Ch 31 Summary

- The three goals of security are confidentiality, integrity, and availability .
- These goals are threatened by attacks such as snooping, traffic analysis, modification, masquerading, replaying, repudiation, and denial of service .
- Cryptography is a technique described in this chapter to achieve security goals; the other technique, steganography, is left for more advanced books on security .
- Confidentiality is achieved through asymmetric-key and symmetric-key ciphers .
- In a symmetric-key cipher the same key is used for encryption and decryption, and the key can be used for bidirectional communication .
- We can divide traditional symmetrickey ciphers into two broad categories: substitution ciphers and transposition ciphers .
- In asymmetric-key cryptography there are two separate keys: one private and one public .
- Asymmetric-key cryptography means that Bob and Alice cannot use the same set of keys for two-way communication .
- Discussion of security is not limited to confidentiality; other aspects of security include integrity, message authentication, entity authentication, and key management .
- Message integrity is achieved using a hashing function to create a digest of the message .
- Message authentication is achieved using techniques such as message authentication code (MAC) or digital signature .

- Entity authentication is achieved using either personal identification, such as a password, or techniques such as the challengeresponse process .

- To provide either confidentiality or other aspects of security, we need either secret keys or the combination of private-public keys .

- The distribution of secret keys can be done by a key distribution center (KDC) or through instantaneous methods such as Diffie-Hellman .

- The certification of public keys can be done through a certification authority (CA) .

31.5.2 Questions

Q31-1. Which of the following attacks is a threat to confidentiality?

a. snooping **b.** masquerading **c.** repudiation

Q31-1. Only snooping is a threat to confidentiality. Masquerading and repudiation are threats to integrity.

Q31-2. Which of the following attacks is a threat to integrity?

a. modification **b.** replaying **c.** denial of service

Every organization should require security to the organization assets or information. There are three security aspects that should achieve the information security.

• Confidentiality: confidentiality is a security aspect that defines the organization information shouldn't share to unauthorized users.

• Integrity: integrity is a security aspect that defines the organization data or information shouldn't alter.

• Availability: Availability is a security aspect that defines the organization made information available to authorized users only.

Therefore, option (C) is wrong answer.

a.

Modification is vulnerability that is used to modify the victim's data. Therefore the integrity isn't achieved.

Therefore, the **correct option is (B)**

b.

Replaying is vulnerability, attacker access the victim data and later replay that accessed data. Therefore integrity of the data isn't achieved.

Therefore, the correct **option is (A).**

c.

Denial of service (Dos) is a vulnerability that shutdown the system and system resources, therefore availability isn't achieved.

Q31-3. Which of the following attacks is a threat to availability?

a. repudiation **b.** denial of service **c.** modification

Q31-3. Only denial of service is a threat to availability. Repudiation and modification are threats to integrity.

Q31-4. Which of the following words means "secret writing"? Which one means "covered writing"?

a. cryptography **b.** steganography

a.

Cryptography: Cryptography is a technique that converts plaintext (which is able to understand) into ciphertext (which is doesn't able to understand) vice versa by using some cryptographic algorithms and methods. It is also known as secret writing.

b.

Steganography: Steganography is a technique that embeds information or data in a picture or file. It is also known as covered writing.

Q31-5. When a sealed letter is sent from Alice to Bob, is this an example of using cryptography or steganography for confidentiality?

Q31-5. This is an example of steganography because the letter is covered by the seal.

Q31-6. When a letter is sent from Bob to Alice in a language that only the two can understand, is this an example of cryptography or steganography?

Cryptography:

Cryptography is a technique that converts plaintext (which is able to understand) into ciphertext (which is doesn't able to understand) vice versa by using some cryptographic algorithms and methods. It is also known as secret writing.

Steganography:

Steganography is a technique that embeds information or data in a picture or file. It is also known as covered writing.

Refer question, given case is example for the steganography because the information or data in the letter is able to read, if the seal is opened by anyone.

Q31-7. Alice has found a way to write secretly to Bob. Each time, she takes a new text, such as an article from the newspaper, but inserts one or two spaces between the words. A single space means a binary digit 0; a double space means a binary digit 1. Bob extracts the binary digits and interprets them using ASCII code. Is this an example of cryptography or steganography? Explain.

P10-7. We apply the key = 1, 2, 3, 4, 5, 6, and 7 to find the plaintext.

Ciphertext	Key	Plaintext
UVACLYZLJBL	1	tuzbkxeykiaxy
UVACLYZLJBL	2	styajwdxjhzwj
UVACLYZLJBL	3	rsxzivcwigyvi
UVACLYZLJBL	4	qrwyhubvhfxuh
UVACLYZLJBL	5	pqvxgtaugewtg
UVACLYZLJBL	6	opuwfsztfdvsf
UVACLYZLJBL	7	notverysecure

Q31-7. This is an example of steganography because the message is hidden inside the essay.

Q31-8. Alice and Bob exchange confidential messages. They share a very large number as the encryption and decryption key in both directions. Is this an example of symmetric-key or asymmetric-key cryptography? Explain.

There are two key techniques used in cryptography for encryption and decryption. That is,

1. Symmetric key technique: symmetric key is a single key that is used for both encryption and decryption in both directions.

2. Asymmetric key technique: asymmetric key is two keys, where one key is used for the encryption and another key for decryption in both directions. It is also known as public key cryptography.

Refer given case, there is single key is shared for the both encryption and decryption. Therefore it is the example for symmetric key cryptography.

Q31-9. Alice uses the same key when she encrypts a message to be sent to Bob and when she decrypts a message received from Bob. Is this an example of symmetric-key or asymmetric-key cryptography? Explain.

There are two key techniques used in cryptography for encryption and decryption. That is,

1. Symmetric key technique: symmetric key is a single key that is used for both encryption and decryption in both directions.

2. Asymmetric key technique: asymmetric key is two keys, where one key is used for the encryption and another key for decryption in both directions. It is also known as public key cryptography.

Refer given case, alice use same key for the encryption and decryption at her end. Therefore it is the example for the symmetric key cryptography.

Q31-9. This is an example of symmetric-key cryptography because the same key is used both for encryption and decryption. In asymmetric-key cryptography, a public key should be used for encryption and a private key for decryption.

Q31-10. Distinguish between a substitution cipher and a transposition cipher.

Traditional ciphers are divided into following two categories,

1. Substitution cipher
2. Transposition cipher

Substitution cipher	**Transposition cipher**
Substitution cipher is a encryption technique, where each letter in plain text is replaced with the another letter or number and symbols in cipher text.	Transposition cipher is a encryption technique, where the position of letter in plaintext is changed into another position in cipher text.
There are two types in Substitution cipher 1. Monoalphabetic cipher 2. Polyalphabetic cipher	There are two types in Transposition cipher 1. keyless transposition 2. keyed transposition
The position of the letter is doesn't changed but identity is changed	The position of the letter is changed but identity is doesn't changed
Example of Substitution cipher is ceaser cipher	Example of transposition cipher is rail fence cipher

Q31-11. In a cipher, all As in the plaintext have been changed to Ds in the ciphertext and all Ds in the plaintext have been changed to Hs in the ciphertext. Is this a monoalphabetic or polyalphabetic substitution cipher? Explain.

There are following two types in Substitution cipher,

1. Monoalphabetic cipher: Monoalphabetic cipher, a letter in plaintext is always replaced with the same letter in ciphertext.

2. Polyalphabetic cipher: Polyalphabetic cipher, a letter is replaced with the different substitutions.

Given case is example for the Monoalphabetic cipher because As in plaintext is replaced with the D and D replaced with the Hs in ciphetext.

Therefore, it is a example for the Monoalphabetic cipher.

Q31-11. This is a monoalphabetic substitution cipher because changing depends on what the character is, not on the position of the character.

Q31-12. Which cipher can be broken more easily, monoalphabetic or polyalphabetic?

There are following two types in Substitution cipher,

1. Monoalphabetic cipher: Monoalphabetic cipher, a letter in plaintext is always replaced with the same letter in ciphertext.

2. Polyalphabetic cipher: Polyalphabetic cipher, a letter is replaced with the different substitutions.

Monoalphabetic cipher is broken easily because every letter is replaced with another letter always.

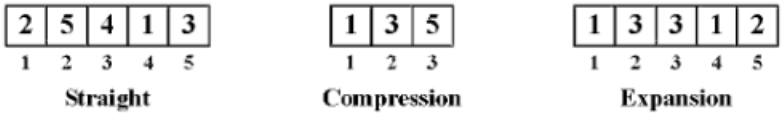
If intruder try to decrypt the ciphertext then intruder initially verify the letter combination. That is useful to identify the Monoalphabetic cipher.

Therefore, Monoalphabetic cipher is easily broken than Polyalphabetic cipher.

Q31-13. Assume Alice and Bob use an additive cipher in modulo 26 arithmetic. If Eve, the intruder, wants to break the code by trying all possible keys (brute-force attack), how many keys should she try on average?

P10-13. As we said about the keys for the transposition cipher, permutation boxes (P-boxes) can be represented by a table in which the contents of each element shows the input number and the index show the output number.

a. A straight permutation box of n x n size is a table of n entries in which each entry is unique. A compression permutation of n x m size is a table of m entries in which the blocked inputs are not shown. An expansion permutation of n x m size is a table of n entries in which some of the entries are repeated. The following shows the three tables for permutation boxes in Figure 10.8 in the text. We have not shown the indexes.



b. The compression and expansion boxes have no inversions because the number of inputs and outputs is not equal. Only the straight boxes can be inverted. We first need to swap the contents and the indexes and then sort the result according to the index. The following shows the inversion of a straight permutation box used in the decryption.

Q31-13. The key in this case needs to be between 0 and 25 (although there is no cipher if the key is 0). on average Eve needs to test 26/2 = 13 keys to break the code.

Q31-14. If we have a single integer key in Example 31.1 and 31.2 in the text, how many integer keys do we have in Example 31.3 in the text?

In additive cipher, the plaintext and ciphertext are performed modulus operation with 26.

Refer example 10.1, 10.2, and 10.3. In three cases same integer key is used. Therefore a letter is replaced with the same letter always.

Therefore, the size of the integer key is single.

Q31-15. Assume we have a plaintext of 1000 characters. How many keys do we need to encrypt or decrypt the message in each of the following ciphers?

a. additive **b.** monoalphabetic **c.** autokey

Q31-15. For the additive cipher, we use only one key. For the monoalphabetic cipher, we use 26 keys. For the autokey cipher, we use 1000 keys.

a.

Additive cipher is the substitution cipher; the lowercase letters in plain text is replaced with the uppercase letters in cipher text. That is the key size is 26 (0 to 25).

Refer question, there are 1000 characters in plaintext but the key size is 26.

b.

Monoalphabetic cipher is substitution cipher, where letters or characters are replaced with the corresponding character. That is the relationship between letters in the plaintext and

ciphertext is one-to-one.

Refer question, there are 1000 characters in plaintext and the key size is 1000.

c.

Autokey is polyalphabetic cipher, where each subkey used to encrypt the plaintext with the corresponding character. The first subkey is predetermined and the second subkey is the plaintext character of the previous block. That is the key size 26 (0 to 25).

Key size of the auto key is 27, predetermined key and 0 to 25 characters.

Q31-16. According to the definitions of stream and block ciphers, find which of the following ciphers is a stream cipher.

a. additive **b.** monoalphabetic **c.** autokey

Stream cipher is symmetric cipher, where data encrypted bit by bit at a time. And the block cipher is also symmetric cipher but the data encrypted block by block.

a.

