Chapter 1 : Introduction

Q. 1 What are passive attacks ? Categorize these attacks and explain one example of each.

Ans. :

A passive attack makes attempt to collect information from the system but does not modify or alter the system data or resources. Eavesdropping or monitoring of information is example of passive attacks. The goal of opponent is to gain the information that is being transmitted. The two types of passive attacks are :

1. Release of message contents
2. Traffic analysis

1. Release of message contents :

We may want to prevent the opponent from learning sensitive and confidential information through transmissions that take place through telephone calls or email messages or files transferred on network .This is quite simple to understand. When we send a confidential email to our friend, our aim is that only intended person should access this mail. If this mail is accessed by unauthorized users then contents of message are released against somewhere else. Such type of attack is called release of message contents. There are different security mechanisms are available to prevent such type of attacks.

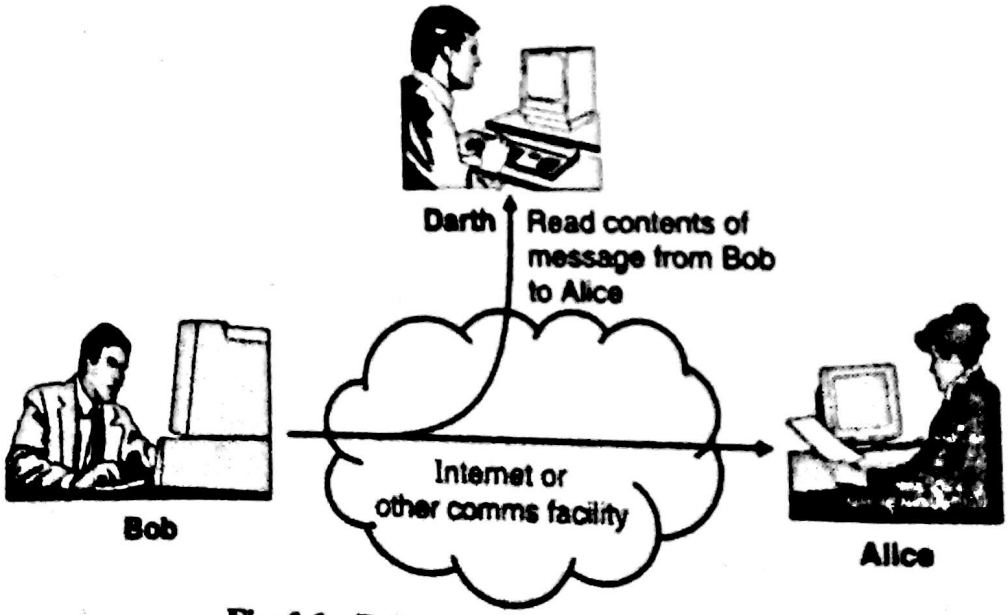


Fig. 1.1 : Release of message contents

For example : Telephonic conversation between two people, an electronic mail and a file may contents sensitive information if we have already transfer it. We would like to prevent third person from modification of these type of transmission as shown in Fig. 1.1.

Q. 2 What are active attacks ? Categorize these attacks and explain one example of each.

May 2014

Ans. :

Active attacks involve modification of a data stream or creation of a false stream of messages. Attacker aim in such type of attack is to corrupt or destroy the data as well as network itself.

Active attacks are divided into four categories :

1. Masquerade
2. Replay attack
3. Modification of messages
4. Denial of service

1. Masquerade :

A masquerade takes place when an attacker pretends to be an authentic user. It is generally done to gain access to a system, or steal important data from system. It is generally done by stealing login id and password of authentic user to gain access to a secure network. Once attacker gain access, they get full access to the network for deletion or changing of data or network policies of organization as shown in Fig. 1.2.

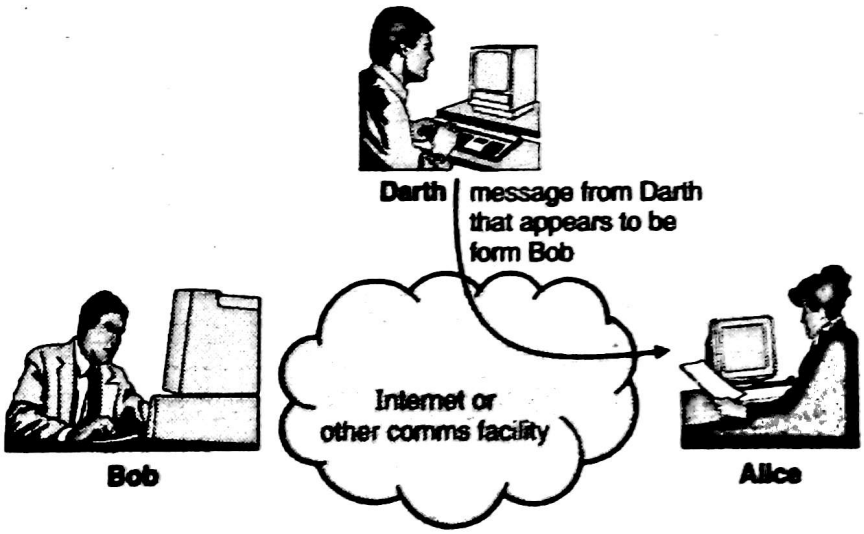


Fig. 1.2 : Masquerade attack

Q. 3 Distinguish between attack, vulnerability and access control. Dec. 2014

Ans. :

Sr. No.	Attack	Vulnerability	Access control
1.	An assault on system security through an intelligent act that is deliberate attempt to evade security services and violate the security policy of a system	An intended flaw in software code or a system that leaves it opens to potential exploitation in the form of unauthorized access and or malicious behaviour.	Access control is a protective measure, technique device etc. that removes or reduces the vulnerability.
2.	**Types of Attack :** Passive attack, Active attack, Distributed attack, phishing Attack, Password Attack.	**Types of Vulnerability :** Data Vulnerability, Hardware Vulnerability, Software Vulnerability.	**Types of Access Control:** Preventive, Corrective, Recovery, Detective, Deferent

Sr. No.	Attack	Vulnerability	Access control
3.	Here a threat is in action.	Here a threat is without mitigation	Here a threat is blocked by control of vulnerability.
4.	**Example :** Water flow out of the crack in the wall and drips the man.	**Example :** Crack in the wall	**Example :** Seal the crack before water comes out

Q. 4 Differentiate between - vulnerability, threats and controls. May 2015

Ans. :

Sr. No.	Vulnerability	Threats	Control
1.	A vulnerability is a software, hardware, procedural, or human weakness that may provide an attacker the open door to enter a computer or network and have unauthorized access to resources within the environment.	A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.	a control is an action, device, procedure, or technique that removes or reduces vulnerability, threat is blocked by control of vulnerability.
2.	Vulnerability is a weakness in the security system.	A threat is any potential danger to information or systems.	A control or countermeasure is a means to counter threats.
3.	Paired with a credible attack, each of these vulnerabilities can allow harm to confidentiality, integrity, or availability.	A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy.	Safeguard implemented to close vulnerabilities and mitigate threats in order to protect the confidentiality, integrity and availability of system.

Q. 5 What are the system security goals ? Explain why the balance among different goals is needed. Dec. 2013, May 2014

Ans. :

Information security consists of methods used to protect data or information being transmitted for preserving the integrity, availability and confidentiality of the information.

1. Confidentiality :

The two important concepts :

Data confidentiality : Assures that private or confidential information is not disclosed to unauthorized individuals.

