FIT3031 – Tutorial 3 Sample Solutions

ASYMMETRIC ENCRYPTION

Review

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

Ans: Message authentication is a procedure that allows communicating parties to verify that received message is authentic. The two important aspects of message authentication are:

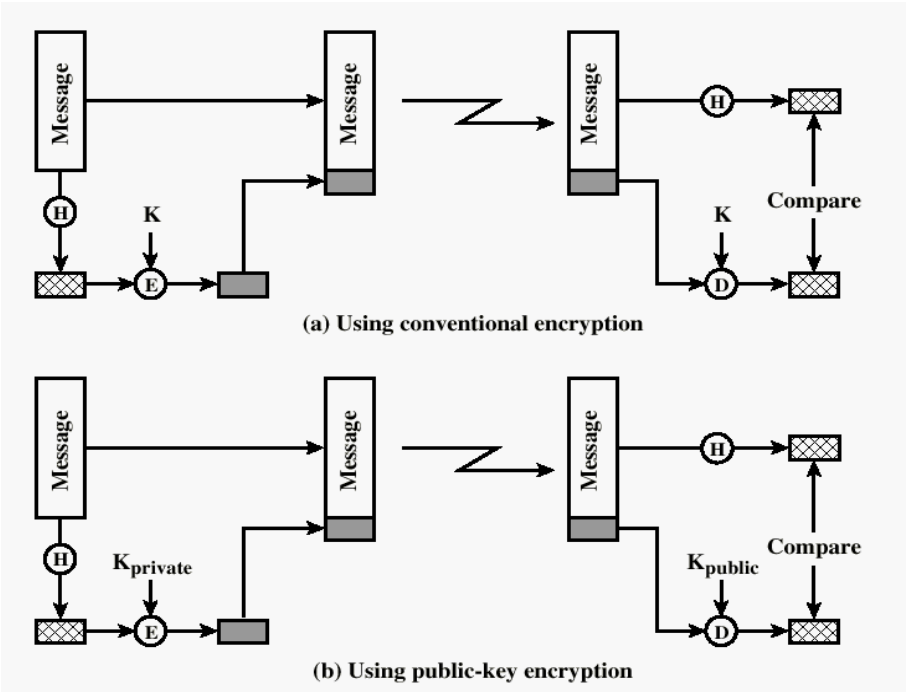
- To verify that the contents of message have not been altered (message integrity is maintained) and
- The source is authentic, message comes from its alleged source.

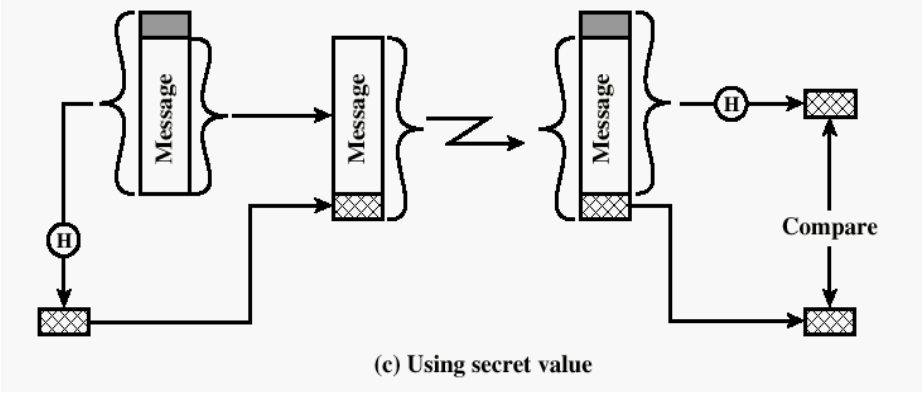
Message encryption, message authentication code, keyed hash function are the three approaches to message authentication.

Q2 What is a message authentication code?

Ans: An authenticator that is a cryptographic function of both the data to be authenticated and a secret key.