Additive cipher is the substitution cipher; the lowercase letters in plain text is replaced with the uppercase letters in cipher text.

Therefore, additive cipher is a stream cipher.

b.

Monoalphabetic cipher is substitution cipher, where letters or characters are replaced with the corresponding character. That is the relationship between letters in the plaintext and ciphertext is one-to-one.

Therefore, Monoalphabetic cipher is a stream cipher.

c.

Autokey is polyalphabetic cipher, where each subkey used to encrypt the plaintext with the corresponding character. The first subkey is predetermined and the second subkey is the plaintext character of the previous block.

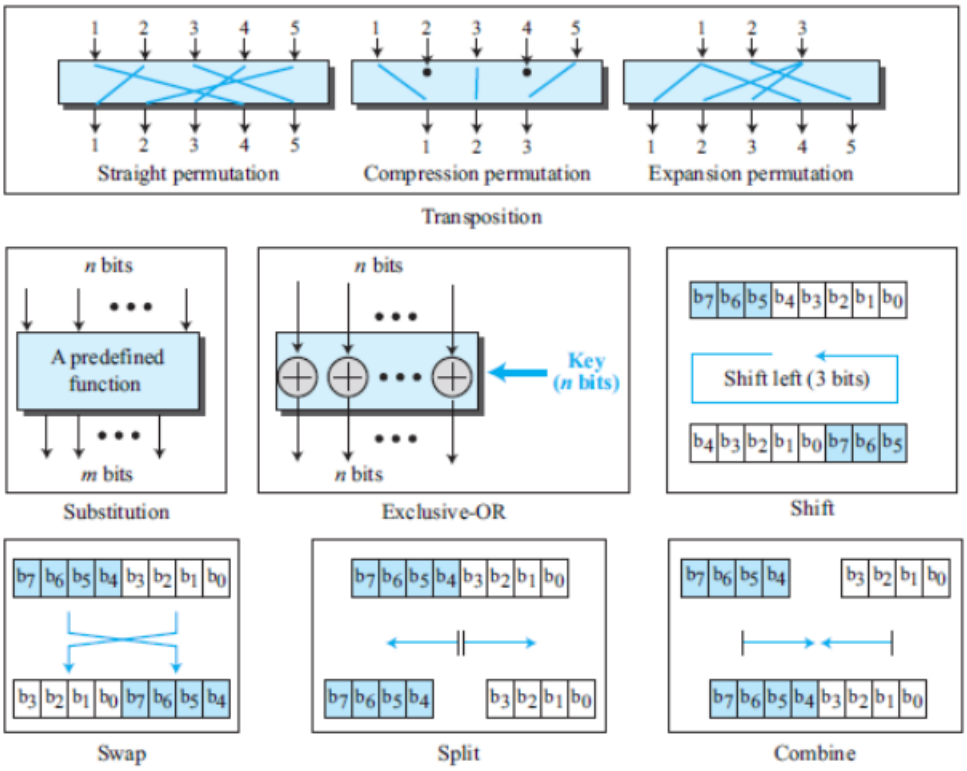
Therefore, Autokey cipher is a stream cipher.

Q31-17. A permutation block (P-box) in a modern block cipher has five inputs and five outputs. This is a _____ permutation?

a. straight **b.** compression **c.** expansion

Q31-17. This is a straight permutation because the number of inputs and the number of outputs are the same.

Q31-18. A permutation block (P-box) in a modern block cipher is an example of a key-less transposition cipher. What does this statement mean? (See Figure 31.8 in the text.)



Permutation box (P-BOX) is following three types,

1. **Straight permutation:** where input size is equal to the output size that is the bits are transposed as usually. (refer figure 10.8)

2. **Compression permutation:** where the output size is less than the input size that is the bits are compressed in this permutation. (refer figure 10.8)

3. **Expansion permutation:** where the output size is greater than the input size that is the bits are expanded in this permutation. (refer figure 10.8)

Refer question, permutation box in a modern block cipher is an example of a keyless transposition cipher.

In compression P-box, the output bits are less transposed when it compared with the plaintext.

Therefore, the given statement is true.

Q31-19. In a modern block cipher, we often need to use a component in the decryption cipher that is the inverse of the component used in the encryption cipher. What is the inverse of each of the following components?

a. swap **b.** shift right **c.** combine

a.

Swap: in swap, the first half is transposed into second half and second half is transposed into first half. That is the inverse operation is performed. (refer figure 10.8)

Therefore, the correct option is A.

b.

Shift right: in shift right, bits are transposed to right to left as per the corresponding shift right (n), where n is the size. (refer figure 10.8)

Therefore, option B is wrong answer.

c.

Combine: in combine, two blocks are combined into a single block. (refer figure 10.8)

Therefore, option C is wrong answer.

Q31-19.

a. The inverse of a swap operation is another swap operation. In other words, the swap operation is self-invertible.

b. The inverse of a shift right operation is a shift left operation using the same number of bits to be shifted.

c. The inverse of a combine operation is a split operation.

Q31-20. In each round of DES, we have all components defined in Figure 31.8 in the text. Which components use a key and which components do not?

Refer figure 10.8, there are following components used a key value *k*,

Compression permutation: in compression permutation, the output size is less than the input size that is the bits are compressed in this permutation as per the key value.

Expansion permutation: in expansion permutation, the output size is greater than the input size that is the bits are expanded in this permutation as per the key value.

Shift operation: in shift operations, the input bits are shifted to the either right side or left side as per the key value.

Refer figure 10.8, there are following components doesn't use key value, these components are used logical operations and predefined functions.

Straight permutation: where input size is equal to the output size that is the bits are transposed as usually, that is input is equal to the output.

Substitution: in substitution, a predefined function is used to produce the output.

Exclusive-OR: it uses logical function, where the both inputs are same then output is high otherwise the output is low.

Swap: swap operation, where the first half is shifted to the second half and second half is shifted to the first half.

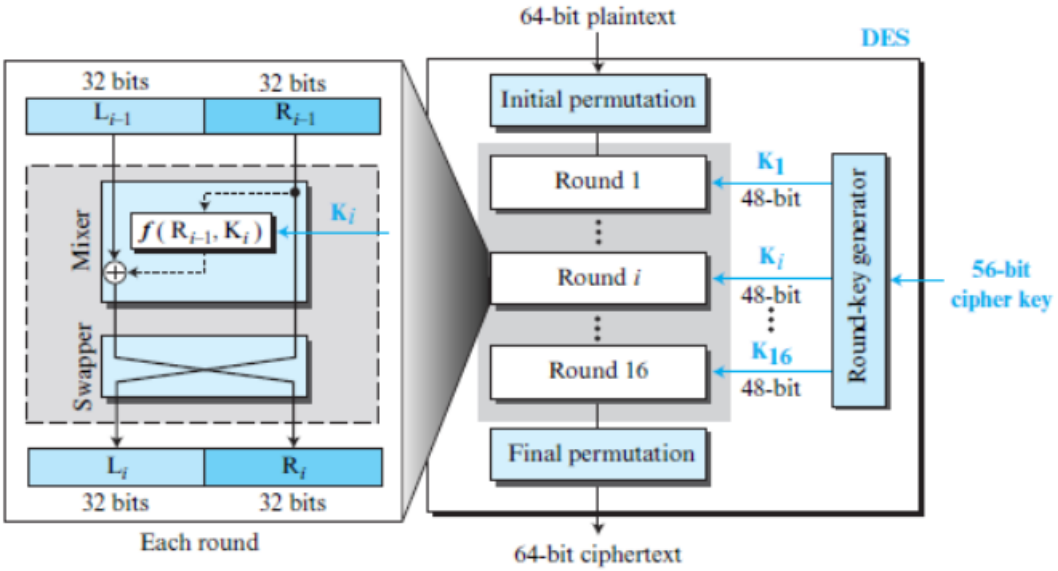
Split: it is reverse process to the swapping, where data is derived into two parts.

Combine: combine is the reverse process to the splitting, where two inputs are combined and produce a single output.

Q31-21. In Figure 31.10 in the text, why do we need an expansion P-box? Why can't we use a straight or a compression P-box?

Q31-21. Half of the input in DES is only 32 bits. The key is applied only to this 32-bit section. The two inputs to an XOR should be of the same size. Since the key is 48 bits, we need to expand the 32-bit section to a 48-bit section using an expansion P-box. Making the key for each round smaller jeopardizes the security of DES.

Q31-22. Figure 31.9 in the text shows that DES creates 16 different 48-bit keys, one for each round. Why do we need 16 different keys? Why can't we use the same key in each round?



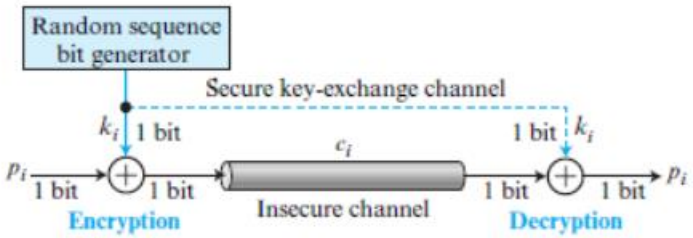
Refer figure 10.9, there are 16 different 48-bit keys are used, because the input the evry round is different to the other round. Therefore it produces different cipher text.

Therefore, the intruder shouldn't decrypt the message, when 16 different key used.

If every round used same key, then it produces the simple ciphertext, which is easily decrypted by the intruder.

Therefore, there are single key doesn't used for every round.

Q31-23. If the one-time pad cipher (Figure 31.12 in the text) is the simplest and most secure cipher, why is it not used all of the time?



Refer figure 10.12, one-time pad is secured cipher, because the key stream in one-time pad is used randomly. And performed EX-OR operation with the random bits to produce the output.

Therefore, intruder can't break the message until tries the all possible random key streams.

One-time pad cipher is most secured cipher but it is not used mostly for encryption operation because each and every time it requires a different random key stream and the main problem is the sharing the on-time pad between sender and receiver.

Q31-23. The one-time pad is an ideal, but a theoretical, cipher; it cannot be implemented easily because it requires that the sender and receiver have a secure channel to exchange the key stream. However, it is controversial; if there is a secure channel, the main message, in plaintext, can be sent through that channel.

Q31-24. If Alice and Bob need to communicate using asymmetric-key cryptography, how many keys do they need? Who needs to create these keys?

Asyemmtric keys used two different keys named public key and private key for the encryption and decryption operations.

Alice encrypted the message with the bob's public key, then bob decrypts the message with own private key.

The keys used in asymmetric keys are designed in key distribution center.

Q31-25. Why do you think asymmetric-key cryptography is used only with small messages.

Q31-25. To be safe, the keys used in asymmetric-key cryptography should be very large. This makes the calculation very long if the message is also long. Compare the short key of DES (56 bits) with the long key of RSA (500 to 1000 bits).

Q31-26. In an asymmetric public key cipher, which key is used for encryption? Which key is used for decryption?

a. public key **b.** private key

Asymmetric keys used two different keys named public key and private key for the encryption and decryption operations.

a.

Public key: Alice encrypted the message with the bob's public key. Therefore public key is used for the encryption.

b.

Private Key: bob decrypt the message with his private key. Therefore private key is used for the decryption.

Q31-27. In RSA, why can't Bob choose 1 as the public key e?

