Q2 (a) What are Passive Attacks? Why are they difficult to detect? Name some passive attacks.

Answer

Passive attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmission, the goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of massage contents and traffic analysis.

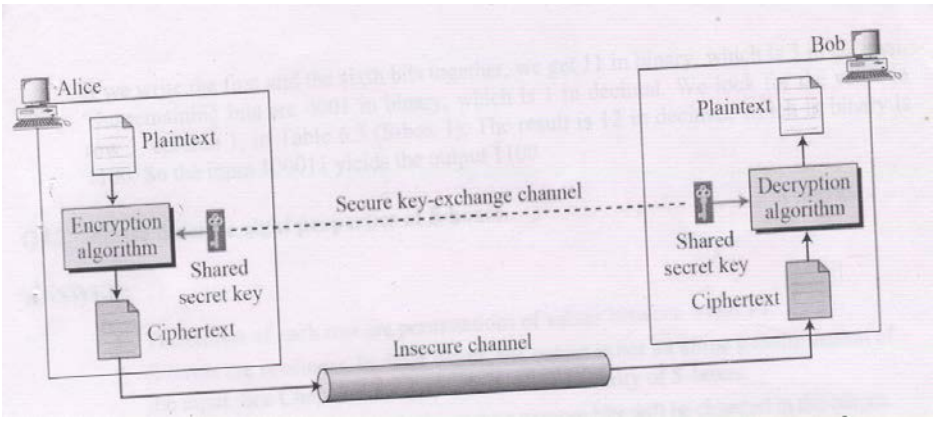
The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these message .the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged .This information might be useful in guessing the nature of the communication that was taking place .

Passing attacks very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the message or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather then detection.

Q3 (a) Draw a diagram for depicting general idea of a symmetric-key cipher.

Answer



Q3 (b) Write a note on Multiplicative Ciphers. What is the key domain for any multiplicative cipher?

Answer

The Key needs to be Z26 *
This set has only 12 members:1,3,5,7,9,11,15,17,19,21,23,25.

Q3 (c) Suppose that we have a block cipher where n = 64. If there are 10 1's in the cipher text, how many trial-and-error tests does Eve need to do to recover the plaintext from the intercepted cipher text in each of the following cases?
(i) The cipher is designed as a substitution cipher.
(ii) The cipher is designed as a transposition cipher.

Answer

a. In the first case, Eve has no idea how many 1's are in the plaintext. Eve needs to try all possible 264 64-bit blocks to find one that makes sense.
b. In the second case, Eve knows that there are exactly 101's the plaintext. Eve can launch an exhaustive – search attacks using only those 64-bit blocks that have exactly 101's

Q4 (a) The input to S-box 1 (the table below) is 100011. What is the output?

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Answer

If we write the first and the sixth bits together, we get 11 in binary, which are 3 in decimal. The remaining bits are 0001 in binary, which is 1 in decimal. We look for the value in row 3, column 1, in Table 6.3(S-box1). The result is 12 in decimal, which in binary is 1100. So the input 100011 yields the output 1100.

Q4 (b) Mention any eight properties of S-boxes.

Answer

1. The entries of each row are permutations of values between 0 and 15.
2. S-boxes are nonlinear .In other words, the output is not an affine transformation of the input. See Chapter 5 for discussion on the linearity of S-boxes.
3. If we change a single bit in the input, two or more bits will be changed in the output
4. If two inputs to an S-boxes differ only in two middle bits (bits 3 and 4). The output must differ in at least two bits. In order words, S(x) and S(x(+)001100) must differ in at least two bits where x is the input and S(x) is the output.
5. If two inputs to an S-box differ in the first two bits (bits 1 and 2) and the same in the last two bits (5 and 6), the two outputs must be different. In other words, we need to have the following relation S(x) $\neq$ S(x (+) 11bc00), in which b and c are arbitrary bits.
6. There are only 32 6-bit input-word ($x_i and x_j$ **),** in which $x_i \oplus x_j \neq (000000)_2$.

These 32 input pairs create 32 4-bit output-word pairs. If we create the difference between the 32 output pairs, d= $y_i \oplus y_j$ **,** no more than 8 of these d's should be the same.

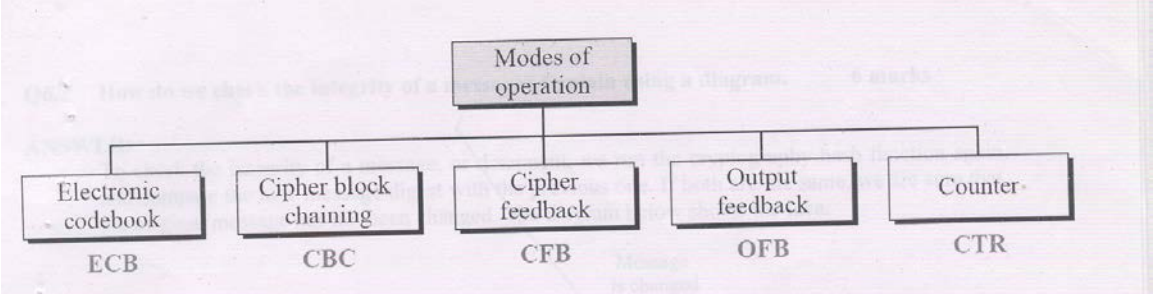
7. A criterion similar to $\neq 6$ is applied to three S-boxes.
8. In any S-box, if a single input bit is held constant (0 or 1) and the other bits are changed randomly, the differences between the number of 0s and 1s are minimized.