Privacy : Assures that individuals control information related to them.

2. Integrity :

The two important concepts :

Data integrity : Assures information is changed only in authorized manner.

System integrity : Assures that the system performs its intended function properly and free from unauthorized manipulation.

3. Availability :

Assures that system works correctly and service is available to authorized users. These three concepts are termed as CIA triad and embody fundamental security objectives for data and information services.

Fig. 1.3 : CIA triad

Q. 6 What are the key principles of security ? May 2013

Ans. :

There are five chief principles security they are : **Confidentiality, integrity, availability, authentication and authorization(access control)** Other than this there are two more security principles which links overall system as whole are :

Non-repudiation and notarization or signature :

Non-repudiation : It is an assurance that somebody cannot deny something. refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated

Notarization : It is an act of authorizing legal document. The purpose of having a legal document **notarized** is to ensure the authenticity of the signatures that appear on the document.

Q. 7 Explain authentication and authorization.

Ans. :

Authentication :

Authentication provides a way of verifying the identity of the user. In other words, Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. The authentication of users prevents unauthorized users from gaining access to information systems.

In connection oriented communication, both sender and receiver should be authenticated. In connectionless communication only the user who is sending data should be authentic user.

Authorization :

Authorization means providing authority or permission of accessing the system, or privilege of accessing data, directories, files etc of the system. Authorization is one of the most important security aspects. It provides identification of the user as authorized user. It is a kind of permission given by the network administrator for accessing the network.

Q. 8 Explain in detail different security mechanisms. Dec. 2012, Dec. 2014, June 2015

Ans. :

X.800 defines security mechanisms as follows :

It is applied to specific protocols in OSI layer or to those which are not so specific to any particular protocol.

Specific Security Mechanism

These mechanisms are incorporated into the appropriate protocol layer in order to provide some OSI security service.

Encipherment :

To use mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery depends on the algorithm and the number of keys used.

Digital signature :

The data is appended to, or cryptographic transformation of data unit that allows the receiver of the message to prove the source and integrity of data unit against forgery.

Access control :

Various mechanisms used to enforce access rights to the resources.

Data integrity :

Various mechanisms used to assure the integrity of the data.

Authentication exchange :

The mechanism used to ensure the identity of the entity by information exchange.

Traffic padding :

To insert bits into gaps in the data stream to frustrate traffic analysis attempt.

Routing control :

To allow some selected routes in network for routing or can change the route if any attack is detected in the network.

Notarization :

To use a trusted third party to assure certain properties in data exchange.

Pervasive Security Mechanisms

These mechanisms are not specific to any of the OSI security service or protocol layer.

Trusted functionality :

That which is perceived to be correct with respect to some criteria. (**Ex.:** as established by a security policy)

Security label :

The marking bond to a resource that designates the security attribute of the resource.

Event detection :

Detection of security related events.

Security audit trail :

Data collected and used to facilitate security audit.

Security recovery :

It deals with the recovery action and management functions for data that is lost or disrupted in the network during communication.

Q. 9 What is computer criminal? What are different types of computer criminals?

Ans. :

Computer criminals are those who involved in computer crimes or who caught in doing computer crime. Computer crime can be anything related to computer or computer network involving some kind criminal activity involving information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (or identity theft) and electronic fraud.

Types of Computer Criminals

1. **Script kiddies :** They are not technically sound hacker. They hack only weak secured systems.
2. **Scammers :** They generally involved in email spoofing.
3. **Hackers group :** They work anonymously, they create tools for hacking different kinds of systems. These hacker groups are generally hired by companies to test their company's security.
4. **Phishers :** They attempt to acquire password credit essential financial data by sending fake email, messages, electronically.
5. **Political/religious/commercial groups :** The malware created by the computer criminals with some political reason.
6. **Insiders :** These attackers are the greatest threat for the organization. They are the persons who reside inside the organization.
7. **Advanced Persistent Threat (APT) Agents :** These are highly skilled persons responsible for highly targeted attacks carried out by extremely organized state-sponsored groups.

❑❑❑

Chapter 2 : Basics of Cryptography

Q. 1 Define cryptography.

Ans. :

The word cryptography comes from the Greek words KPVIIT (hidden or secret) and $y_p \propto \phi_n$ (writing). **Cryptography** is the art as well as science of secret writing of information / message and makes them non-readable.

Q. 2 Explain types of cryptography.

Ans. :

There are two types of cryptography i.e. symmetric key cryptography & asymmetric key cryptography as shown in Fig. 2.1.

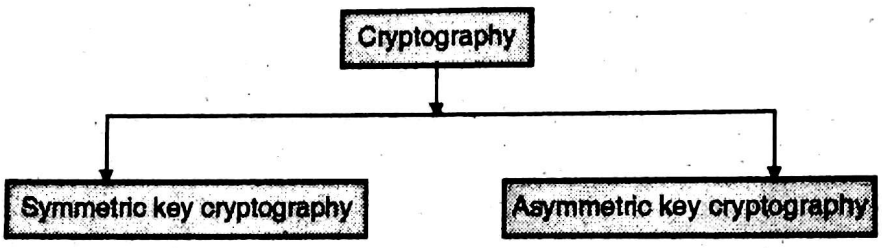


Fig. 2.1: Types of cryptography

(i) Symmetric Key Cryptography

Symmetric key cryptography is also called as secret key cryptography. In secret key cryptography a single key is used for encryption as well as decryption.

Encryption and decryption process uses same key as shown in Fig. 2.2.

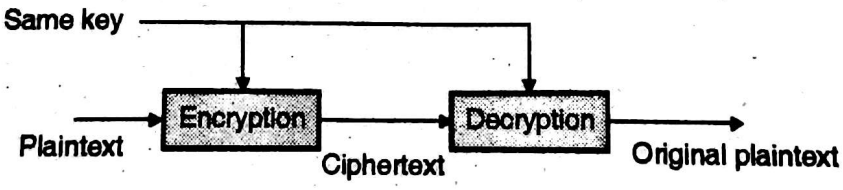


Fig. 2.2 : Symmetric key cryptography

It is represented as P = D (K, E(P)).

For Example : Stream and block cipher, Data Encryption Standard (DES), Advance Encryption Standard (AES) and BLOFISH.

Asymmetric key cryptography is also called as public key cryptography.

(ii) Asymmetric Key Cryptography

In asymmetric key cryptography two keys are used, one for encryption and other for decryption as shown in Fig. 2.3.

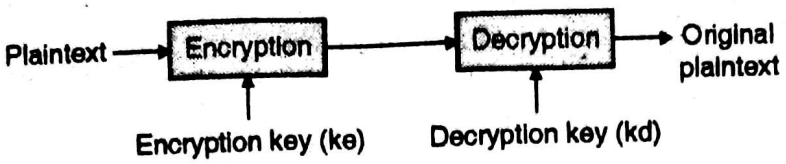


Fig. 2.3 : Asymmetric key cryptography

It is represented as P = D(Kd, E (Ke,P))

For Example : Rivest Shamir Adlman (RSA) and Diffie Hellman key exchange algorithm.

Dec. 2013

Q. 3 Explain substitution cipher.

Ans. :

A substitution is a technique in which each letter or bit of the plaintext is substituted or replaced by some other letter, number or symbol to produce ciphertext.

Caesar Cipher

Julius Caesar introduced the easiest and the simplest use of substitution cipher.