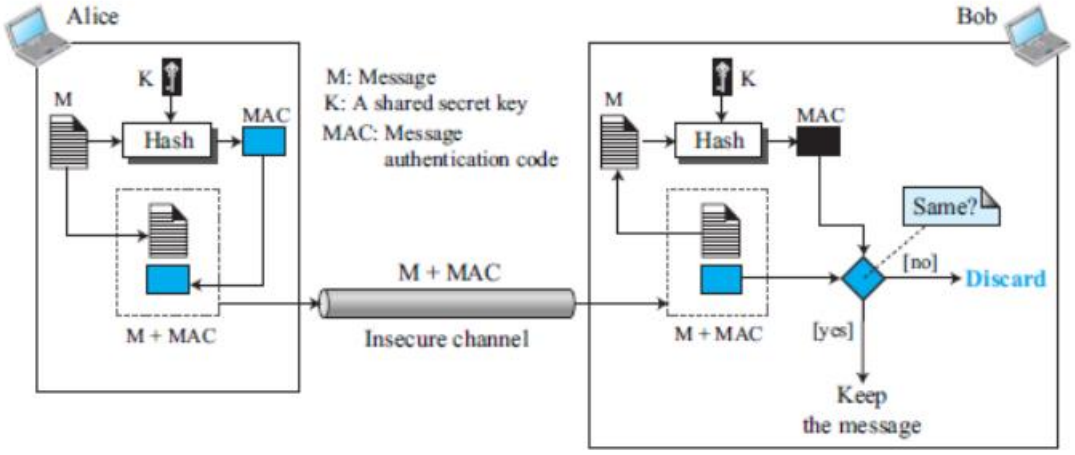
Q31-27. If $e = 1$, there is no encryption: $C = P^1 = P$. If Eve intercepts the ciphertext, she has the plaintext.

RSA has two exponents named *e* and *d*. *e* value shouldn't 1, because *e* should be releatively prime to the *p* and *q* values.

The value of *e* is used to produce the ciphertext, that is $C = P^e$. If value of *e* is 1 then the ciphertext is equal to the plaintext.

Therefore, bob can't choose the *e* as the public key and it's value as 1.

Q31-28. What is the role of the secret key added to the hash function in Figure 31.17 in the text (MAC)? Explain.



Message authentication code (MAC) used hash function and secret key to achieve the message integrity and message authentication.

Secret key is the only source to known about the originator of the message and its intended recipient.

When intended receiver receives the message, the secret key used to verify the message integrity.

If receiver doesn't known about the secret value, and the hash value is different then receiver doesn't known about the original sender of the message.

Q31-29. Distinguish message authentication and entity authentication.

Message authentication and entity authentication both are used for the securing the message.

Message authentication	Entity authentication
Message authentication is the process to verify the sender and recipient of the message, and it run when the new message is arrived.	Entity authentication should verify the all entities in the session until the communication is completed.
Message authentication shouldn't process in real time.	Entity authentication is processed only in real time.

Q31-29. Message authentication and entity authentication both authenticate the sender for the receiver. As their names indicate, however, message authentication authenticates the sender for a particular message, while entity authentication authenticates the sender for the entire session in which several messages can be sent. If the sender is sending only a single message, message authentication has the same effect as entity authentication; if a sender is sending several messages, one entity authentication authenticates the sender for all messages.

Q31-30. Alice signs the message she sends to Bob to prove that she is the sender of the message. Which of the following keys does Alice need to use?

a. Alice's public key **b.** Alice's private key

a.

If alice use her public key to prove the original sender:

If alice use her public key to encrypt the message. Then the message is not encrypted because everyone public key is known by the other people.

Therefore, option A is wrong answer.

b.

If alice use her private key to prove the original sender:

If alice use her private key to encrypt the message. Then the message is considered as a encrypted message because that message is only decrypted with the alice public key. Then bob known the alice is original sender of the message.

Therefore, **correct answer is option B.**

Q31-31. Alice needs to send a message to a group of fifty people. If Alice needs to use message authentication, which of the following schemes do you recommend?

a. MAC **b.** digital signature

Q31-31

a. The first choice is actually very inefficient and not practical because Alice needs to have a shared secret key between herself and each of the recipients. She also needs to create fifty separate MACs, one for each secret key.

b. Alice can use digital signature and sign only one message with her own private key. She then sends a copy of the message to each recipient. Each recipient needs to use Alice's public key to verify the message.

Q31-32. Which of the following services are not provided by digital signature?

a. message authentication **b.** confidentiality **c.** nonrepudiation

Digital signature:

Digital signature is the electronic signature, which is used to verify the sender and intended receiver of the message.

Message authentication is the process that should verify the sender and recipient of the message. Digital signature provides the message authentication.

Hence, the option A is wrong.

Non-repudiation: non- repudiation is the process, which states about the sender details. In digital signature it is the main component.

Hence, option c is wrong.

Confidentiality is the process that shouldn't disclose the information to unauthorized people. Digital signature shouldn't provide the confidentiality. To provide confidentiality message and signature should be encrypted.

Therefore, the **correct answer is option B.**

Q31-33. Assume Alice needs to send a confidential signed document to 100 people. How many keys does Alice need to use to prepare 100 copies if she uses asymmetric-key confidentiality? Explain.

Q31-33. Alice needs to use the public key of each recipient, which different for each of them. This means Alice needs to use 100 public keys.

Q31-34. In a club with 50 members, how many secret keys are needed to allow secret messages to be exchanged between any pair of members?

MAC:

Message authentication code (MAC) used hash function and secret key to achieve the message integrity and message authentication.

Secret key is the only source to known about the originator of the message and its intended recipient.

When intended receiver receives the message, the secret key used to verify the message integrity.

Refer the question, if the recipients are fifty members then there are 50 secret key are required. But between any pair of members a single key is used.

Therefore, a single secret key is enough to exchange a secret message between the pair of members.

Q31-35. A key distribution center (KDC) is designed to solve the problem of distributing _____ keys.

a. secret **b.** public **c.** private

Q31-35. A KDC is designed to solve the problem of *secret-key* distribution.

a.

Secret key: secret key is shouldn't known by the sender and receiver, therefore third party is designed the secret keys. The third party is referred as a key distribution centre (KDC).

Therefore, the **correct option is A**

b.

Public key: public key is the open key to all recipents because with the public key is decrypt the message. Certification authority is designed the public keys to all.

Therefore, the option B is wrong answer.

c.

Private Key: private key is used to encrypt the message; therefore it is designed by the self.

Therefore, option C is wrong answer.

Q31-36. A certification authority (CA) is designed to solve the problem of distributing _____ keys.

a. secret **b.** public **c.** private

a.

Secret key: secret key is shouldn't known by the sender and receiver, therefore third party is designed the secret keys. The third party is referred as a key distribution centre (KDC).

Therefore, the option A is wrong answer.

c.

Private Key: private key is used to encrypt the message; therefore it is designed by the self.

Therefore, option C is wrong answer.

b.

Public key: public key is the open key to all recipients because with the public key is decrypting the message. Certification authority is designed and distributing the public keys to all recipients.

Therefore, **the correct option is B**

=

31.5.3 Problems

P31-1. Define the type of attack in each of the following cases:

a. A student breaks into a professor's office to obtain a copy of the next test.

b. A student gives a check for $10 to buy a used book. Later the student finds out that the check was cashed for $100.

c. A student sends hundreds of e-mails per day to the school using a phony return e-mail address.

P31-1.

a. This is *snooping* (an attack to confidentiality). Although the contents of the test are not confidential on the day of the test, they are confidential before the test day.

b. This is *modification* (an attack to integrity). The value of the check is changed (from $10 to $100).

c. This is *denial of service* (an attack to availability). Sending so many e-mails may crash the server and the service may be interrupted.

Every organization should require security to the organization assets or information. There are three security aspects that should achieve the information security.

• Confidentiality: confidentiality is a security aspect that defines the organization information shouldn't share to unauthorized users.

• Integrity: integrity is a security aspect that defines the organization data or information shouldn't alter.

• Availability: Availability is a security aspect that defines the organization made information available to authorized users only.

a.

Refer given case, student obtain a copy of test paper. Therefore confidentiality of that test paper is lost.

Therefore, it is a confidentiality attack.

b.

Refer given case, check is modified as $100 but the actual price is different. Therefore

Data modification is occurred.

Therefore, it is data integrity attack.

C.

Refer given case, the availability of the school email service; therefore availability of that service is lost.

Therefore, it is availability attack.

P31-2. Use the additive cipher with k = 10 to encrypt the plaintext "book". Then decrypt the message to get the original plaintext.

In additive cipher, the plaintext and ciphertext are performed modulus operation with 26.

Given plain text is "book" and the k = 10

Step1: note down the values of plain text as per the figure 10.4,

b = 1

o = 14

o = 14

k = 10

step2: perform the addition operation initially with the K value and after modulus operation with 26 (refer example 10.1)

b = (1+10) mod 26 = 11

o = (14+10) mod 26 = 24

o = (14+10) mod 26 = 24

k = (10+10) mod 26= 20

step3: note down the step2 values and convert them as a ciphertext by using figure 10.4

11 = L

24 = Y

24 = Y

20 = U

Therefore, the ciphertext of the book is **LYYU.**

P31-3. Encrypt the message "this is an exercise" using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext.

P31-3.

a. The ciphertext is **NBCMCMUHYRYLWCMY** as shown below:

Plaintext			Encryption	Ciphertext		
t	→	19	**(19 + 20) mod 26 = 13**	13	→	N
h	→	07	**(07 + 20) mod 26 = 01**	01	→	B
i	→	08	**(08 + 20) mod 26 = 02**	02	→	C
s	→	18	**(18 + 20) mod 26 = 12**	12	→	M
i	→	08	**(08 + 20) mod 26 = 02**	02	→	C
s	→	18	**(18 + 20) mod 26 = 12**	12	→	M
a	→	00	**(00 + 20) mod 26 = 20**	20	→	U
n	→	13	**(13 + 20) mod 26 = 07**	07	→	H
e	→	04	**(04 + 20) mod 26 = 24**	24	→	Y
x	→	**23**	**(23 + 20) mod 26 = 17**	17	→	R
e	→	04	**(04 + 20) mod 26 = 24**	24	→	Y
r	→	17	**(17 + 20) mod 26 = 11**	11	→	L
c	→	02	**(02 + 20) mod 26 = 22**	22	→	W
i	→	08	**(08 + 20) mod 26 = 02**	02	→	C
s	→	18	**(18 + 20) mod 26 = 12**	12	→	M
e	→	04	**(04 + 20) mod 26 = 24**	24	→	Y

b. We can retrieve the plaintext by subtracting 20 from each ciphertext character using modulo 26 arithmetic as shown below:

Ciphertext			Decryption	Plaintext		
N	→	13	**(13 – 20) mod 26 = 19**	19	→	**t**
B	→	01	**(01 – 20) mod 26 = 07**	07	→	**h**
C	→	02	**(02 – 20) mod 26 = 08**	08	→	**i**
M	→	12	**(12 – 20) mod 26 = 18**	18	→	**s**
C	→	02	**(02 – 20) mod 26 = 08**	08	→	**i**
M	→	12	**(12 – 20) mod 26 = 18**	18	→	**s**
U	→	20	**(20 – 20) mod 26 = 00**	00	→	**a**
H	→	07	**(07 – 20) mod 26 = 13**	13	→	**n**
Y	→	24	**(24 – 20) mod 26 = 04**	04	→	**e**
R	→	17	**(17 – 20) mod 26 = 23**	23	→	**x**
Y	→	24	**(24 – 20) mod 26 = 04**	04	→	**e**
L	→	11	**(11 – 20) mod 26 = 17**	17	→	**r**
W	→	22	**(22 – 20) mod 26 = 02**	02	→	**c**
C	→	02	**(02 – 20) mod 26 = 08**	08	→	**i**
M	→	12	**(12 – 20) mod 26 = 18**	18	→	**s**
Y	→	24	**(24 – 20) mod 26 = 04**	04	→	**e**

P31-4. Atbash was a popular cipher among Biblical writers. In Atbash, "A" is encrypted as "Z", "B" is encrypted as "Y", and so on. Similarly, "Z" is encrypted as "A", "Y" is encrypted as "B", and so on. Suppose that the alphabet is divided into halves and the letters in the first half are encrypted as the letters in the second and vice versa. Find the type of cipher and key. Encipher the plaintext "an exercise" using the Atbash cipher.

