7.3.1 Q1

Q: symmetric key encryption + ad. + limit.

problem

PKI

Solution : ① Symmetric key uses the same shared key to encrypt and decrypt the message

② Advantage (1) It can be used effectively for data storage protection

(2) Fast, secure and requires shorter key

③ Disadvantages

(1) For the sender and receiver to have the same key, it must be sent over a communication media that is insecure, thus, how to exchange the ky

(2) If the secret key is lost or stolen, the encryption system fails.

③ Solve problem

(1) public key encryption solves the problem of exchanging keys

(2) In this method every user has a pair of numeric keys: private and public

(3) The keys can only be used in pairs.

④ Encryption can provide four key dimensions of e-commerce security

(1) It can provide assurance that the message has not been altered (Integrity)

(2) Prevent the user from denying that he/she has sent the message (non repudiation)

(3) provide verification of the identity of the message (authentication)

(4) Gives assurance that the message has not been read by others (confidentiality)