In Caesar cipher technique each letter is replaced by the letter /alphabet which is three place next to that letter which is to be substituted.

For example :

Plaintext : Sun rises in the East

Ciphertext : VXQULVHVLQWKHHDVW

Following is the list of possible combination showing the letters 3 places down of each alphabet :

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

The corresponding number equivalent to each alphabet is given below :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Mathematically the Caesar cipher algorithm can be expressed as

$$C = E(3,P) = (P+3) \bmod 26$$

$$P = D(3,C) = (C-3) \bmod 26$$

Where

C = Ciphertext/ or alphabet

P = Plaintext/ alphabet

E = Encryption

D = Decryption

Mod 26 because in English there are total 26 alphabets .

Caesar cipher is more prone to Brute force attack because the attacker will be having only 25 possible keys to decrypt the ciphertext.

Q. 4 What is keyless Transposition Cipher ? Give any example of rail fence cipher. **Dec - 2013, May 2014**

Ans. :

In transposition technique, there is no replacement of alphabets or numbers occurs instead their positions are changed or reordering of position of plaintext is done to produce ciphertext.

There are two types of transposition techniques :

(a) Columnar transposition techniques

(b) Keyless transposition techniques

(a) Columnar transposition technique is very simple to understand.

(1) Write plaintext message into a rectangle with some predefined size.

(2) Select the random key according to the size of rectangle also called columns.

(3) Read the text present in each selected random key columns.

(4) Combine all text present in each column as per selected random key order.

(5) The resultant text called ciphertext as shown in Fig. 2.4.

Step 1 : **Plaintext :** Are you missing somebody.

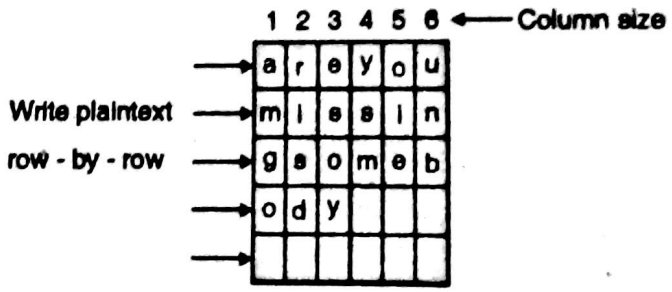


Fig. 2.4 : Columnar transposition technique

Step 2 : Select random key 5 4 2 3 1 6

Step 3 : Read text present in each column according to key.

Step 4 : Oieysmrisdesoyamgoumb

Step 5 : Final ciphertext is

Ciphertext : Oieysmrisdesoyamgourmb

The ciphertext obtained in step 5 can be made more complicated by performing multiple rounds of such permutations. Diffusion means permutation of bit or byte positions

(b) Keyless Transposition Techniques :

Keyless transposition technique also called **Rail fence technique.**

Algorithm for keyless transposition technique is given below :

(1) Write plaintext message into Zigzag order.

(2) Read plaintext message of step 1 in order of row by row as shown in Fig. 2.5.

For example : Plaintext : be careful while chatting.

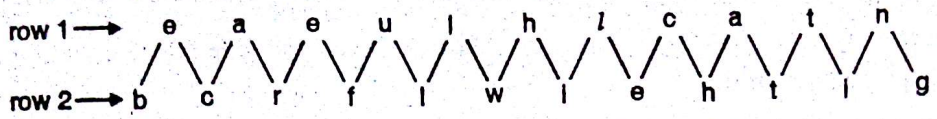


Fig. 2.5 : Zigzag order of plaintext

Write plaintext obtained in row 1 and row 2. The resultant ciphertext is

Ciphertext : eqeulhlcatnbcrflwiehtig.

This technique doesn't want any key. Rows are also fixed (2) so that attacker may get clue to break the ciphertext obtained using rail fence technique.

A more complex way to encrypt the message would be to write it in a rectangle, row by row, and then read off the message column by column, but to decide the order of the columns. The order of the column will be the key of the algorithm.

For example :

Plaintext : The book is related to history.

Key : 4351267

4	3	5	1	2	6	7
t	h	e	b	o	o	k
i	s	r	e	l	a	t
e	d	t	o	h	i	s
t	o	r	y			

Ciphertext : BEOYOLHHSDOTIETERTROAIKTS

Q. 5 What are the different types of ciphers? Describe block ciphers in detail.. May 2015

Ans. :

(i) Cryptographic algorithm is used for transformation of plaintext into ciphertext.

(ii) The generation of plaintext into ciphertext in two basic ways **Stream cipher** and **Block cipher.** This is shown in Fig. 2.6

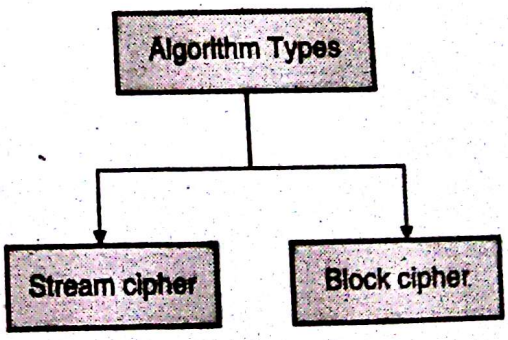


Fig. 2.6 : Types of Cipher

Block Cipher

(i) A block cipher operates on plaintext accepting a block of bit at a time. Generally a block size of 64 or 128 bits is used.

(ii) Like in stream cipher block cipher also uses the concept of key generator. Block cipher are used in **Chaining mode,** this is because for repeating text pattern, the same cipher block will be

generated which can give clue to cryptanalyst regarding what is the original plaintext hence chaining mode is used for block ciphers as we shall see later in this chapter.

(iii) As in chaining method, previous block is mixed with current block to avoid repeats in patterns. Block cipher is little time consuming then stream cipher so generally used in computer based cryptographic algorithms.

Q. 6 Give difference between confusion and diffusion.

Ans. :

Difference between Confusion and Diffusion

Sr. No.	Confusion	Diffusion
1.	Confusion obscures the relationship between the plaintext and ciphertext.	Diffusion spreads the plaintext statistics through the ciphertext.
2.	A one-time pad relies entirely on confusion while a simple substitution cipher is another (weak) example of a confusion-only cryptosystem.	A double transposition is the classic example of a diffusion-only cryptosystem.
3.	Confusion alone is, apparently, "enough", since the one-time pad is provably secure.	Diffusion alone is, perhaps, not enough, at least using relatively small blocks. A stream cipher is simply a weaker version of a one-time pad.
4.	The codebook aspects of such systems provide confusion analogous to though on a much grander scale a simple substitution.	Well-designed block ciphers spread any local statistics throughout the block, thus employing the principle of diffusion.

❑❑❑

Chapter 3 : Secret Key Cryptography

Q. 1 Explain any one of block ciphers with example. Also explain structure of DES. **May 2015**

Ans. :

DES is block cipher published by National Institute of Standards and Technology (NIST). DES was originally developed by an IBM team formed in early 1970 in response to customer request for a method to secure data. Data encryption standard takes 64-bit plaintext as a input and creates 64-bit Ciphertext i.e. it encrypts data in block of size 64-bits per block.

Divide plaintext message into 64-bit block each.

OR

The given plaintext message is divided into size 64-bits block each and encrypted using 56-bit key at the initial level. Fig. 3.1 shows conceptual view of DES.