Refer question, it is a substitution cipher because characters are replaced with another characters.

Atbash cipher format: the letters are divided into two halves. The first half is replaced with the second half vice versa.

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Given plaintext is "an exercise", the cipher text is

a = z

n = m

e = v

x = c

e = v

r = i

c = x

i = r

s = h

e = v

therefor, the cipher text of the plain text "an exercise" is **zmvcvixrhv.**

P31-5. A substitution cipher does not have to be a character-to-character transformation. In a Polybius cipher, each letter in the plaintext is encrypted as two integers. The key is a 5×5 matrix of characters. The plaintext is the character in the matrix, the ciphertext is the two integers (each between 1 and 5) representing row and column numbers. Encipher the message "An exercise" using the Polybius cipher with the following key:

	1	2	3	4	5
1	z	q	p	f	e
2	y	r	o	g	d
3	x	s	n	h	c
4	w	t	m	i / j	b
5	v	u	l	k	a

P31-5. The plaintext and ciphertext are shown below, ignoring the space:

Plaintext	Ciphertext
an exercise	**(5, 5), (3, 3), (1, 5), (3, 1), (1, 5), (2, 2), (3, 5), (4, 4), (3, 2), (1, 5)**

P31-6. Alice can use only the additive cipher on her computer to send a message to a friend. She thinks that the message is more secure if she encrypts the message two times, each time with a different key. Is she right? Defend your answer.

P31-7. One of the attacks an intruder can apply to a simple cipher like an additive cipher is called the *ciphertext* attack. In this type of attack, the intruder intercepts the cipher and tries to find the key and eventually the plaintext. One of the methods used in a ciphertext attack is called the *brute-force* approach, in which the intruder tries several keys and decrypts the message until the message makes sense. Assume the intruder has intercepted the ciphertext "UVACLYZLJBYL". Try to decrypt the message by using keys beginning with 1 and continuing until a plaintext appears that makes sense.

P31-7. We apply the key = 1, 2, 3, 4, 5, 6, and 7 to find the plaintext.

Ciphertext	Key	Plaintext
UVACLYZLJBL	**1**	tuzbkxeykiaxy
UVACLYZLJBL	**2**	styajwdxjhzwj
UVACLYZLJBL	**3**	rsxzivcwigyvi
UVACLYZLJBL	**4**	qrwyhubvhfxuh
UVACLYZLJBL	**5**	pqvxgtaugewtg
UVACLYZLJBL	**6**	opuwfsztfdvsf
UVACLYZLJBL	**7**	**notverysecure**

P31-8. Another method used in a ciphertext attack (see previous problem) is called the *statistical* approach, in which the intruder intercepts a long ciphertext and tries to analyze the statistics of the characters in the ciphertext. A simple cipher like the additive cipher does not change the statistics of the characters because encryption is one-to-one. Assume the intruder has intercepted the following ciphertext and the most common character in an English plaintext is the character "e". Use this knowledge to find the key of the cipher and decrypt the ciphertext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASV
XLQSVILYVVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

P10-8. Since the ciphertext is long, we first find the frequency of each character. In our finding, the frequency of letter I is the highest (14). If we assume that the character "e" in the plaintext is encrypted to character "I", then the key is 4. We try to decrypt the message with k = 4, from which we get something that makes sense. We have added spaces between the words for readability, although there are no spaces in the ciphertext.

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

---

P31-9. In a transposition cipher the encryption and decryption keys are often represented as two one-dimension tables (arrays) and the cipher is represented as a piece of software (a program).

a. Show the array for the encryption key in Figure 31.6 in the text. Hint: the value of each element can show the input-column number; the index can show the output-column number.

b. Show the array for the decryption key in Figure 31.6 in the text.

c. Explain, given the encryption key, how we can find the decryption key.

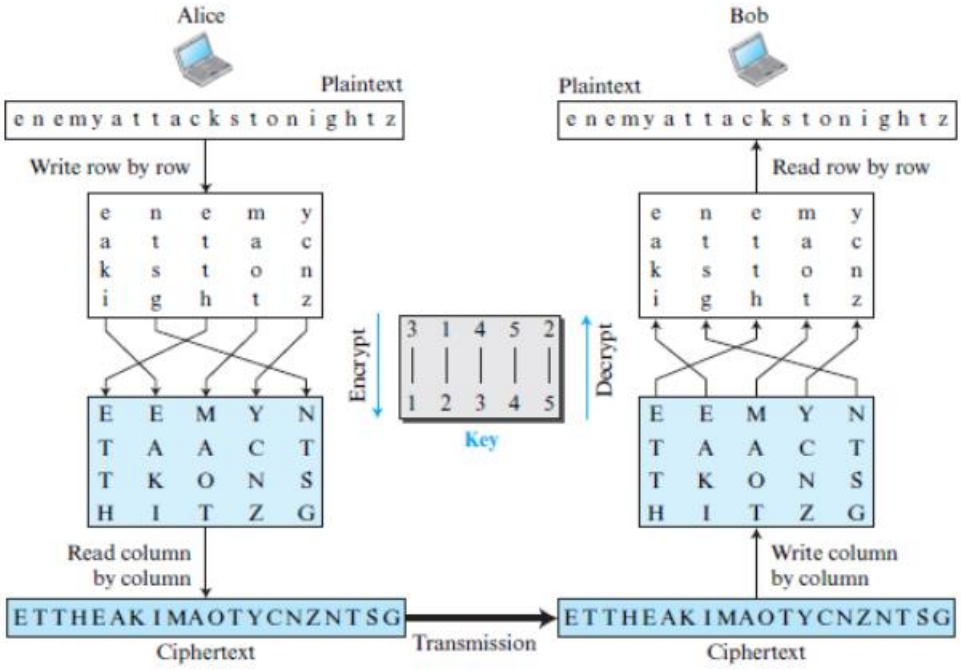


Figure 31.6

P10-9. The content of each element represents the input column number; the index represents the output column number.

a. The encryption key can be represented as shown below.

b. The decryption key can be represented as shown below. Note that the indexes are sorted.

2	5	1	3	4
1	2	3	4	5

c. We can first exchange the content and index and then sort the array according to the index. For example, to get the decryption key from the encryption key in part a, we can first swap the contents and the index and then sort it according to the index.

1: Swap

1	2	3	4	5
3	1	4	5	2

2: Sort

2	5	1	3	4
1	2	3	4	5

P31-9. The content of each element represents the input column number; the index represents the output column number.

a. The encryption key can be represented as shown below.

3	1	4	5	2
1	2	3	4	5

b. The decryption key can be represented as shown below. Note that the indexes are sorted.

2	5	1	3	4
1	2	3	4	5

c. We can first exchange the content and index and then sort the array according to the index. For example, to get the decryption key from the encryption key in part a, we can first swap the contents and the index and then sort it according to the index.

1: Swap

1	2	3	4	5
3	1	4	5	2

2: Sort

2	5	1	3	4
1	2	3	4	5

P31-10. The circular shift operation is one of the components of the modern block ciphers.

a. Show the result of a 3-bit circular left shift on the word $(10011011)_2$.

b. Show the result of a 3-bit circular right shift on the result of part *a*.

c. Compare the result of part *b* with the original word in part *a* to show that shift right and shift left operations are inverses of each other.

Circular left shift: Bits (n) in the word is shifted to the left with the k positions.

a.

Given word n = 10011011 and k = 3;

3-bit left circular shift = 11011001

b.

Circular right shift: Bits (n) in the word is shifted to the right with the k positions.

Word n = 11001101 and k = 3;

3-bit right circular shift = 10011011

c.

Yes. Shift right and shift left operations are inverse to each other, because initially original word perform the left shift operation. After result of the left shift is performed right shift operation then the result is original word.

Therefore, the left shift and right shift are inverse to each other.

P31-11. The swap operation is one of the components of the modern block ciphers.

a. Swap the word $(10011011)_2$.

b. Swap the word resulting from part *a*.

c. Compare the results of part *a* and part *b* to show that swapping is a self-invertible operation.

P31-11.

a. Swap of (**1001**1011) is (1011**1001**).

b. Swap of (1011**1001**) is (**1001**1011).

c. The original word in part *a* and the result of part *b* are the same, which shows that swapping is a self-invertible operation.

P31-12. A very common operation in block ciphers is the XOR operation. Find the results of the following operations. Interpret the results.

a. (01001101) ⊕ (01001101)

b. (01001101) ⊕ (00000000)

X-OR operation: if the inputs are same then the result is low (0) otherwise the result is high (1).

a.

$$\begin{array}{r} 01001101 \\ 01001101 \\ \hline 00000000 \end{array}$$

The result is 00000000 because two inputs are same therefore the result is **00000000.**

b.

$$\begin{array}{r} 01001101 \\ 00000000 \\ \hline 01001101 \end{array}$$

The result is one of the input (01001101) because that input is performed X-OR operation with the 00000000. If any of the input (*a*) perform X-OR operation with the low input (all 0's) then the result is *a*.

P31-13. Assume you want to write a program to simulate the permutation boxes in Figure 31.8 in the text.

a. Show how you represent each box as a table.

b. Show the inversion of each box as a table.

P10-13. As we said about the keys for the transposition cipher, permutation boxes (P-boxes) can be represented by a table in which the contents of each element shows the input number and the index show the output number.

a. A straight permutation box of n x n size is a table of n entries in which each entry is unique. A compression permutation of n x m size is a table of m entries in which the blocked inputs are not shown. An expansion permutation of n x m size is a table of n entries in which some of the entries are repeated. The following shows the three tables for permutation boxes in Figure 10.8 in the text. We have not shown the indexes.

b. The compression and expansion boxes have no inversions because the number of inputs and outputs is not equal. Only the straight boxes can be inverted. We first need to swap the contents and the indexes and then sort the result according to the index. The following shows the inversion of a straight permutation box used in the decryption.

P31-13. As we said about the keys for the transposition cipher, permutation boxes (P-boxes) can be represented by a table in which the contents of each element shows the input number and the index show the output number.

a. A straight permutation box of $n \times n$ size is a table of n entries in which each entry is unique. A compression permutation of $n \times m$ size is a table of m entries in which the blocked inputs are not shown. An expansion permutation of $n \times m$ size is a table of n entries in which some of the entries are repeated. The following shows the three tables for permutation boxes. We have not shown the indexes.

2	5	4	1	3
1	2	3	4	5

Straight

1	3	5
1	2	3

Compression

1	3	3	1	2
1	2	3	4	5

Expansion

b. The compression and expansion boxes have no inversions because the number of inputs and outputs is not equal. Only the straight boxes can be inverted. We first need to swap the contents and the indexes and then sort the result according to the index. The following shows the inversion of a straight permutation box used in the decryption.