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





(c) Using secret value

Ans:

a) A hash code is computed from the source message, encrypted using symmetric encryption and a secret key, and appended to the message. At the receiver, the same hash code is computed. The incoming code is decrypted using the same key and compared with the computed hash code.
b) This is the same procedure as in (a) except that public-key encryption is used; the sender encrypts the hash code with the sender's private key, and the receiver decrypts the hash code with the sender's public key.
c) A secret value is appended to a message and then a hash code is calculated using the message plus secret value as input. Then the message (without the secret value) and the hash code are transmitted. The receiver appends the same secret value to the message and computes the hash value over the message plus secret value. This is then compared to the received hash code.
(In each of these schemes you will need to explain why each of these three schemes provide message authentication.)

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

Ans:

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

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

Ans: There are the followings:
Plaintext: This is the readable message or data that is fed into the algorithm as input.
Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.

The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts.

Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

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

Ans:

Encryption/decryption: The sender encrypts a message with the recipient's public key.

Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

Key exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

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

Ans: The key used in conventional encryption is typically referred to as a secret key. The two keys used for public-key encryption are referred to as the public key and the private key.

Q8* What is a digital signature and a digital certificate?

Ans: A digital Signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

Digital certificate binds an identity to a pair of keys that can be used to encrypt & sign digital information. It makes it possible for anyone to verify claims from individuals that they have the right to use a given key.

Q9* What is a public key certificate?

Ans: A pubic-key certificate consists of a public key plus a User ID of the key owner, with the whole block signed by a trusted third party. Typically, the third party is a certificate authority (CA) that is trusted by the user community, such as a government agency or a financial institution.

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

Ans: Several different approaches are possible, involving the private key(s) of one or both parties. One approach is Diffie-Hellman key exchange. Another approach is for the sender to encrypt a secret key with the recipient's public key.

Problems:

Modular Arithmetic Applications

Q1* Find the integers x such that

a. $5x \equiv 4 \pmod 3$

$5x \pmod 3 = 5 \times 2 \pmod 3 = 10 \pmod 3 = 1$

$4 \pmod 3 = 1$

$x = 2$

b. $7x \equiv 6 \pmod 5$

$7x \pmod 5 = 7 \times 3 \pmod 5 = 1$

$6 \pmod 5 = 1$

$x = 3$

c. $9x \equiv 8 \pmod 7$

$9x \pmod 7 = 9 \times 4 \pmod 7 = 36 \bmod 7 = 1$

$8 \pmod 7 = 1;$

$x = 4;$

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;

Hint: Decryption is not as hard as you think;

$n = p \times q = 3 \times 11 = 33;$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20;$

$ed \bmod \phi(n) = 1;$

$7 \times d \bmod \phi(n) = 7 \times d \bmod 20 = 1;$

$d = 3$

Encryption:

$$C = M^e \bmod n = 5^7 \bmod 33$$
$$= 5^3 \times 5^3 \times 5 \bmod 33$$
$$= 26 \times 26 \times 5 \bmod 33$$
$$= 2 \times 13 \times 2 \times 13 \times 5 \bmod 33$$
$$= 4 \times 169 \times 5 \bmod 33$$
$$= 4 \times 4 \times 5 \bmod 33$$
$$= 80 \bmod 33$$
$$= 14$$

Decryption

$M = C^d \bmod n = 14^3 \bmod 33 = 196X14 \bmod 33;$
$= 31X14 \bmod 33 = 434 \bmod 33 = 5 = M;$

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

$$n = p \times q = 5 \times 11 = 55;$$
$$\phi(n) = (p-1)(q-1) = 4 \times 10 = 40;$$
$$ed \bmod \phi(n) = 1;$$
$$e = 3;$$
$$3 \times d \bmod 40 = 1;$$
$$3 \times 27 \bmod 40 = 81 \bmod 40 = 1;$$
$$d = 27$$