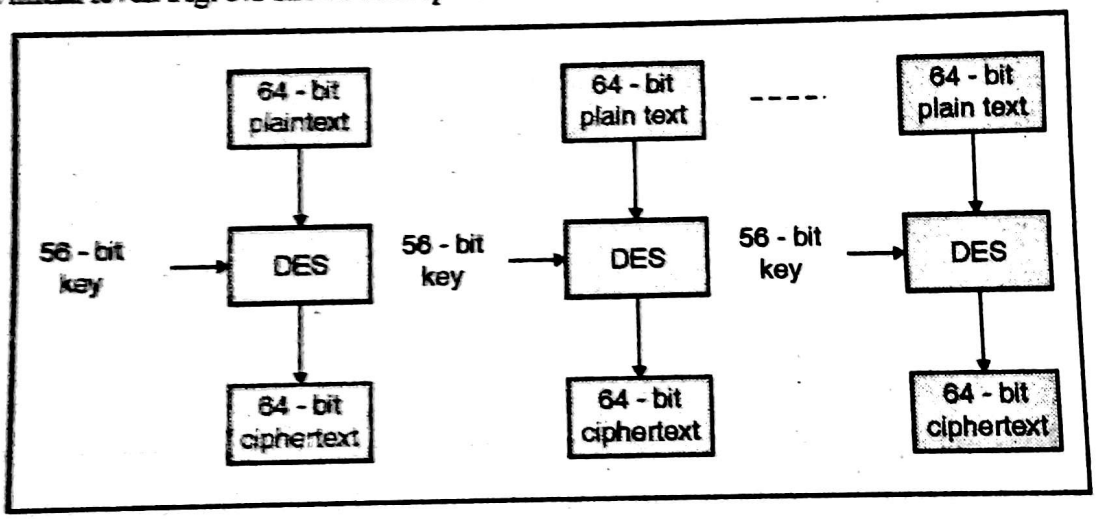


Fig. 3.1 : Conceptual view of DES

At the decryption side, DES takes 64-bit ciphertext and creates 64-bit plaintext and 56-bit key.

Steps of DES

The principle of DES is very simple. Divide plaintext message into block of size 64-bits each, which is initial permutation. After initial permutation on 64-bit block, the block is divided into two halves of 32-bit called left plaintext and right plaintext.

The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each rounds. 16 rounds of encryption process left plaintext and right plaintext gets combined and final permutation is performed on these combined blocks. The result of final permutation produces 64-bit of ciphertext as shown in Fig 3.2.

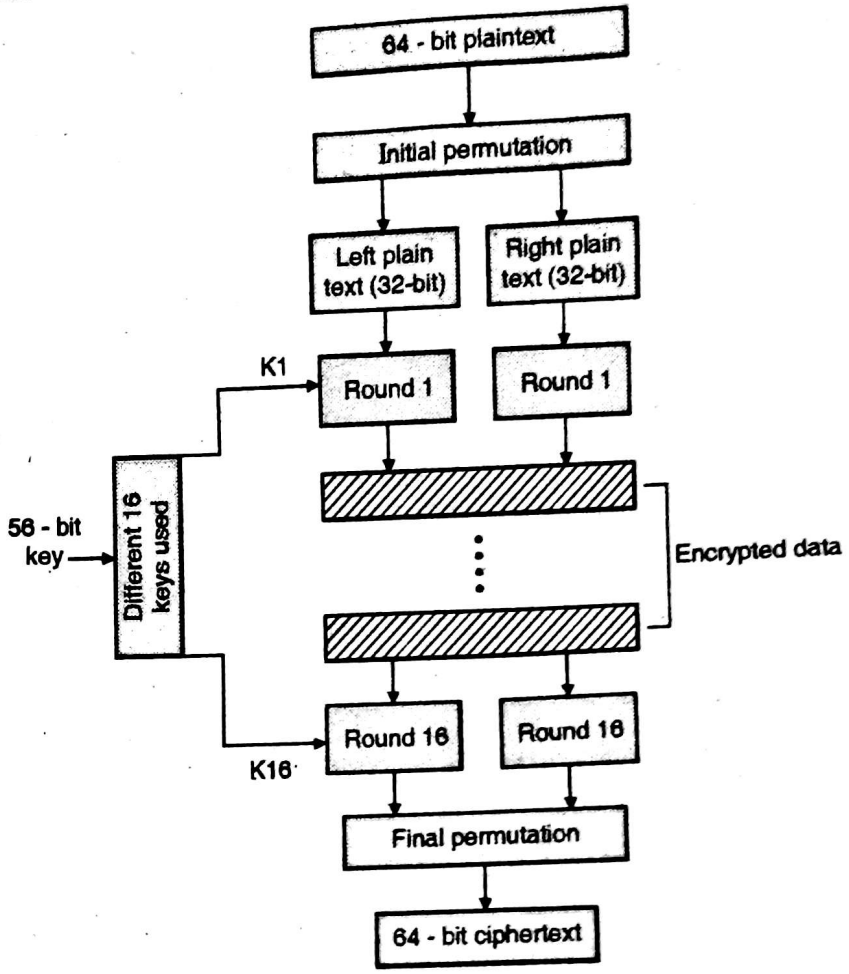


Fig. 3.2 : Detail Steps in DES

Q. 2 Explain Initial permutation steps in DES.

Ans.:

Initial permutation is the process of rearranging or shuffling each bit of original plaintext block with any other random bit of same plaintext message block.

For example : First bit of original plaintext block replace with 48th bit of original plaintext block, the 2nd bit replaces with 57th bit of original plaintext message shown in Table 3.1.

Table. 3.1 : Initial permutation

48	57	59					64
					1		
2	3						7

Plaintext block (64 bits)

This process called jugglery of bit position of plaintext block which is applied to all original plaintext blocks in a sequence. After initial permutation the 64-bit plaintext block get divided into two

halves LPT (32-bit) and RPT (32-bit). Now 16 rounds of encryption process were completed on LPT and RPT.

Q. 3 What are advantages and disadvantages of DES ?

Ans. :

Advantages of DES

1. The DES encryption technique ideally suited for implementation of hardware (bit shifts, lookups etc).
2. Dedicated hardware could run DES at 200 M byte/s.
3. Technique well suited for voice, video encryption.
4. DES uses 56-bit keys so that there are 2^{56} possible key combinations which is roughly equal to 7.2×10^{16} keys required to break DES cipher.
5. A machine performing one DES encryption per microsecond would take more than a thousand year to break the cipher.
6. If a small change in either plaintext or the key, the ciphertext should change markedly.

Disadvantages in DES

1. Trying all possible combination of 2^{56} possible keys is not that much hard these days.
2. If you spend ~ $25 K you can build.
3. In an exhaustive search known plaintext attack, the cryptanalyst will obtain the solution after 2^{55} i.e. 3.6029×10^{16} trials on an average.
4. If you spend $25 K you can build DES password crackers that will successes in few hours.

Q. 4 Write short note on : Multiple DES or double DES. **May 2014**

Ans. :

Double performs the same operation as DES only difference is that double DES use two keys K1 & K2. First it perform encryption on plaintext which is encrypted using K1 obtains first ciphertext again this ciphertext is encrypted by using another key called K2 & converted into final ciphertext. Mathematically double DES is represented as

$$Pt \Rightarrow EK1(Pt) \Rightarrow TEMP = EK1(Pt) \Rightarrow EK2(E(K1(P))) \Rightarrow Cp = EK2(E(K1(Pt)))$$

Where
- Pt = Plaintext
- EK1(Pt) = Encrypted plaintext with Key K1
- TEMP = EK1(Pt) = Temporary Variable to store results
- EK2(E(K1(P))) = Encrypted Results of first step using K2
- Cp = Final Ciphertext.