1: Original

2	5	4	1	3
1	2	3	4	5

$\rightarrow$

2: Swap

1	2	3	4	5
2	5	4	1	3

$\rightarrow$

3: Reorder

4	1	5	3	2
1	2	3	4	5

P31-14. Assume we have a keyless substitution box (S-box) with three inputs (x_1, x_2, and x_3) and two outputs (y_1 and y_2). The relation between the inputs and outputs is defined as follows ($\oplus$ means XOR):

$$y_1 = x_1 \oplus x_2 \oplus x_3 \qquad y_2 = x_1$$

What is the output if the input is (110)? What is the output if the input is (001)?

EX-OR operation: if the inputs are same then the result is low (0) otherwise the result is high (1).

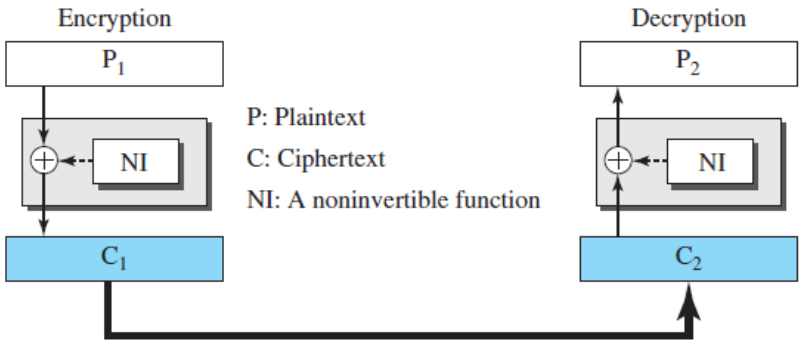
Refer question, there are three inputs x_1, x_2, x_3 and two outputs y_1, y_2 .where $y_1 = x_1 \oplus x_2 \oplus x_3$ and $y_2 = x_1$.

x_1	x_2	x_3	y_1,	y_2
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	0
1	0	0	1	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

- If the input is 110 then the output y_1, = 0 and y_2 = 1
- If the input is 001 then the output y_1, = 1 and y_2 = 0.

P31-15. Each round in a block cipher should be invertible to make the whole block invertible. Modern block ciphers use two approaches to achieve this. In the first approach, each component is invertible; in the second approach some components are not invertible but the whole round is invertible using what is called a *Feistel cipher*. This approach is used in DES, described in the text. The trick in the Feistel cipher is to use the XOR operation as one of the components. To see the point, assume that a round is made of a noninvertible component, NI, and an XOR operation, as shown in Figure 31.29. Prove that the whole round is invertible, which means that the plaintext can be recovered from the ciphertext. Hint: use XOR properties ($x \oplus x = 0$ and $x \oplus 0 = x$).

Figure 31.29 *Problem P31-15*



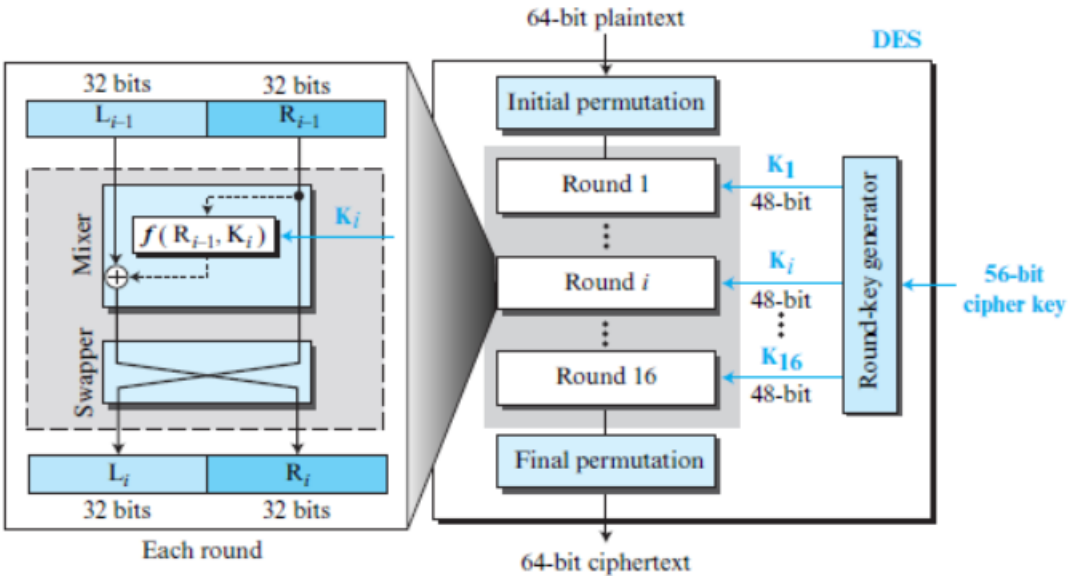
P31-15. le. In other words, we need to show that the component NI is eliminated in the decryption process.

Encryption: $C1 = P1 \oplus NI$

Decryption: $P2 = C2 \oplus NI = C1 \oplus NI = (P1 \oplus NI) \oplus NI = P1 \oplus (NI \oplus NI)$

$P2 = P1 \oplus (0) = P1$

P31-16. In Figure 31.9 we have a swapper in each round. What is the use of this swapper?



Swapper: swapper is used to transpose bits like second half into first half and first half into second half (refer figure 10.8).

Refer figure 10.9, where the feistel cipher is performed, that is the bits are performed X-OR operation with the some key material and after bits are swapped.

If swapper may not use in this case, then there is no use to performing feistel cipher functioning, then the security of the algorithm may lost because the security of the algorithm is depends in feistel structure.

P31-17. In Figure 31.9, we have two straight permutation operations: *initial permutation* and *final permutation*. Experts believe these operations are useless and do not help to make the cipher stronger. Can you find the reason for this statement?

P31-17. Both operations are keyless and the operations are predefined. If Eve, the intruder, wants to break the cipher, she can easily simulate them.

P31-18. The key in DES is 56 bits. Assume Eve, the intruder, tries to find the key using a brute-force attack (tries all of the keys one by one). If she can try one million keys (almost 2^{20}) in each second (using a powerful computer), how long does it take to break the code?

> **P10-18.** The number of possible keys is 256. Eve, on average, needs to try half of the keys or 255 keys. Testing 220 keys in each second, it takes 235 seconds or almost 1089 years. This means DES cannot be broken by a brute-force attack.

P31-19. Assume Bob, using the RSA cryptosystem, selects $p = 11$, $q = 13$, and $d = 7$, which of the following can be the value of public key e?

a. 11 **b.** 103 **c.** 19

P31-19. We first find the value of $\phi = (p - 1) \times (q - 1) = 120$. We then need to see which of the e values satisfies the relation $(d \times e) \bmod 120 = 1$. We will find that 103 is the answer.

a. $(7 \times 11) \bmod 120 = 77$

b. $(7 \times 103) \bmod 120 = 721 \bmod 120 = 1$ **(Answer is 103)**

c. $(7 \times 19) \bmod 120 = 133 \bmod 120 = 13$

P31-20. In RSA, given $p = 107$, $q = 113$, $e = 13$, and $d = 3653$, encrypt the message "THIS IS TOUGH" using 00 to 26 (A: 00 and space: 26) as the encoding scheme. Decrypt the ciphertext to find the original message.

P10-20. The plaintext is: 190708182608182619142006O7. Since the modulus, which is n = p × q = 12091, is five digits long, we use 4-digit plaintext to make P smaller than n. We add 26 (space) to the end to make the last block also four digits. We use five-digit blocks for ciphertext. The ciphertext C is never greater than n because the calculation is in modulo n.

a. To create the ciphertext we use C = Pe mod 12091.

Plaintext	Encryption	Ciphertext
$P_1 = 1907$	$1907^{13} \bmod 12091 = 10614$	$C_1 = 10614$
$P_2 = 0818$	$0818^{13} \bmod 12091 = 07787$	$C_2 = 07787$
$P_3 = 2608$	$2608^{13} \bmod 12091 = 01618$	$C_3 = 01618$
$P_4 = 1826$	$1826^{13} \bmod 12091 = 10717$	$C_4 = 10717$
$P_5 = 1914$	$1914^{13} \bmod 12091 = 04084$	$C_5 = 04084$
$P_6 = 2006$	$2006^{13} \bmod 12091 = 06558$	$C_6 = 06558$
$P_7 = 0726$	$0726^{13} \bmod 12091 = 07077$	$C_7 = 07077$

b. To create the ciphertext we use P = Cd mod 12091. The original message can be recovered from the plaintext two digits at a time.

Ciphertext	Encryption	Plaintext
$C_1 = 10614$	$10614^{3653} \bmod 12091 = 1907$	$P_1 = 1907$
$C_2 = 07787$	$07787^{3653} \bmod 12091 = 0818$	$P_2 = 0818$
$C_3 = 01618$	$01618^{3653} \bmod 12091 = 2608$	$P_3 = 2608$
$C_4 = 10717$	$10717^{3653} \bmod 12091 = 1826$	$P_4 = 1826$
$C_5 = 04084$	$04084^{3653} \bmod 12091 = 1914$	$P_5 = 1914$
$C_6 = 06558$	$06558^{3653} \bmod 12091 = 2006$	$P_6 = 2006$
$C_7 = 07077$	$07077^{3653} \bmod 12091 = 0700$	$P_7 = 0726$

P31-21. A cryptographic hash function needs to be *second preimage resistant,* which means that given the message M and the message digest *d,* we should not be able to find any other message, M′, whose digest is *d*. In other words, two different messages cannot have the same digest. Based on this requirement, show that a traditional checksum in the Internet cannot be used as a hash function.

Message digest value also referred as hash value, Hash value is created by using the secret key.

For every message, there are new secret key is used to produce the new message digest value.

Refer question, message M has some digest value. With that digest value intruder shouldn't find the another message M', because One hash value is used only once because the secret key is used only once.

P31-21. Two messages can easily have the same traditional checksum. For example, two different messages in which two bytes are swapped will have the same traditional checksum because the calculation of a traditional checksum is independent from the position of the bytes. This means a traditional checksum cannot be used as a cryptographic hash function.

P31-22. Explain why private-public keys cannot be used in creating a MAC.

Message authentication code (MAC) used hash function and secret key to achieve the message integrity and message authentication.

Secret key is the only source to known about the originator of the message and its intended recipient.

When intended receiver receives the message, the secret key used to verify the message integrity.

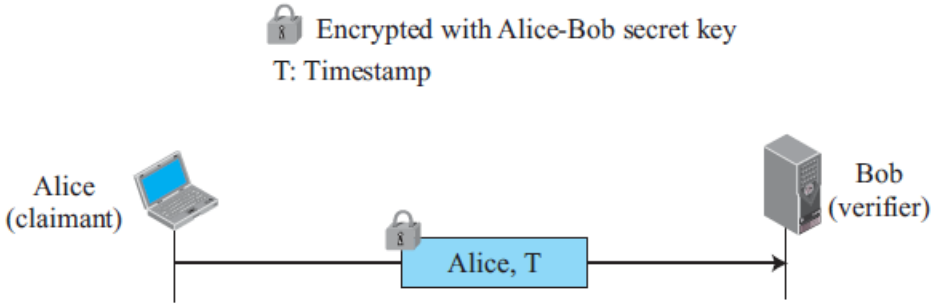
If receiver doesn't known about the secret value, and the hash value is different then receiver doesn't known about the original sender of the message.

