Tutorials 2

Questions and answers

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

•A user's private key is kept private and known only to the user.
• The private key can be used to decrypt ciphertext messages encrypted by public key.
•The private key can also be used to create a signature that can be verified by anyone with the public key.

•The user's public key is made available to others to use.
•The public key can be used to encrypt information that can only be decrypted by the possessor of the private key.

- 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?

For conventional encryption, each pair of communicating parties will need to share one secret key, so the total number of keys required are 20*19/2 or (N*(N-1)/2) [190 keys]

For public key encryption, every communicating party need 2 keys, one public key and one private key. So the total number of keys needed are 40 keys (or 20 pairs of keys).

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

- Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel.
- It allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.
- *Then briefly describes the algorithm (see slides)*

- 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?

You need to show all the works of calculation, i.e. steps of how you get the results.

YA= α^XA mod q = 81 mod 31= 19
Yb= α^XB mod q = 9 mod 31 =9

Key: 19^2 mod q = 20
9^4 mod q = 20

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

• Plaintext: Un-encrypted text/data that is fed into the algorithm as input.
• Encryption algorithm: Performs various transformations on the plaintext.
• Public and private keys: A pair of keys of the communicating parties, if one is used for encryption, the other is used for decryption.
• Ciphertext: Encrypted version of the plaintext and the key.
• Decryption algorithm: Accepts the ciphertext and the matching key and produces the original plaintext.

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

• 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. E.g. Diffie-hellman key exchange

- What is the RSA? What are its uses?

RSA is a public-key encryption algorithm. Block cipher in which the plaintext and ciphertext are integers between 0 and n-1.

n = p * q where p and q are prime numbers

Encryption: c = m^e mod(n)

Decryption: m = c^d mod(n)

where Public--key k_u=(e,n) and Private--key k_r=(d,n)

It can be used for:

Confidential communications..

Signed electronic documents (signature)..

- Define what we mean by message authentication code

Message authentication code (MAC) is a method used to check the integrity of a message. It requires a key or secret value.
A MAC takes a variable-length message and a secret key as input and produces a fixed length authentication code.

- What is an one-way hash function?

A hash is a one way cryptographic function and the sender and receiver do not need to share a secret key. A hash function takes a message of a variable length and produces a fixed length output as message digest.

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

•The difference between a MAC and a hash function is that the sender and the receiver of a MAC need to share a secret key, but no key is required for hash functions.

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

•To replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module.

- 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

You need to show all the works of calculation, i.e. steps of how you get the results.

Solution key:
d = 3, C = 14
d = 27, C = 14
d = 53, C= 57

- 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?

You need to show all the works of calculation, i.e. steps of how you get the results.

Solution key
M = 5

Past Exam question

Alice wants to send Bob a message. She wants to ensure that only Bob can read the message, and she also wants to ensure that Bob is certain the message is from Alice and no one else. answer the following:

i. What are the two security services Alice wants to provide?

ii. Briefly explain the steps through which Alice can achieve these using the security methods you have learnt.

- The security methods we have learnt include:

Conventional encryption, public-key encryption,

Hash functions, MAC, digital signature

- One possible way for Alice to achieve the two security services is:
- Alice can use MAC to generate a mac which is appended to the plaintext message, and then the overall message is encrypted using conventional encryption. Then the ciphertext is sent to Bob. Bob can then decrypt the ciphertext, then calculate a new mac which can be compared to the mac sent by Alice. If the two macs match with each other, then Bob is certain the message is from Alice and Bob is also certain the message is not read by anyone else.