Decryption of Double DES is reverse of Encryption. Whatever the ciphertext obtained after double DES encryption process get decrypted using K2 & obtain the first ciphertext, the result of previous step (ciphertext) decrypted using K1 which yields the original plaintext.

Q. 5 Write short note on : Multiple DES or triple DES. **May 2014**

Ans. :

Triple DES performs the same operation as double DES only difference is that triple DES uses three keys K1, K2 & K3 while encrypting plaintext. First it perform encryption on plaintext which is encrypted using K1 obtains first ciphertext again this ciphertext is encrypted by using another key called K2 which obtains the second ciphertext which is again encrypted using K3 & converted into final ciphertext Cp.

Mathematically, Double DES is represented as,

$Pt \Rightarrow EK1(Pt) \Rightarrow TEMP = EK1(Pt) \Rightarrow \quad EK2(E(K1(P))) \Rightarrow EK3\ (EK2(EK1(Pt)))$

$\Rightarrow Cp = EK3\ (EK2(EK1(Pt)))$

Where Pt = Plaintext

EK1(Pt) = Encrypted plaintext with Key K1

TEMP = EK1(Pt) = Temporary Variable to store results

EK2(E(K1(P))) = Encrypted Results of first ciphertext using K2

EK3 (EK2(EK1(Pt))) = Encrypted Results of second step using K2

Cp = EK3 (EK2(EK1(Pt))) Final ciphertext encrypted using K1, K2 & K3

Decryption of Triple DES is reverse of Encryption.

The final ciphertext obtained after Triple DES encryption process get decrypted using K3 which results second ciphertext, second ciphertext decrypted using K2 which results first ciphertext, first ciphertext again decrypted using K1which generate the original plaintext Pt.

Q. 6 What is International Data Encryption Algorithm (IDEA) ? Explain key generation process.

Ans.:

It is a block cipher algorithm designed by Xuejia Lai and James L. Massey of ETH-Zürich in 1991. It is a modified version of Data encryption Standard algorithm. It operates on 64-bit plaintext and ciphertext blocks and key used is of 128 bit. It was used in Pretty Good Privacy PGP v2.

Total 8 numbers of rounds are done using 6 keys in each round. Like this 48 keys are there and in last round another 4 keys (6*8= 48 + 4=52) are used for both encryption and decryption. The operations performed in this process are i) XOR ii) Addition iii) Multiplication

Key generation process :

The 128 bit keys are divided into 8 sub parts i.e. 16 bit in each subpart. Then this 128 bit key is cyclic shifted to the left by 25 positions and generates a new 128 bit key. Similarly this 128 bit key is divided into 8 sub blocks which will be used in next round. The same process is repeated from which 52 keys are generated. Table 3.2 show sub blocks of key generation.

Table 3.2 : Encryption of the key sub-blocks

Round 1	$Z_1^{(1)}\ Z_2^{(1)}\ Z_3^{(1)}\ Z_4^{(1)}\ Z_5^{(1)}\ Z_6^{(1)}$
Round 2	$Z_1^{(2)}\ Z_2^{(2)}\ Z_3^{(2)}\ Z_4^{(2)}\ Z_5^{(2)}\ Z_6^{(2)}$
Round 3	$Z_1^{(3)}\ Z_2^{(3)}\ Z_3^{(3)}\ Z_4^{(3)}\ Z_5^{(3)}\ Z_6^{(3)}$

Round 4	$Z_1^{(4)}\ Z_2^{(4)}\ Z_3^{(4)}\ Z_4^{(4)}\ Z_5^{(4)}\ Z_6^{(4)}$
Round 5	$Z_1^{(5)}\ Z_2^{(5)}\ Z_3^{(5)}\ Z_4^{(5)}\ Z_5^{(5)}\ Z_6^{(5)}$
Round 6	$Z_1^{(6)}\ Z_2^{(6)}\ Z_3^{(6)}\ Z_4^{(6)}\ Z_5^{(6)}\ Z_6^{(6)}$
Round 7	$Z_1^{(7)}\ Z_2^{(7)}\ Z_3^{(7)}\ Z_4^{(7)}\ Z_5^{(7)}\ Z_6^{(7)}$
Round 8	$Z_1^{(8)}\ Z_2^{(8)}\ Z_3^{(8)}\ Z_4^{(8)}\ Z_5^{(8)}\ Z_6^{(8)}$
Output Transform	$Z_1^{(9)}\ Z_2^{(9)}\ Z_3^{(9)}\ Z_4^{(9)}$

Q. 7 What are block cipher algorithmic modes ? Describe any two modes. **May 2015**

Ans. :

The block cipher is basic building block for providing data security. In block cipher rather that encrypting one bit at a time, block of bits is encrypted at one go.

The Federal Information Processing Standard (FIPS) defines four modes of operation for block cipher that may be used in a wide variety of applications like symmetric key cryptographic algorithms (DES, AES etc). The modes specify how data will be encrypted and decrypted. The modes included in this standard are :

1. Electronic Codebook (ECB) mode
2. Cipher Block Chaining (CBC) mode
3. Cipher Feedback (CFB) mode and
4. Output Feedback (OFB) mode
5. Counter (CTR) Mode

1. Electronic Codebook (ECB) Mode

In Electronic Codebook (ECB) mode the given plaintext message is divided into blocks of 64 bits each and each 64-bits blocks get encrypted independently. The plaintext block produces ciphertext of same size (64-bits each). The given plaintext is encrypted using same key and transfers the encrypted data (ciphertext) to receiver.

At the receiver end each block is decrypted independently using same key in order to produce original plaintext message of same size i.e. blocks of 64-bits each. The Electronic Codebook (ECB) mode encryption and decryption process is shown in Fig. 3.3 and Fig. 3.4.

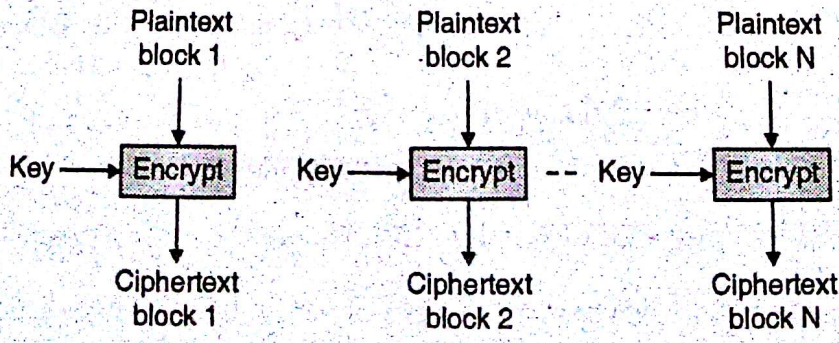


Fig. 3.3 : The Electronic Code Book (ECB) mode encryption process

The drawback of ECB mode is that for the occurrence of more than one plaintext block in the input generates the same ciphertext block in the output, which gives clue to the attacker or cryptanalyst. Only small messages can be encrypted using ECB mode of operation where the chances of repeating the same plaintext message are quite less.