The public key and private doesn't used to create MAC, because public key is used to the hash value then everyone easily decrypt the message because public key is open to all.

If private key is used to create hash value then also message easily decrypted, because one hash value is used only once because the secret key is used only once. If private key is used after the first time message can be decrypted.

P31-23. The nonce in Figure 31.22 is to prevent a replay of the third message. Eve cannot replay the third message and pretend that it is a new request from Alice, because when Bob receives the response, the value of R_B is not valid anymore. This means that we can eliminate the first and the second message if we add a timestamp to the diagram. Show a new version of Figure 31.22 using a timestamp.

P31-23. The following shows the new diagram. The timestamp, T, included in the only message does the job of the challenge message and R_B.



P31-24. Explain why encryption is used in the second message (from Bob to Alice) in Figure 31.23, but signing is done in the third message (from Alice to Bob) in Figure 31.24.

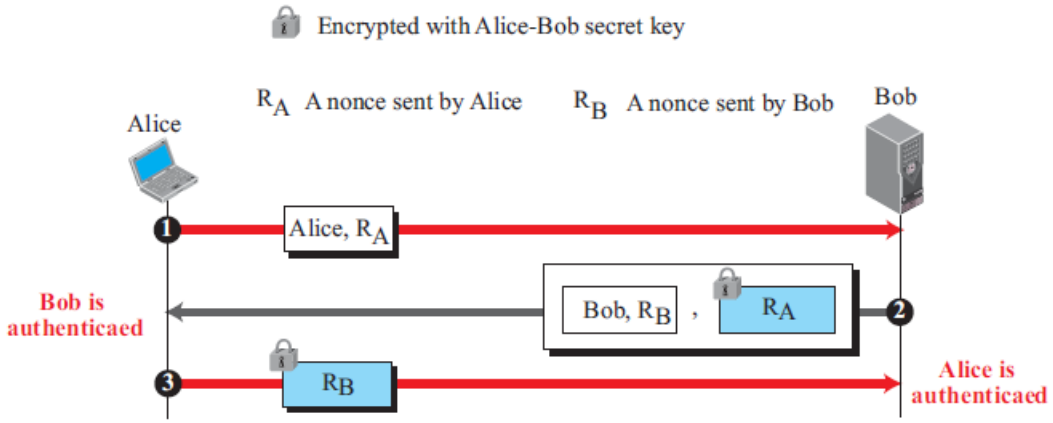
Refer figure 10.23, the second message is encrypted which is transmitted from bob to alice.in this message encryption used to verify the entity authentication.

Entity authentication is the process that will verify the total entities, which are transmitted during the session.

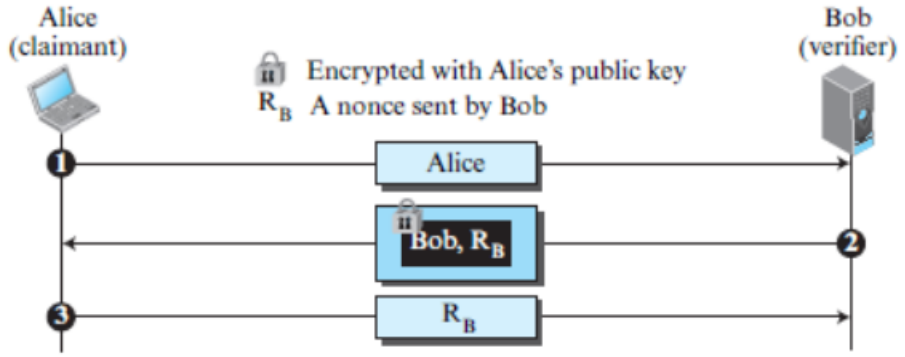
Refer figure 10.24, the third message is signed which is transmitted from the alice to bob, because the message is signed in the purpose of the response.

P31-25. Figure 31.22 shows a unidirectional authentication that authenticates Alice for Bob. Change this figure to provide bidirectional authentication: to authenticate Alice for Bob and then Bob for Alice.

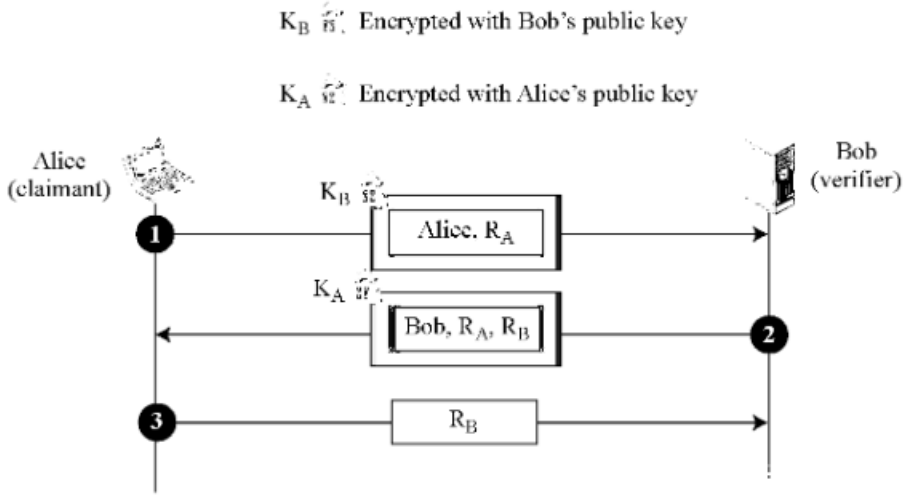
P31-25. The following shows one simple solution. It shows the idea, but it is vulnerable to some attacks. There are some better but more complicated solutions. In the first message, Alice sends her identification and her nonce. In the second message, Bob sends his identification, his nonce, and Alice's encrypted nonce. Alice's nonce is encrypted with the shared secret key. When Alice receives this message and decrypts her nonce, Bob is authenticated for her because only Bob can encrypt Alice's nonce with the shared secret key. In the third message, Alice sends Bob's encrypted nonce. When Bob receives this message and decrypts his nonce, Alice is authenticated for Bob because only Alice can encrypt Bob's nonce with the shared secret key.



P31-26. Change Figure 31.23 to allow bidirectional authentication. Alice needs to be authenticated for Bob and Bob for Alice.

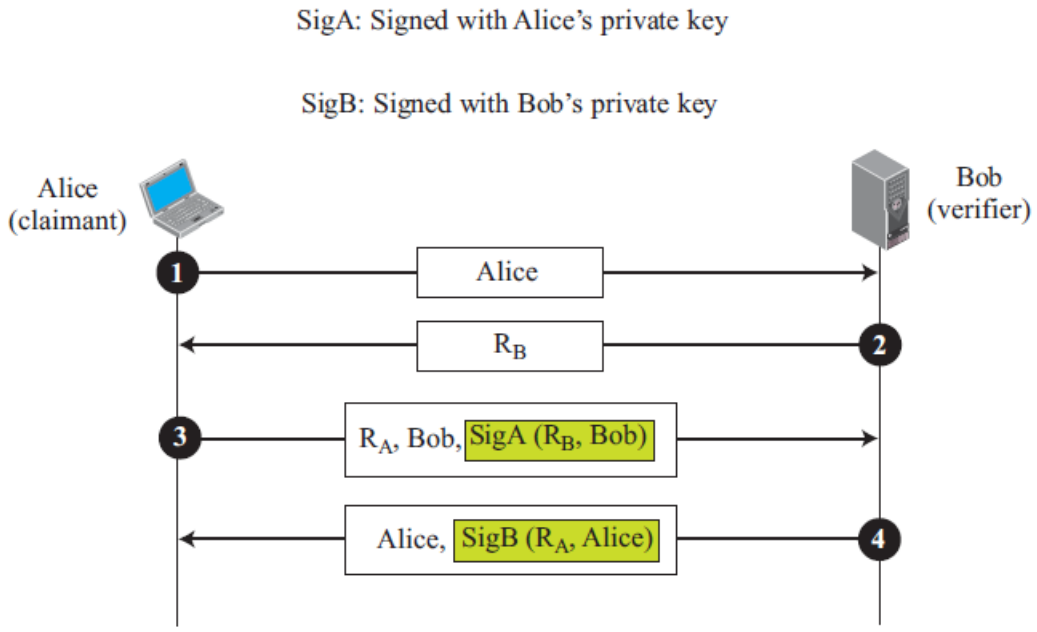


P10-26. The following shows a new diagram. Two nonces are used to achieve bidirectional authentication.



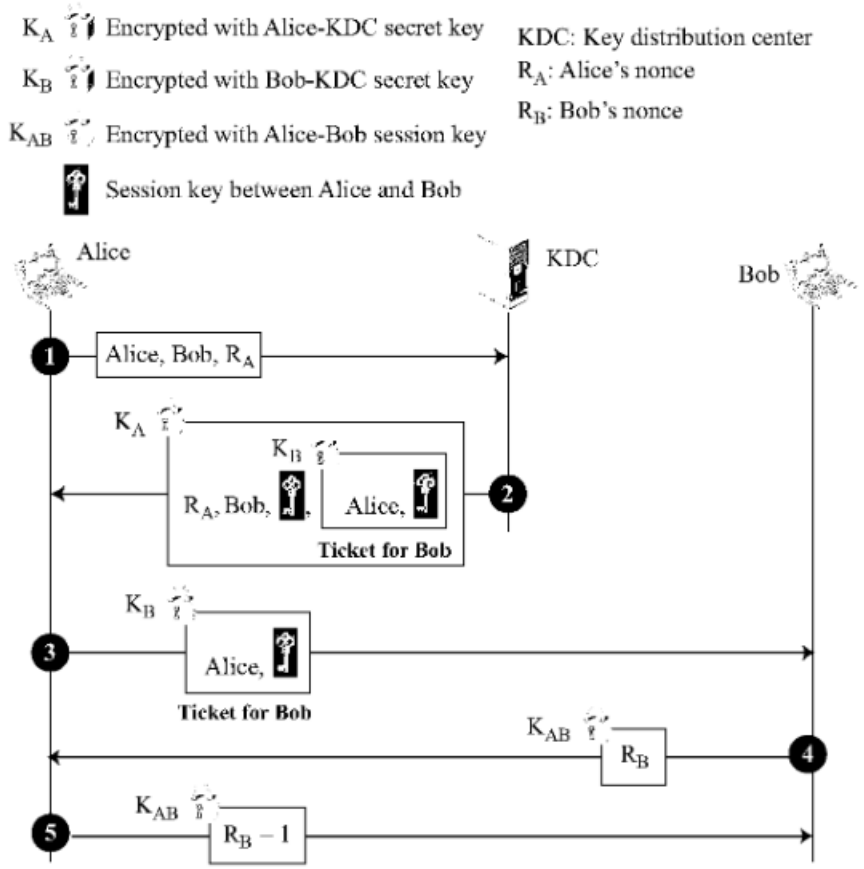
P31-27. Change Figure 31.24 to allow bidirectional authentication. Alice needs to be authenticated for Bob and Bob for Alice.

P31-27. The following shows the new diagram. Two nonces and two keys are used to achieve bidirectional authentication.



P31-28. You may have noticed that there is a flaw in Figure 31.26. Eve, the intruder, can replay the third message and, if she can somehow get access to the session key, can pretend to be Alice and exchange messages with Bob. The problem can be avoided if both Alice and Bob use two nonces. Remember that nonces have a lifetime and their main purpose is to prevent replaying. Modify Figure 31.26 to add two nonces.

