FIT2093: Sample Tutorial 7 Solutions

Public Key Cryptography

Review

1. What are the essential ingredients of an asymmetric cipher?
   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 key:** 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 ciphertexts.
   Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

2. List and define three uses of a public key cryptosystem.
   a. Encryption/decryption: The sender encrypts a message with the recipient's public key.
   b. 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.
   c. 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.

3. What is the difference between a private key and a secret key?
   Secret key is used in symmetric cryptography where only one key is needed for encryption and decryption.
   Private key is using in public key cryptography to decrypt what have been encrypted with the public key.

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

5. What is a public-key certificate?
   In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature of the Certification Authority (CA) to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

6. Briefly explain Diffie-Hellman key exchange.

   Two parties (A & B) each create a public-key(A, B), private-key (a, b) pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key (a, b) and the other side's public key. It is assumed both parties have already agreed on a prime number, p and its primitive root g. Using the following equations each user can calculate the shared secret key, K as show below:.

   $A = g^a \bmod p$ (A's public key); a = A's private key

   $B = g^b \bmod p$ (B's public key); b = B's private key

   $K = B^a \bmod p$ (which A calculates) = $A^b \bmod p$ (which B calculates)

7. How many keys are required for two people to communicate via an asymmetric cipher? How many keys are required for n people to communicate with each other securely?
   Only 2 keys (Public & Private key of one user to communicate between 2 users securely.
   For n users, they would need 2n keys to securely exchange information with each other.

Problems

1. Assume that Alice and Bob live in the 21st century and have access to encryption technology. What are Alice's options to securely send the recipe to Bob? Discuss the potential security threats for each of the options.
   Options:
   a. Rewrite the recipe using a pre-determined way of scrambling the message, eg transpose all letter by 3 positions. Communicate the way to scramble the letters in the recipe using the phone.

   Marvin can tap Alice's phone to find out the method of scrambling the message. Once it is known it will be easy to break the cipher text.

b. Using the idea of private encryption such as DES. Encrypt the message with DES key. Communicate the value of the key using phone or postal. An improvement of the way the key is communicated is by using the Diffie-Helmann method.

Marvin can find the value of the key when telephone or postal communication is used but it will be relatively more difficult to decrypt the message. Marvin needs reasonable powerful computer to decipher the text.

If Alice and Bob use the Diffie-Helmann key-exchange then Marvin will have a problem in finding the value of the shared key.

3. Using the public key encryption system.
Alice and Bob do not need to exchange the shared key. They can use the combination of their private and public keys to encrypt the recipe and sent it using email.

Marvin will find it to be difficult to decipher the message without getting hold of either Alice or Bob's secret key.

2. Perform encryption and decryption using RSA algorithm (where $n = p*q$; $C = M^e \bmod n$; $P = C^d \bmod n$; $e*d \bmod \phi(n) = 1$; plaintext M & Ciphertext C; e & d are public and private key.)
for the following:
   a. p=3; q=11; e = 7; M = 5;
   b. p =5; q = 11; e = 3; M = 9;

a. p = 3; q = 11; n = p.q = 33 ; e = 7; M = 5; $\varnothing(n) = 2X10 = 20$; edmod20 = 1; d =3;

Encryption
$C = M^e \bmod n = 5^7 \bmod 33$;
$= 5^3 5^3 5 \bmod 33$;
$= 26X26X5 \bmod 33$;
$= 2X13X2X13X5 \bmod 33$
$= 4X169X5 \bmod 33$
$= 4X4X5 \bmod 33 = 80 \bmod 33 = 14$;

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 n = pq =55; e = 3; M = 9;
$\varnothing(n) = (p-1)(q-1) = 4X10 = 40$;
$ed \bmod 40 = 1$; $3X27 \bmod 40 = 81 \bmod 40 = 1$; d=27;

Encryption
$C = 9^3 \bmod 55 = 81X\ 9 \bmod 55 = 26X9 \bmod 55 = 26X3X3 \bmod 55$
$= 78X3 \bmod 55 = 23X3 \bmod 55 = 14$;

Decryption

M = C^{27}mod 55 = 14^{27}mod55 = $(14^3)^9$mod55 = $(7X2^3)^9(7^2)^9$mod55 = 7^{18}mod55;

= $(7^3)^6$mod55 ;

= $(343)^6$mod55 = 13^6mod55;

= $(169)^3$mod55 = 4^3mod55 = 64 mod55 = 9 = M;

3. 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;

4. Users A and B use the Diffie-Hellman key exchange technique with a common prime p=11, primitive root g= 2;

   a. a = 6 (A's private key), what is A = g^a mod p (A's public key)?

      9, because 2^6 mod 11 = 9

   b. If B = g^b mod p (B's public key) = 3, what is the shared secret session key?

      K = 3^6 mod 11= 3

   c. What is b, B's private key?

      B = 3 = g^b mod 11 = 2^b mod11;

      b = 1 ; 2^1 mod 11 =2
      b = 2 ; 2^2 mod 11 =4
      b = 3 ; 2^3 mod 11 =8
      b = 4 ; 2^4 mod 11 = 16 mod 11 = 5
      b = 5 ; 2^5 mod 11 = 2^4 X 2 mod 11 = 5 X 2 mod 11 = 10
      b = 6 ; 2^6 mod 11 = 2^5 X 2 mod 11 = 10 X 2 mod 11 = 20 mod 11 = 9
      b = 7 ; 2^7 mod 11 = 2^6 X 2 mod 11 = 9 X 2 mod 11 = 7
      b = 8 ; 2^8 mod 11 = 2^7 x 2 mod 11 = 7 X 2 mod 11 = 14 mod 11 = 3
      Thus, b=8 is the answer