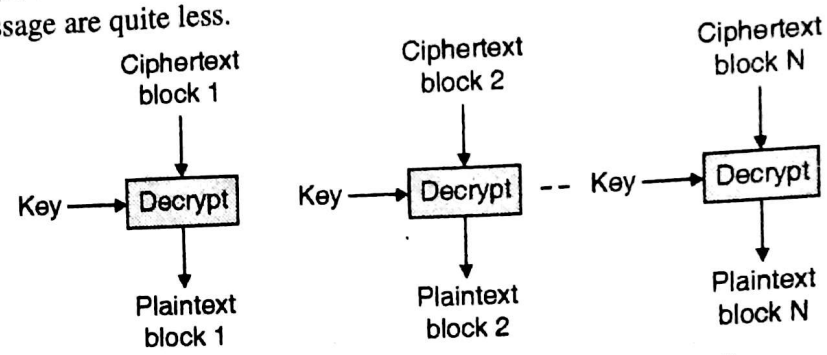


Fig. 3.4 : The Electronic Code Book (ECB) mode decryption process

2. Cipher Block Chaining (CBC) Mode

To overcome the problem of repetition and order independence in ECB even for repeated plaintext the Cipher Block Chaining (CBC) mode is used. In the cipher-block chaining mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.

In CBC mode the first block of the message (plaintext bolck1) is XORed with an initialization vector (IV). Initialization Vector doesn't have special meaning it is simply used to make input message more complicated or unique.

Different criteria for IV are fixed-size input value it should be random or pseudorandom. A good initialization vector should be unique and unpredictable. In all modes of operation plaintext blocks are represented by using P1, P2, P3,.....Pn and corresponding ciphertext blocks are represented by using C1, C2, C3,.....Cn. In case of cipher block chaining mode even if plaintext block repeats in the input, output of CBC mode yields totally different ciphertext blocks as shown in Fig. 3.5.

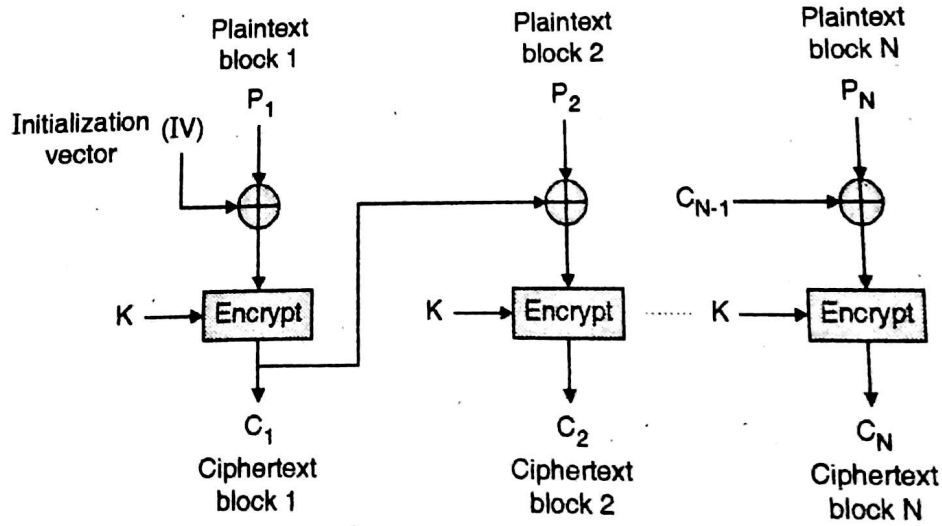


Fig. 3.5 : Cipher Block Chaining (CBC) mode encryption process

CBC mode is applicable whenever large amounts of data need to be sent securely, provided that all data is available in advance (e.g. email, FTP, web etc.). In CBC decryption, ciphertext block 1 get decrypted using same key used during encryption process for all plaintext blocks.

The output of this step is then XOR with initialization vector (IV) and produces plaintext block 1. In next step the ciphertext block 2 is decrypted and its output is XOR with ciphertext block 1 which results plaintext block 2. Repeat the process for all ciphertext block in order to produce original plaintext blocks as shown in Fig. 3.6.

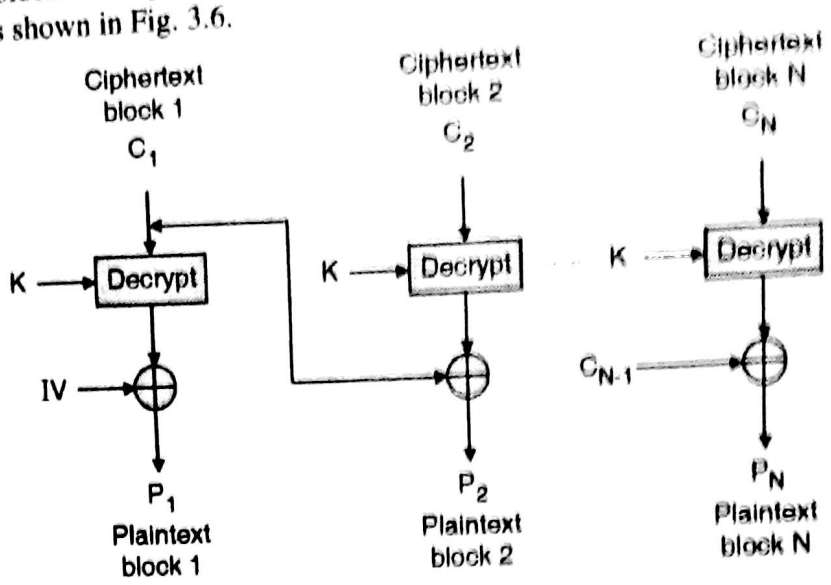


Fig. 3.6 : Cipher Block Chaining (CBC) mode decryption process

Q. 8 Write short note on BLOWFISH.

Ans. :

Blowfish is a symmetric block cipher, designed in 1993 by Bruce Schneier and can be effectively used for encryption and protecting data from unwanted theft. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes).

The algorithm was developed for encrypting 64-bits of plaintext and converts it into 64-bits of ciphertext efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required for encrypting and decrypting data on 32-bit processors.

BLOWFISH Encryption Algorithm

Let us start with the BLOWFISH encryption process, during encryption, the 64-bits plaintext is divided into left plaintext LPT (xL) and right plaintext RPT (xR) 32 bit each.

In the first round, left plaintext (32-bits) XOR with first subkeys of P-array (consists of 18 32-bit subkeys) called Pa1 which generates new output of 32-bits which is again inserted through a transformation function called F, which then XORed with the right plaintext 32 bits of the message to produce a new value as shown in Fig. 3.7.

Now swapping between newly generated LPT (xL) and RPT (xR) was done which undergoes through 16-round Feistel cipher and uses large key-dependent S-boxes. The detail step of BLOWFISH algorithm is shown below.

1. The input is a 64-bit data element, x.
2. Divide x into two 32-bit halves: xL, xR.
3. Then, for i = 1 to 16:
4. xL = xL XOR Pi

5. xR = F(xL) XOR xR
6. Swap xL and xR
7. After the sixteenth round, swap xL and xR again to undo the last swap.
8. Then, xR = xR XOR Pa17 and xL = xL XOR Pa18.
9. Finally, recombine xL and xR to get the ciphertext.

The F function takes the 32-bit input and separates it into 4 bytes (8-bits each). The S-boxes accept 8-bit input and produce 32-bit output.