P10-28. The following shows a solution:



P31-29. Assume we have a very simple message digest. Our unrealistic message digest is just one number between 0 and 25. The digest is initially set to 0. The cryptographic hash function adds the current value of the digest to the value of the current character (between 0 and 25). Addition is in modulo 26. What is the value of the digest if the message is "HELLO"? Why is this digest not secure?

P31-29. The following shows the value of the digest after hashing each character of the text. The method is not secure because the digest is always between 0 and 25. The total number of possible digests is N = 26.

Initial value of the digest:	$d = 00$
After hashing the first character (H: 07):	$d = (00 + 07) \bmod 26 = 07$
After hashing the second character (E: 04):	$d = (07 + 04) \bmod 26 = 11$
After hashing the third character (L: 11):	$d = (11 + 11) \bmod 26 = 22$
After hashing the fourth character (L: 11):	$d = (22 + 11) \bmod 26 = 07$
After hashing the fifth character (O: 14):	$d = (07 + 14) \bmod 26 = 21$

P31-30. To understand the concept of secret-key distribution, assume a small private club has only 100 members (excluding the president). Answer the following questions:

a. How many secret keys are needed if all members of the club need to send secret messages to each other?

b. How many secret keys are needed if everyone trusts the president of the club? If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member.

c. How many secret keys are needed if the president decides that the two members who need to communicate should contact him first. The president then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.

a.

Refer question, there are 100 members in the club and one president. That is totally 101 members in the club, If everyone needs to send the document to all club members then totally 10000 ((101-1)*100) secret keys required, because every club member needs to send 99 club members and one president.

Therefore, totally 10000 secret keys are required.

b.

Initially there are 100 secret keys are required that is used to send the president. And after that president use another 100 keys to send the every member.

Therefore, totally 200 secret keys are required.

c.

Initially there are 50 temporary secret keys are required, because every two members in the club can share a single temporary key.

Therefore, 50 secret keys are required.

Ch 32 Summary

- IP Security (IPSec) is a collection of protocols designed by the IETF to provide security for a packet at the network level .

- IPSec operates in transport or tunnel mode .

- IPSec defines two protocols: Authentication Header (AH) Protocol and Encapsulating Security Payload (ESP) Protocol .

- IPSec creates a connection-oriented association at the top of the connectionless IP protocol to be able to provide security .

- A transport-layer security protocol provides end-to-end security services for applications that use the services of a connection-oriented transport-layer protocol such as TCP .

- Two protocols are dominant today for providing security at the transport layer: Secure Sockets Layer (SSL) and Transport Layer Security (TLS) .

- We discussed SSL in this chapter; TLS is similar .

- Although SSL or TLS can provide security for applications that use the service of connection-oriented protocols such as TCP, the e-mail application is exceptional because the application uses a one-way communication .

- The Pretty Good Privacy (PGP), invented by Phil Zimmermann, provides e-mail with privacy, integrity, and authentication .

- Another security service designed for electronic mail is Secure/Multipurpose Internet Mail Extension (S/MIME) .

- A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet .

- It is designed to forward some packets and filter others .

- A firewall is usually classified as a packet-filter firewall or a proxy firewall .

32.6.2 Questions

Q32-1. Why does IPSec need a security association?

> **Q32-1.** IPSec needs a set of security parameters before it can be operative. In IPSec, the establishment of the security parameters is done via a mechanism called *security association (SA)*.

Q32-2. How does IPSec create a set of security parameters?

> A set of security parameters between any two entities is created using the security association. Security association uses three protocols: IKE, Oakley, and SKEME to create a security association between two parties or a security association database between group of users. Internet Key Exchange's creates security associations for IPSec.

Q32-3. What are the two protocols defined by IPSec?

> **Q32-3.** The two protocols defined by IPSec for exchanging datagrams are *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*.

Q32-4. What does AH add to the IP packet?

The Authentication Header (AH) protocol adds an AH header that contains next header, payload length, security parameter index, sequence number, Reserved and digest fields.

Q32-5. What does ESP add to the IP packet?

The Encapsulating Security Payload (ESP) protocol adds an ESP header, ESP trailer, and the authentication data. The ESP header contains the security parameter index and the sequence number. The ESP trailer contains the padding, the padding length, and the next header.

Q32-5. The *Encapsulating Security Payload (ESP)* protocol adds an ESP header, ESP trailer, and the digest. The ESP header contains the security parameter index and the sequence number fields. The ESP trailer contains the padding, the padding length, and the next header fields. Note that the digest is a field separate from the header or trailer.

Q32-6. Are both AH and ESP needed for IP security? Why or why not?

Both AH and ESP needed for IP security because those protocols are used to provide authentication or encryption or both for the packets at the IP level. ESP has more functionality than AH and ESP was developed after AH was already in use.

Q32-7. What are the two protocols discussed in this chapter that provide security at the transport layer?

The two protocols dominate to provide security at the transport layer is:

1. Secure Socket Layer : this protocol designed to provide security and compression service to data generated from the application layer and

2. Transport Layer Security: It is the IETF standard version of SSL.

Q32-7. The two dominant protocols for providing security at the transport layer are the *Secure Sockets Layer (SSL)* Protocol and the *Transport Layer Security (TLS)* Protocol. The latter is actually an IETF version of the former.

Q32-8. What is IKE? What is its role in IPSec?

Internet Key Exchange (IKE): IKE is a protocol designed to create both inbound and outbound security associations in SADB's.

Q32-9. What is the difference between a session and a connection in SSL?

Q32-9. A session between two systems is an association that can last for a long time; a connection can be established and broken several times during a session. Some of the security parameters are created during the session establishment and are in effect until the session is terminated. Some of the security parameters must be recreated (or occasionally resumed) for each connection.

Q32-10. How does SSL create a set of security parameters?

Whenever two parties involved in data exchange needs to have a set of parameters for each association.SSL has similar goal, but a different approach. There are no SA's, but there are cipher suites and cryptographic secrets that together make the security parameters.

Q32-11. What are the names of the protocols, discussed in this chapter, that provide security for e-mail?

One protocol provides security for email system is Pretty Good Privacy (PGP).PGP was invented by Phil Zimmerman to provide privacy, integrity and authentication in e-mail.

Q32-11. One of the protocols designed to provide security for email is *Pretty Good Privacy (PGP)*. PGP is designed to create authenticated and confidential e-mails.

Q32-12. How does PGP create a set of security parameters?

In PGP, the security parameters need to be sent with message. The sender of the message needs to include the identifiers of the algorithms used in the message as well as the values of the keys.

Q32-13. What is the purpose of the Handshake Protocol in SSL?

Q32-13. The *Handshake Protocol* establishes a cipher set and provides keys and security parameters. It also authenticates the server to the client and the client to the server, if needed.

Q32-14. What is the purpose of the Record Protocol in SSL?

The record protocol carries messages from the upper layer. It carries messages from three other protocols as well as the data coming from the application layer. Messages from the recorded protocol are payloads to the transport layer.

Q32-15. What is the purpose of a firewall?

Q32-15. A *firewall* is a security mechanism that stands between the global Internet and a network. A firewall selectively filters packets.

Q32-16. What are the two types of firewalls?

Types of firewalls: a firewall is usually classified into two types. They are:

1. Packet-filter firewall: A firewall can be used as a packet filter. It can be forward or block packets based on the information in the network layer and transport layer headers. and
2. Proxy-based firewall: A proxy firewall filters at the application.

Q32-17. What is a VPN and why is it needed?

A Virtual Private Network (VPN) provides privacy for LAN's that must communicate through the global internet. A technology that creates a network that is physically public, but virtually private.

Q32-17. A *VPN* is a virtual network that uses VPN technology.The technology allows an organization to use the global Internet yet safely maintain private internal communication.

Q32-18. How do LANs on a fully private internet communicate?

The Direct communication is done between LANs communicating on WAN using routers. The router, installed on the leased line, reads the headers on each packet of data that passes through the WAN, sending it to the proper LAN. When the packet arrives at the LAN, a device called a switch sends the data packet on to the correct machine. Hence, the WAN acts like an interface between LANs for long-distance communication. A WAN that runs on a leased line is a private WAN, as there is no public traffic on the line.So, LANs on a fully private internet can communicate through routers and leased lines.

32.6.3 Problems

P32-1. Host A and host B use IPSec in the transport mode. Can we say that the two hosts need to create a virtual connection-oriented service between them? Explain.

P32-1. When IPSec is used in the transport mode, two parties need to first create cryptographic secrets between themselves before exchanging secure data. This cannot be done using the connectionless service provided by IP. The two parties need to create a virtual connection-oriented service between themselves over the services provided by IP. This is done using the Security Association (SA) described in the text.

P32-2. When we talk about authentication in IPSec, do we mean *message authentication* or *entity authentication*? Explain.

IPSec:

• This can be utilized for end-to-end communication.

• For instance, in order to communication among both client and a server or between workstation and a gateway (This comprises with the host).

• A decent illustration can be an encrypted Telnet or remote host session from a workstation to a server.

• This is generally utilized while another tunneling protocol like **GRE (Generic Routing Encapsulation)** is utilized to first wrap up the IP information datagram at that point IPSec is utilized to ensure the GRE tunnel datagram.

• This secures the **GRE (Generic Routing Encapsulation)** tunnel activity in transport mode.

• Transport mode gives the security of information, otherwise called IP payload, and comprises of TCP/UDP header, information through an **AH (Authentication Header)** or **ESP (Encapsulating Security Payload)** header.

• The IP payload is wrapped up by the IPSec headers and trailers.

• The first IP headers stay in place, aside from that the IP protocol field can be transformed to ESP (50) or AH (51).

Authentication:

• Authentication is the process of recognizing an individual, with the help of a username and password.

• In the security system, Authentication is different from authorization, which is the way toward giving the individual access system objects in the view of identity.

• Verification just guarantees that the individual is who users(he/she) claims to be, however says nothing in regards to the access rights of the individual.

IPSec utilizes the both types of the Authentication which name is as follows:

• **Message Authentication:**

• This is also called Message integrity.

• Message Authentication save in both AH (Authentication Header) and ESP (Encapsulating Security Payload).

• In this data can be made and forward by the sender and can be checked by the receiver.

• **Entity Authentication:**

• This is also called data source authentication.

• This is also save in both AH (Authentication Header) and ESP (Encapsulating Security Payload).

• In this Security Association and keyed hash digest of data can be forward by the sender.

• IPSec gives the both types of authentication which is entity authentication and message authentication.

• So, the two entities can be authenticated for each other with the help of ISAKMP (Internet Security Association and Key Management Protocol).

• In IPSec, the ISAKMP protocol gives the entity authentication while it gives the Security association.

Hence, the entity authentication is required for the IPSec.

P32-3. If Alice and Bob are continuously sending messages to each other, can they create a security association once and use it for every packet exchanged? Explain.

P32-3. Although it is possible to create an SA permanently, it is strongly discouraged because of the leak of security parameters. With the passage of time, Eve may find the secrets between Alice and Bob and misuse them.

P32-4. Can we use SSL with UDP? Explain.

SSL:

• This stands for Secure Socket Layer.

• The SSL and TLS (Transport Layer Security) is the most generally can be used for security protocol utilized now a day.

• This is basically a protocol that gives the protected channel between two machines working over the internet or an inner network.

• In the present, Internet centered world, the SSL protocol is commonly utilized when a web browser needs to safely associates with a web server over the naturally insecure internet.

