{mod}\, 5)$
c. $9x \equiv 8 (\mathrm{mod}\, 7)$

Q2 Perform encryption and decryption using the RSA algorithm as in Figure 3.9 (of the text book) for the following;

a. p=3; q=11; e = 7; M = 5;
b. p =5; q = 11; e = 3; M = 9;

Hint: Decryption is not as hard as you think;

Q3 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?

Q4 Consider a Diffie-Hellman scheme with a common prime q = 17 and a primitive root α = 3.

a. If user A has private key X_A=4, what is A's public key, Y_A? (*Hint: 17x5=68*)
b. A sends Y_A to B. If B has a private key X_B=6, what is the shared secret key, K that B can calculate and share with A? (*Hint:17*6=102; 17*9=153; 15*17=255;*)

c. If B computes Y_B and sends it to A,, what is the shared secret Key, K computed by A? (*Hint: 13*17=221)*

Other Problems:

Q5 Suppose Bob uses RSA cryptosystem with a very large modulus, *n* for which the factorisaton cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (A→0, ….Z→25), and then encrypting each number separately using Bob's public key *e* and a large *n.* Is this scheme secure? If not, describe the most efficient attack against this encryption method.

Q6 State the value of the padding field in SHA-512 if the length of the message is

a. 1919
b. 1920
c. 1921

Q7 State the value of the length field in SHA-512 if the length of the message is

a. 1919
b. 1920
c. 1921