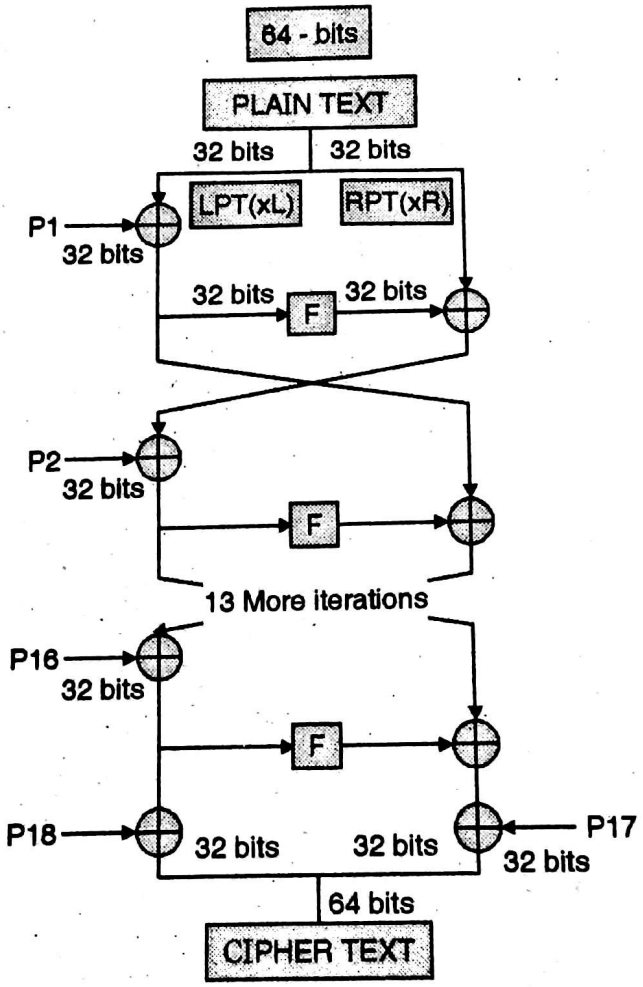


Fig. 3.7 : BLOWFISH Encryption process

The 32-bit output of the S-boxes is then added, XORed and then added again and finally produces 32-bits output ciphertext as shown in Fig. 3.8.

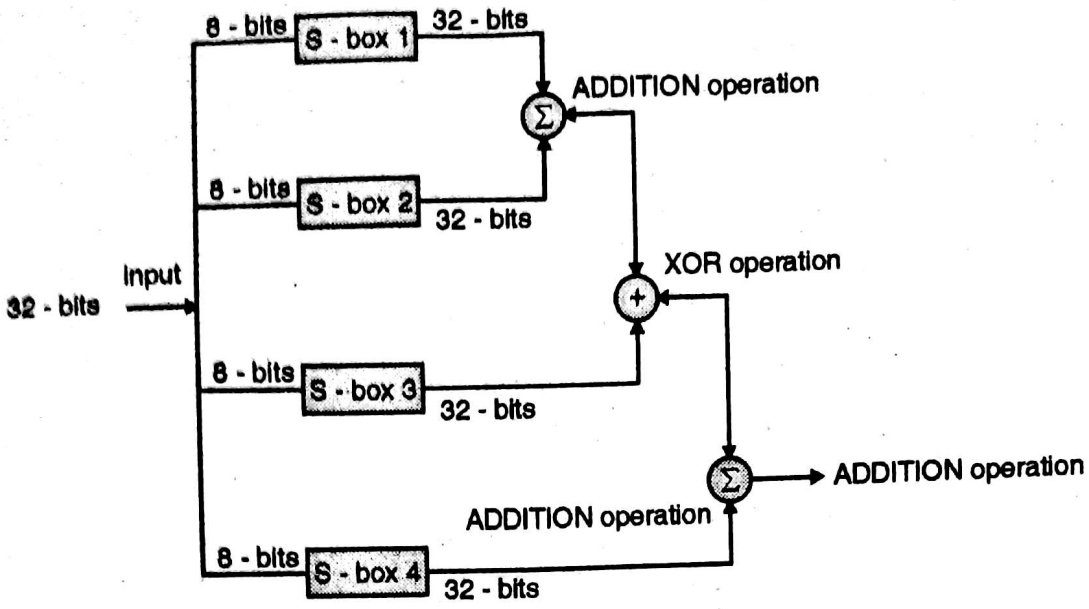


Fig. 3.8 : Blowfish F function

The major difference between DES and BLOWFISH is that DES uses 56-bit key, blowfish can have a key that ranges from 32 to 448-bits.

Blowfish algorithm consists of two parts: a key-expansion part also called **sub key** generation and a data encryption part. Decryption is exactly the same as encryption, except that Pa1, Pa2,..., Pa18 are used in the reverse order.

Q. 9 Explain in detail subkey generation technique.

Ans. :

This process converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes. Blowfish uses a large number of subkeys.

These keys must be pre-computed before any data encryption or decryption. The P-array consists of 18 32-bit subkeys :

Pa1, Pa2,..., Pa18.There are four 32-bit S-boxes with 256 entries each :

S1,0, S1,1,..., S1,255;

S2,0, S2,1,.., S2,255;

S3,0, S3,1,..., S3,255;

S4,0, S4,1,.., S4,255.

Subkey generation steps :

Following are the steps of subkey generation using the Blowfish algorithm :

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi.

   For example :

   Pa1 = 0x254f6aa1

   Pa2 = 0x45b307d4

Pa3 = 0x12298a2f

Pa4 = 0x02506355

2. XOR Pa1 with the first 32 bits of the key, XOR Pa2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to Pa14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits.
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps 1 and 2.
4. Replace Pa1 and Pa2 with the output of step 3.
5. Encrypt the output of step 3 using the Blowfish algorithm with the modified subkeys.
6. Replace Pa3 and Pa4 with the output of step 5.
7. Continue the process, replacing all entries of the P- array, and then all four S-boxes in order, with the output. Total 521 iterations are required to generate all required subkeys.

Q. 10 Write short note on CAST 128.

Ans. :

CAST 128 :

(1) It is a symmetric encryption algorithm.
(2) Developed by Carlisle Adams and Stafford Tavares.
(3) It belongs to Fiestel cipher structure.
(4) It is similar to Data encryption standard.
(5) **Input :** plaintext m1...m64; key K = k1...k128.
(6) **Output :** ciphertext c1...c64.
(7) Key size can vary from 40 bit to 128 bit key.

Q. 11 Write working of AES algorithm in detail. May 2015

Ans. :

- The Advanced Encryption Standard (AES Algorithm) is a Symmetric key cryptographic algorithm published by National Institute for Standards and Technology (NIST) in December 2001.
- The plaintext given is divided into 128 - bit block as consisting of a 4×4 matrix of bytes.
- Therefore, the first four bytes of a 128-bit input block occupy the first column in the 4×4 matrix of bytes. The next four bytes occupy the second column, and so on. AES operates on a 4×4 column-major order matrix of bytes; called as ***state array*** shown in Fig. 3.11. AES also has the notion of a word. A word consists of four bytes that is 32 bits. The overall structure of AES encryption and decryption process is shown in Fig. 3.9.
- The number of rounds are 10, is for the case when the encryption key is 128 bit long. (The number of rounds is 12 when the key is 192 bits and 14 when the key is 256.) Before any round-based processing for encryption can begin each byte of the state (plaintext) is combined with the round key using bitwise XOR operation. Nr stands for number of rounds.
- AES divide plaintext into 16 byte (128-bit) blocks, and treats each block as a 4×4 State array as shown in Fig. 3.9. It then performs four operations in each round consists of several processing

steps like substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. Except for the last round in each case, all other rounds are identical. Final Round doesn't have (MixColumns) it includes only SubBytes, ShiftRows and AddRoundKey.