Q4 (c) What is the probability of randomly selecting a weak, a semi-weak or a possible weak key in DES?

Answer
DES has a key domain of 256. The total numbers of the above keys are 64(4+12+48). The probabilities of choosing one of these keys is 8.8 $\times$10-16, almost impossible.

Q5 (a) What are the different modes of operation designed to be used with modern block ciphers? Describe any four.

Answer



Q6 (a) Explain the meaning of "Document & Finger print" and "Message & Message Digest". What's the difference between the 2 pairs?

Answer Page Number 340 of Text-Book

Q6 (b) Explain Davies Meyer scheme with diagram

Answer Page Number 366 of Text-Book

Q7 (a) What are the differences between conventional signatures and digital signatures? Write a note on "Attacks on digital signature".

Answer

1. Inclusion: A conventional signature is included in the document; it is part of the document. But when we sign a document digitally, we send the signature as a separate document.
2. Verification Method: for a conventional signature, when the recipient receives a document, she compares the signature on the document with the signature on file. For a digital signature, the recipient receives the message and the signature. The

recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.

3. Relationship: for a conventional signature, there is normally a one-to-many relationship between a signature and documents. For a digital signature, there is a one-to-one relationship between a signature and a message.
4. Duplicity: In conventional signature a copy of the sighned document can be distinguished from the original one on file. In digital signature, there is no such distinction unless there is a factor of time on the document.

Q8 (a) If e-mail is one-time activity, how can the sender and receiver agree on a cryptographic algorithm to use for e-mail security? If there is no session and no handshaking to negotiate the algorithms for encryption/decryption and hashing, how can the receiver know which algorithm the sender has chosen for each purpose?

Answer

One solution is for the underlying protocol to select one algorithm for cryptographic operation and to force Alice to use only those algorithms. This solution is very restrictive and limits the capabilities of the two parties.

A better solution is for the underlying protocol to define a set of algorithms for each operation that the user used in his/her system. Alice includes the name (or identifiers) of the algorithms she has used in e-mails. For example, Alice can choose triple DES for encryption / decryption and MD5 for hashing. When Alice sends a message to Bob, she receives the message and extracts the identifiers first. He then knows which algorithm to use for decryption and which one for hashing.

Q8 (b) Let us assume that Alice has only two user IDs, alice@some.com and alice@anet.net. We also assume that Alice has two sets of private/public keys, one for each user ID. Please draw the private key ring table for Alice.

Answer

User ID	***Key Id***	***Public Key***	***Encrypted Private Key***	***Timestamp***
alice@anet.net	AB13…45	AB13…45…..59	**32452398….23**	031505-16:23
alice@some .com	FA23…12	FA23….12…22	**564A4923…23**	031504-08:11

Q8 (c) Explain the need for Key Revocation. How it is done?

Answer

It may become necessary for an entity to revoke his or her public key from the ring. This may happen if the owner of the key feels that the key is compromised (stolen, for example) or just too old to be safe.

Q9 (a) "SSL differentiates a connection from a session". Elaborate through a diagram.

Answer

1. SSL differentiates a connection from session. Let us elaborate on these two terms here. A session is an association between a client and server. After a session is established, the two parties have common information such as the session identifier, the certificate authenticating each of them (if necessary), the compression method (if needed), the cipher suite, and a master secret that is used to create keys for message authentication encryption .
2. For two entities to exchange data, the establishment of a session is necessary, but not sufficient: they need to create a connection between themselves. The two entities exchange two random numbers and create, using the master secret, the keys and arameted, the two parties can also terminate the session, but it is not mandatory. A session can be suspended and resumed.
3. To create a new session, the two parties need to go through a negotiation process. To resume an old session and create only a new connection, the two parties can skip part of the negotiation process and go through a shorter one. There is no need to create a master secret when a session is resumed.
4. The separation of a session from a connection prevents the high cost of creating a master secret. By allowing a session to be suspended and resumed, the process of the master secret calculation can be eliminated.

Q9 (b) What are the four phases in a handshake protocol? Draw a diagram to elaborate four cases in phase II.

Answer Page Number 518 of Text-Book

Text Book

Behrouz A. Forouzan, Cryptography & Network Security, Special Indian Edition.