Encryption:

$$C = M^e \bmod n = 9^3 \bmod 55$$
$$= 81 \times 9 \bmod 55$$
$$= 26 \times 3 \times 3 \bmod 55$$
$$= 78 \times 3 \bmod 55$$
$$= 23 \times 3 \bmod 55$$
$$= 69 \bmod 55$$
$$= 14;$$

Decryption

$M = C^d \bmod n = 14^{27} \bmod 55$

$= (14^3)^9 \bmod 55$

$= (2744)^9 \bmod 55$

$= 49^9 \bmod 55 = 7^{18} \bmod 55$

$= (7^3)^6 \bmod 55 = (343)^6 \bmod 55$

$= 13^6 \bmod 55$

$= (13^2)^3 \bmod 55 = (169)^3 \bmod 55 = 4^3 \bmod 55$

$= 64 \bmod 55$

$= 9 = M;$

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?

e= 5; n = 35 = 7X5 ; ∅(n) =6X4 = 24 ; C = 10;
ed mod24 = 1; d = 5;
M = C^dmodn = 10^5mod35 = 10^2X10^2X10mod35 = 30X30X10mod35
= 90X100mod35 = 20X30mod35 =
60X10mod35=25X10mod35=5 mod35;
= 5;

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*)

$Y_A = a^{X_A} \bmod q = 3^{X_A} \bmod 17;$

$3^4 \bmod 17 = 81 \bmod 17 = 13;$

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; 17*13=221; 15*17=255;*)

Using Y_A, B calculates the shared secret key, K_{AB} as follows:

$K_{AB} = Y_A^{X_B} \bmod 17$

$K_{AB} = 13^6 \bmod 17 = (13^2 \bmod 17)^3 \bmod 17$

$= (169 \bmod 17)^3 \bmod 17 = 16^3 \bmod 17$

$= 16 \bmod 17 \times 16^2 \bmod 17 = 16 \bmod 17 \times 256 \bmod 17$

$= 16 \times 1 \bmod 17 = 16$

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)*

$$Y_B = \alpha^{X_B} \bmod q$$
$$= 3^6 \bmod 17 = 81 \times 9 \bmod 17 = 13 \times 9 \bmod 17$$
$$= 117 \bmod 17 = 15;$$

B calculates Y_B =15 and sends it to A; A then calculates the shared secret key K_{AB} as follows:

$$K_{AB} = Y_B^{X_A} \bmod 17$$
$$= 15^4 \bmod 17 = 15^2 \bmod 17 \times 15^2 \bmod 17$$
$$= 225 \bmod 17 \times 225 \bmod 17$$
$$= 4 \times 4 \bmod 17 = 16$$

Other Problems:*

Q5 Suppose Bob uses RSA cryptosystem with a very large modulus, *n* for which the factorization 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 RSA with large *e* and *N.* is this scheme secure? If not, describe the most efficient attack against this encryption method.

Ans: Consider a set of alphabetic characters {A, B, …, Z}. The corresponding integers, representing the position of each alphabetic character in the alphabet, form a set of message block values SM = {0,1, 2, …, 25}. The set of corresponding ciphertext block values SC = {0^e mod *N*, 1^e mod *N*, …, 25^e mod *N*}, and can be computed by ***everybody with the knowledge of the public key of Bob.***

Thus, the most efficient attack against the scheme described in the problem is to compute ***Me* mod *N* for all possible values of *M***, then create a lookup table with a ciphertext as an index, and the corresponding plaintext as a value of the appropriate location in the table.

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

a. 1919
b. 1920
c. 1921

Ans:
a. 1 bit
b. 1024 bits
c. 1023 bits

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

a. 1919
b. 1920
c. 1921

Ans:

a. 1919 $(011101111111)_2$ = less than 128 bits $(1919)_{10}$
b. 1920 $(011110000000)_2$ = less than 128 bits $(1920)_{10}$
c. 1921 $(011110000001)_2$ = less than 128 bits $(1921)_{10}$