(a)

The given state block is a 4x4 matrix where each element is one byte , thus the size of the block is 16 bytes.

The new state after applying the AES S-box transformation is as follows:

3E CB 59 12

F7 25 65 57

56 91 2C 66

EB 2C D3 F7

(b)

For the first row, we have:

3E XOR 36 = 08 CB XOR 24 = EF 59 XOR A3 = FA 12 XOR 82 = 90

For the second row, we have:

F7 XOR 00 = F7 25 XOR 00 = 25 65 XOR 00 = 65 57 XOR 00 = 57

For the third row, we have:

56 XOR AA = FC 91 XOR B2 = 23 2C XOR 30 = 1C 66 XOR 57 = 31

For the fourth row, we have:

EB XOR 11 = FA 2C XOR 43 = 6F D3 XOR 1D = CE F7 XOR C1 = 36

The result of the last state of the round:

08 EF FA 90

F7 25 65 57

FC 23 1C 31

FA 6F CE 36

2.

* Ya = 2^Xa mod 11

2^1 \mod 11 = 2

2^2 \mod 11 = 4

2^3 \mod 11 = 8

2^4 \mod 11 = 5

2^5 \mod 11 = 10

2^6 \mod 11 = 9

Ya=9 -> Xa=6

A’s private key Xa is 6.

* Yb = 2^Xb mod 11

2^1 mod 11 = 2

2^2 mod 11 = 4

2^3 mod 11 = 8

2^4 mod 11 = 5

2^5 mod 11 = 10

2^6 mod 11 = 9

2^7 mod 11 = 7

2^8 mod 11 = 3

Yb=3 -> Xb=8

K = Ya^Xb mod q = 9^8 mod 11 = 3

Therefore, the shared secret key K = 3.

3.

First, we calculate d from e\*d mod φ(n) = 1 .

According to the subject e=5,n=35.

φ(n)=φ(p) \*φ(q) = (p - 1)\*(q - 1) ,two primes p and q(5and7) -> φ(n)=φ(p) \*φ(q) =24.

So we can get the result of d, d=5.

Second, we calculate p from p=C^d mod n.

d=5,C=10,n=35 -> p=5.

4.

This solution presents a major security risk. A passive attacker can intercept and record this random string and the XOR result, and then forward it to the legitimate receiver without being discovered by the legitimate receiver. This enables passive attackers to derive secret keys and gain unauthorized access.

To solve this problem, we need to add authentication mechanisms in the protocol, such as adding digital signatures or using public key encryption when sending messages. This way, even if a passive attacker intercepts a message, it cannot forge a legitimate message, and the recipient can verify the integrity and origin of the message.

5.

Hash collisions occur because a hash function maps an input of arbitrary length to an output (hash value) of fixed length, resulting in the possibility of different plaintext inputs producing the same hash value.

The security of a hash function is not compromised by hash collisions because a collision attack does not allow an attacker to change the underlying plaintext to another plaintext whose hash collides with the original plaintext's hash value.

6.

a. With a digital signature (DS), Bob can detect that the message has been tampered with because the signature will not verify. With a message authentication code (MAC), Bob can detect the tampering because the MAC value will not match the recalculated MAC value.

b. With a DS, Bob will detect the replay attack because the signature will not verify for the repeated messages. With a MAC, Bob will detect the replay attack because the MAC value will be the same for all repeated messages, which is inconsistent with the expected behavior of a MAC.

c. With a DS, Bob can verify the signature using Oscar's public key and confirm that the message was signed by Oscar. With a MAC, Bob cannot resolve the conflict because the MAC value is not specific to any sender.

d. With a DS, Alice can prove that she did not sign the message by showing that her private key did not generate the signature. With a MAC, Alice cannot prove her innocence because the MAC value does not provide any information about the sender.

7.

Public Key Infrastructure (PKI) is a system that provides a framework for managing digital certificates used in public key encryption. PKI enables users to securely exchange information over an insecure network by verifying the identity of the communicating parties and providing confidentiality, integrity, and non-repudiation of data.

PKI does not perform encryption itself. Instead, it provides the necessary infrastructure to manage digital certificates, which contain public keys used for encryption and digital signatures.

PKI uses asymmetric encryption to provide secure communication between parties. It uses public and private keys to encrypt and decrypt data, respectively.

PKI needs a means to cancel or invalidate certificates because certificates may become compromised due to key theft, loss, or expiration. If a certificate is not revoked, it may be used by an attacker to impersonate the legitimate user and conduct fraudulent activities.

It is not sufficient for the PKI to stop distributing a certificate after it becomes invalid because the certificate may have already been distributed and used by others. Therefore, the PKI needs a mechanism to revoke or cancel certificates and to propagate the revocation status to all parties who rely on the certificate.