• In fact, SSL is a transparent protocol which needs little cooperation from the end client while setting up a safe session.

• In the situation of a browser for example, clients are alarmed to the nearness of SSL when the program shows a padlock.

• Or in the situation of Expanded approval of SSL when the address bar shows both padlock or green bar.

• This is the way to achievement of SSL.

• This is simple experience for the end clients.

UDP is an unreliable, connectionless, transport layer protocol. It stands for user datagram protocol (UDP).

• The sender sends the data packets to the receiver while receiver does not send acknowledgement to the sender. That's why it is an unreliable protocol.

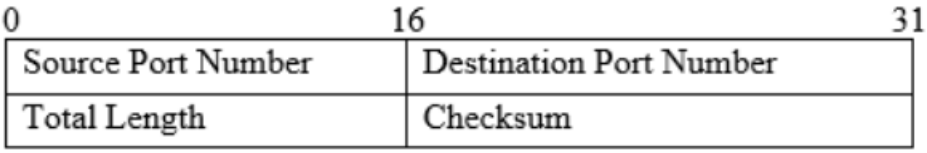
User datagram is the UDP packet; it contains 8 bytes of header and data which is sending to the receiver side.

• The length of UDP packet is maximum to 65535 bytes.

• UDP packets are encapsulated with IP datagram with length 65535 bytes. IP fields consist header length and total length.

• At the receiver side, to calculate the UDP length of the data from provided information of UDP user datagram.

The header format of the UDP is:



• Source port number is the port number which is used by the source host at the running time. It consists 16-bit length.

• Destination port number is the port number which is used by the destination host at the running time. It consists also 16-bit length.

• UDP length of the data from provided information of UDP user datagram. *data length = Total length – header length*

• Checksum is used to detect errors in the datagram.

There is way by which a SSL cab be used with the UDP which description is as follows:

• So, one method is by which SSL can be used with UDP.

• SSL can be used with UDP for socket.

• The protocol name is DTLS (Datagram Transport Security Layer) and implementation can be provided by the OpenSSL documentation.

DTLS:

• This stands for Datagram Transport Security Layer).

• This is a type of communication protocol that gives the safe security for the datagram based application.

• DTLS is designed in such way in order to prevent fake message that can be used with SSL also for security purpose.

• This depends upon both stream based Transport Layer Security protocol that gives the guarantee of security.

• Below is the documentation that defines the DTLS.

• RFC 6347 that can be used for UDP.

• RFC 5238 that can be used for Datagram Congestion Control Protocol.

Hence, SSL can be used with the UDP and that method is the DTLS which is safe.

P32-5. Why is there no need for a Security Association with SSL?

P32-5. An SA provides two services for IPSec: it creates a virtual connection and establishes security parameters between the two parties. The first service is not needed in the case of SSL because SSL runs over TCP, which is a connection-oriented protocol. The second service of SA is provided by the handshake protocol in SSL.

P32-6. Compare and contrast PGP and S/MIME. What are the advantages and disadvantages of each?

PGP:

- This stands for Pretty Good Privacy.
- This is a type of cryptographic tools in order to give the end users with good level of cryptography.
- This is the most famous program that can be utilized to encrypt and decrypt email over the internet.
- This can also be utilized for authenticate message with digital signatures as well as encrypted stored files.
- This encryption program gives the cryptographic privacy and authentication for data communication.
- This can be utilized for signing, encrypting, and decrypting words-mails.
- This can be used in order to increase the security level of e-mail.
- PGP gives the authentication with the help of digital signatures.
- PGP defines the operational description which is as follows:
- **Confidentiality:** This can be achieved with the help of symmetric block encryption.
- **Compression:** This can be achieved with the help of ZIP algorithm.
- **E-Mail Compatibility:** This can be achieved with the help of radix-64 encoding scheme.
- **Authentication:** This can be achieved by the digital signature services which is given by the PGP.
- **Segmentation and Reassembly:** Suppose that a message is too large then PGP automatically divides a message into the segments and at the receiver site segment messages will be reassembled. This can be done after all above process will done.

S/MIME:

• This stands for Secure/Multipurpose Internet Mail Extension.

• S/MIME is the version of MIME.

• S/MIME can be used for encryption of messages and that uses the concept of RSA public key encryption algorithm.

• This was developed with the help of RSA security.

• In order to secure the e-mail communication many software services and e-mail services can use the S/MIME.

• This also has the features to make the secure e-mail services which is as follows:

• **Authentication:** This can be achieved by the digital signature services which is given by the S/MIME.

• **Encryption**

• **Message Integrity** and **other related services**.

• This uses the public key to encode and decode the messages.

• Validation can be done for sender recognition with the help of digital signatures.

Contrast between the PGP and S/MIME:

• The PGP and S/MIME uses the encryption with the two keys but S/MIME uses the RSA public key encryption algorithm and PGP uses two keys in this one key can be generated with the browser automatically.

• Both uses some formats which is different from each other.

• Both uses the different key exchanges for the formats.

Comparison between PGP and S/MIME:

• PGP relies on every client's key exchange while S/MIME utilizes hierarchically approved certifier for key exchange.

• PGP was created to address the security issue of plain text data while S/MIME is intended to secure a wide range of information records.

• These days S/MIME is known to overwhelm the protected electronic industry since it is incorporated into e-commercial email packages.

• S/MIME items are efficiently low cost available than for the PGP.

Advantage of PGP:

• PGP gives the higher level of security.

• All the small files can be sent over the internet because files can be compressed before encryptions.

• This uses the digital signatures in order to identify the sender.

• This can be used to make a trust among the people.

Disadvantage of PGP:

• **Compatibility Issues:** In this both client and server must have the same version of PGP.

• **No recovery:** There might be chance of forget the password, So, in the PGP there is not any mechanism to recover password only has the strong encryption methods.

• **Complexity:** PGP uses the symmetric encryption with two keys while browser generate the by default 1 key. So, PGP uses the symmetric encryption with two key makes the Complex.

Advantage of S/MIME:

• This encode and decode the emails automatically for the users.

• This resolves the certificate management issues that means S/MIME can encrypts the e-mails itself.

• This uses the public key encryption algorithm that means sender can send the messages after the recipient's certificates.

• This has another advantage that, this tells a particular file belongs to which category which is as follows:

• **Application**

• **Text**

• **Video**

• It has another advantage that S/MIME type can be identified with the help of file contents, not with the help of name.

Disadvan **tage of S/MIME:**

• In this some mixed formats can be examined an application that can be application/ pdf or application/vorbis.

• **Email Client Program:** In Email Client Program whole email program does not supports the S/MIME while another internet application e-mail reader like **Gmail, Hotmail and so on** does not support the S/MIME.

• **Trust:** Regardless of the possibility that all the specialized pieces of the S/MIME work. There is as yet the more troublesome issue of the trust.

• Would be able to believe an email messages with a digital signature?

• While safe email depends upon cryptographic algorithm which are unbreakable yet there are lot of the processes around them which could turn out wrong.

P32-7. Should the handshaking in SSL occur before or after the three-way handshaking in TCP? Can they be combined? Explain.

P32-7. The handshake protocol in SSL should start its function after the three-way handshaking in TCP because the handshaking protocol in SSL does not create a connection; it uses the connection established by TCP to exchange security parameters.

P32-8. We defined two security services for e-mail (PGP and S/MIME). Explain why e-mail applications cannot use the services of SSL/TLS and need to use either PGP or S/MIME.

• SSL stands for the secure socket layer.

• TLS stands for the transport layer security

• PGP stands for the pretty good privacy

• MIME stands for the multipurpose internet mail extension.

PGP and S/MIME is used for the email service as a security service but it is not used the SSL/TLS security services, because SSL and TLS are the create session between the sender and receiver. But actually in email services sender and receiver may communicate in various times. PGP and S/MIME doesn't create any session between the sender and receiver.

Therefore, email services used the PGP and S/MIME as a security services.

P32-9. Assume Alice needs to send an e-mail to Bob. Explain how the integrity of the e-mail is achieved using PGP.

P32-9. Alice creates a message digest and signs it with her private key. She then sends the message and the signed digest.

P32-10. Assume Alice needs to send an e-mail to Bob. Explain how the confidentiality of the e-mail is achieved using PGP.

PGP is stands for the pretty good privacy. PGP is used in email services to provide the integrity, confidentiality, privacy and authentication.

Confidentiality in PGP:

Refer figure 10.32, when alice and bob communicated through the email services, then alice used bob's public key to encrypt the message, after then bob used own private key to decrypt the message.

Therefore, confidentiality of the email is achieved.

P32-11. Assume Alice needs to send an e-mail to Bob. Explain how the integrity of the e-mail is achieved using S/MIME.

P32-11. Alice creates a message digest from the content. Alice then sends the digest, the hash algorithm, and the content. The whole is referred to as *digestedData* object.

P32-12. Assume Alice needs to send an e-mail to Bob. Explain how the authentication of the e-mail is achieved using S/MIME.

• S/MIME is stands for the secured/multipurpose internet mail extension.

S/MIME advantages:

1. S/MIME embeds the automatic encryption and decryption specification.

2. Confidentiality should achieve.

S/MIME disadvantages:

1. High amount of resources are required for implementation.

2. Complexity in execution.

Authentication in S/MIME:

Refer question, alice should use secret key that is symmetric key to communicate with the bob. The secret key is created by the key distribution center. Key distribution center send this secret key to alice and bob. That is no one can use this.

The secret key is shared between the alice and bob. Then bob can only decrypt the message. Therefore, authentication is achieved.

P32-13. Assume Alice needs to send an e-mail to Bob. Explain how the confidentiality of the e-mail is achieved using S/MIME.

P32-13. Alice uses an *envelopedData*. She creates a random number as the session key. She then encrypts the session key with Bob's public key. The message is encrypted with the session key.

P32-14. When we talk about authentication in SSL, do we mean *message authentication* or *entity authentication*? Explain.

Message authentication and entity authentication both are used for the securing the message.

Message authentication	Entity authentication
Message authentication is the process to verify the sender and recipient of the message, and it run when the new message is arrived.	Entity authentication should verify the all entities in the session until the communication is completed.
Message authentication shouldn't process in real time.	Entity authentication is processed only in real time.

SSL is stands for the secure socket layer. SSL is used to create the session between the sender and receiver. During the session SSL verifies the user's entities. When session is terminated then SSL doesn't worked. That is SSL is verified the entity authentication.

Therefore, authentication in SSL is entity authentication.

P32-15. When we talk about authentication in PGP (or S/MIME), do we mean *message authentication* or *entity authentication*? Explain.

P32-15. In e-mail communication, there is no virtual connection between the two parties. Each e-mail is a unidirectional communication between the sender and receiver. This means that there cannot be entity authentication in PGP or in S/MIME. When we talk about authentication in PGP or S/MIME, we mean message authentication.

P32-16. If cryptography algorithms in PGP or S/MIME cannot be negotiated, how can the receiver of the e-mail determine which algorithm has been used by the sender?

PGP and S/MIME is used for the email service as a security service but it is not used the SSL/TLS security services, because SSL and TLS are the create session between the sender and receiver. But actually in email services sender and receiver may communicate in various times. PGP and S/MIME doesn't create any session between the sender and receiver.

If PGP and S/MIME services may negotiated, then email services use the data encryption standard (DES) and message digest (MD5) algorithms to provide the security to the email service.

DES is used for the encryption and decryption and MD5 is for hashing, because these algorithms used to verify the identifiers first.