CAE - II

Name: Mahnish Devaraj

Reg No: 39110636

Roll No: 195115398

Date: 04 Apr 2022

Subject Name: Network security

subject code: SCSA1602

Total pages: 6

PART - B

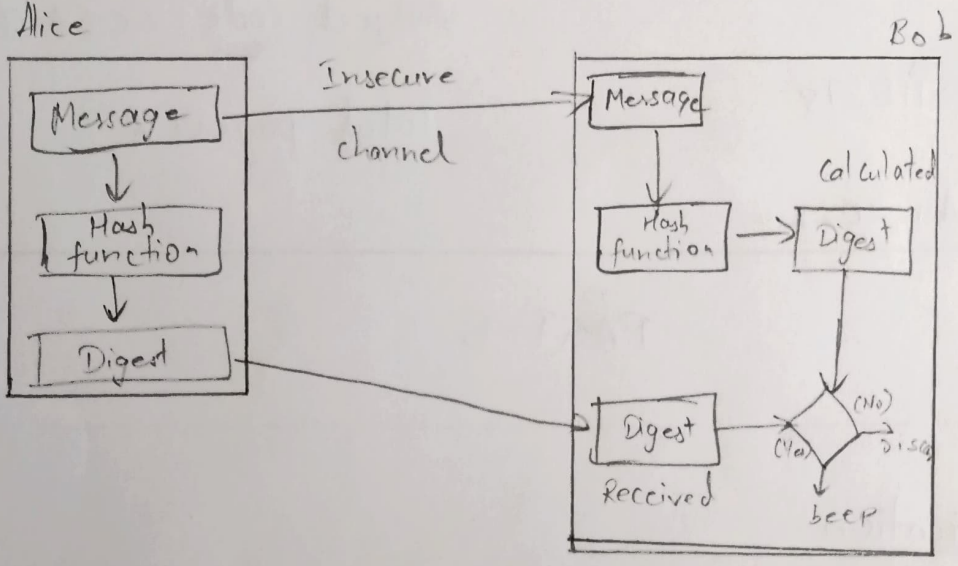
(8) Authentication

The process of authentication in the context of computer systems means assurance and confirmation of a user's identity. Before a user attempts to access information stored on network, he or she must prove their identity and permission to access the data.

MD5 (Message Digest)

Message Digest is used to ensure the integrity of message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through Cryptographic hash function

This function creates a compressed image of the messaged called Digest.



This message and digest pair is equivalent to a physical document and finger print of a person on that document. Unlike the physical document and the finger print, the message and the digest can be set seperately.

- Most importantly, the digest should be unchanged during the transmission.
- The cryptographic hash function is a one way function, that is, a function which is practically infeasible to invert. This cryptographic hash function takes a message of variable length as input and creates a digest/hash/finger print of fixed length, which is used to verify the

of the message.

- Message digest ensures the integrity of the document. To provide authentication of the message, digest is encrypted with sender's private key. Now this digest is called digital signature, which can be decrypted by the receiver who has sender's public key. Now the receiver can authenticate the sender and also ~~verify~~ verify the integrity of the sent message.

(6) Given,

$C = 10$

$e = 5$

$n = 35$

We know that the ciphertext $C = 10$, and the public key $PU = \{e, n\} = \{5, 35\}$. Based on Eulers totient function, $\phi(n)$ is defined as the number of positive integers less than n and relatively prime to n.

~~$\phi(n) = (p-1)(q-1)$~~

$\phi(n) = 24.$

We guess prime numbers p and q. Let p and q be 5 and 7 respectively. All the following conditions will be satisfied based on the guess:

(1) $n = p * q = 5 * 7 = 35$

(2) $\phi(n) = (p-1)(q-1) = (5-1)(7-1) = (4)(6) = 24$

(3) $gcd(\phi(n), e) = gcd(24, 5) = 1, \quad 1 < e < \phi(n)$

Based on RSA key generation algorithm,

$d = e^{-1} \bmod \phi(n)$

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

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

Now, $e = 5$, $\phi(n) = 24$. So, $5d \bmod 24 = 1$ and $d = 5$

find the private key $PR = \{d, n\} = \{5, 35\}$

Based on RSA decryption Algorithm,

$$M = C^d \bmod n$$
$$= 10^5 \bmod 35$$
$$= 5$$

we also can verify the correctness by RSA encryption algorithm as the following:

$$C = M^e \bmod n$$

$$= 5^5 \bmod 35$$

$$= 10$$

∴ the plaintext is 5

PART-A

① Private Key

The private key is used to bothe encrypt and decrypt the data. This key is shared between the ~~source~~ sender and receiver of the encrypted sensitive information. The private key is also called symmetric being common for both parties. Private key cryptographic is faster than public key cryptographic mechanism.

Public Key

The public key is used to encrypt and a private key is used to decrypt the data. The private key is shared between the sender and receiver of the encrypted sensitive information. the public key is also called as asymmetric cryptography.

(2) Yes, we can use the DES algorithm to generate the message authentication code (MAC).

Two parties must preshare a secret key (such as a DES Key). Once shared, the sender may generate a HMAC by hashing the message with an algorithm such as MD5 or SHA-1, and then encrypting the hash with the preshared key.

(3) Digital Signature
Encryption
Authentication
Non Repudiation
Integrity
Confidentiality
Key generation
signing
Verification

(4) H can be applied to a block of data of any size. H produces a fixed length output. $H(x)$ is relatively easy to compute. For any given code h, it is computationally infeasible to find x such that $H(x)=h$. It is computationally infeasible to find any pair (x,y) such that $H(x)=H(y)$

(5) A digital signature is a mathematical scheme for verification the authentication of digital message. A valid digital signature, where the prerequisties are satisfied, giver a recipient very high confidence that the message was created by a known sender.