- The process of transforming the cipher text back into the original plaintext using same encryption key is called as decryption process of AES, during decryption process the set of rounds are reversed.

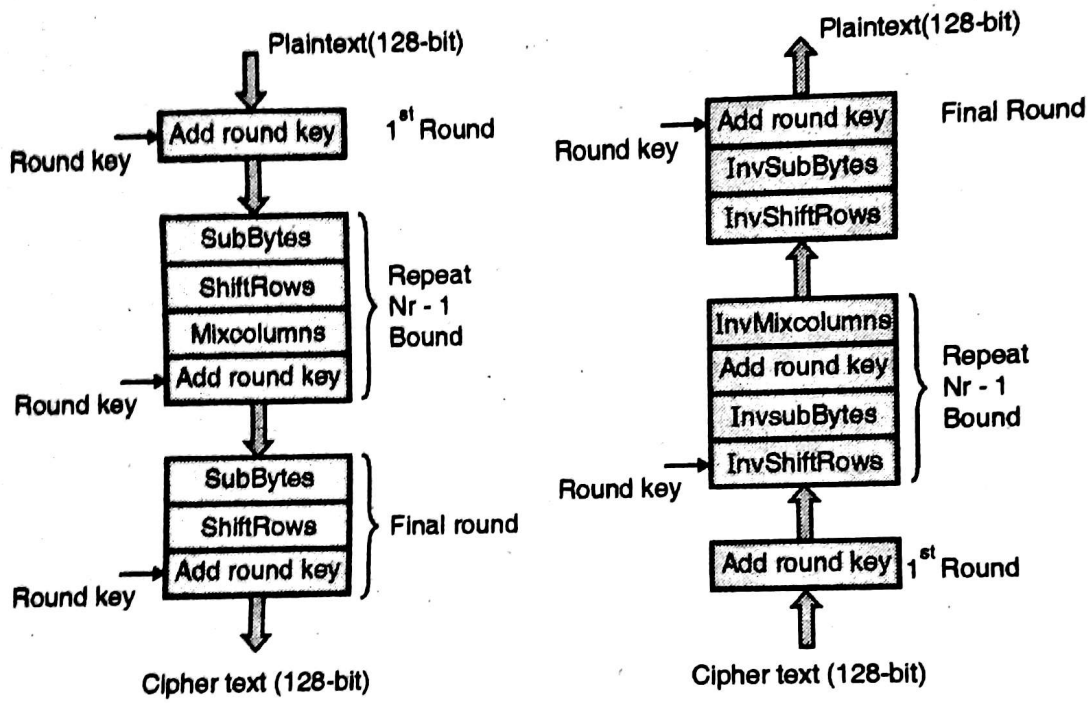


Fig. 3.9 : AES Encryption and Decryption process

Detail Steps for AES Encryption

For encryption, each round consists of the following four steps :

(1) Sub Bytes (2) Shift Rows

(3) Mix Columns, and (4) Add Round Key

1. The SubByte step/Substitute byte :

SubBytes() consists of replacement of each byte using a fixed S-box lookup table as shown in Fig. 3.10 to achieve non-linearity into the 4 × 4 state array (16 byte). It performs roughly the same function as the S- BOX in DES.

It operates on each byte in the state and performs a non-linear substitution in the Galios Filed GF (2^8) field, which is what makes AES a non-linear cryptographic system.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	F
X	0	63	7c	77	7b	F2	6b	6f	C5	30	1	67	2b	Fe	D7	Ab	76
	1	ca	82	C9	7d	Fa	59	47	F0	Ad	D4	A2	Af	9c	A4	72	C0

		Y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	F
	2	b7	Fd	93	26	36	3f	F7	Cc	34	A5	E5	F1	71	D8	31	15
	3	4	C7	23	C3	18	96	5	9a	7	12	80	E2	Eb	27	B2	75
	4	9	83	2c	1a	1b	6e	5a	A0	52	3b	D6	B3	29	E3	2f	84
	5	53	D1	0	Ed	20	Fc	B1	5b	6a	Cb	Be	39	4a	4c	58	Cf
	6	D0	Ef	Aa	Fb	43	4d	33	85	45	F9	2	7f	50	3c	9f	A8
	7	51	A3	40	8f	92	9d	38	F5	Bc	B6	Da	21	10	Ff	F3	D2
	8	Cd	0c	13	Ec	5f	97	44	17	C4	A7	7e	3d	64	5d	19	73
	9	60	81	4f	Dc	22	2a	90	88	46	Ee	B8	14	Be	5e	0b	Db
	a	E0	32	3a	0a	49	6	24	5c	C2	D3	Ac	62	91	95	E4	79
	b	E7	C8	37	6d	8b	D5	4e	A9	6c	56	F4	Ea	65	7a	Ae	8
	c	Ba	78	25	2e	1c	A6	B4	C6	E8	Dd	74	1f	4b	Bd	8b	8a
	d	70	3e	B5	66	48	3	F6	0e	61	35	57	B9	86	C1	1d	9e
	e	E1	F8	98	11	69	D9	8e	94	9b	1e	87	E9	Ce	55	28	Df
	f	8c	A1	89	0d	bf	E6	42	68	41	99	2d	0f	B0	54	bb	16

Fig. 3.10 : S-Box Lookup table for SubBytes

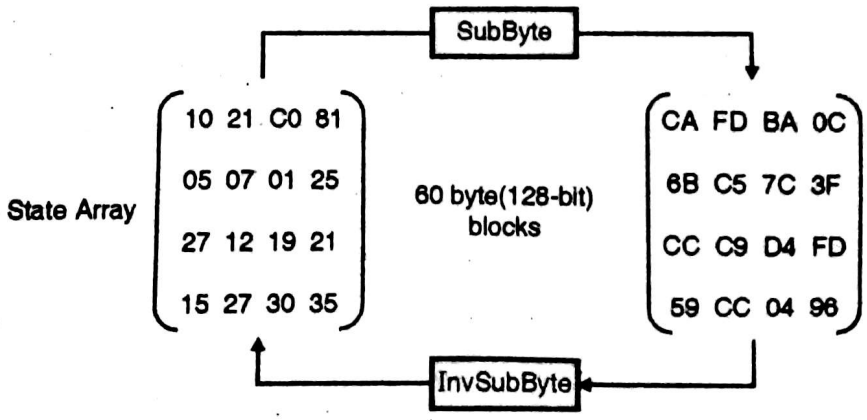


Fig. 3.11 : SubByte transformation

Fig. 3.11 shows the state transformation using SubBytes techniques and if apply reverse called as InvSubBytes transformation which will create original values. For every same two byte value the resulting transformation is also same. It also shows that the InvSubBytes transformation creates the original one. Note that if the two bytes have the same values, their transformation is also the same. The corresponding substitution step used during decryption is called InvSubBytes.

2. ShiftRows :

The output of the SubByte transformation is input to the ShiftRows transformation which consists of rotation of each byte of the state array in the order of a row of data matrix (rotation of row byte positions are done in this step). Each byte of the first row remains unchanged. Each byte of the

second row is rotate over one byte to the left position. Similarly the third and fourth rows are also rotated left by two and three position as shown in Fig. 3.12. The corresponding transformation during decryption process is called Inverse shift row transformation (InvShiftRows).

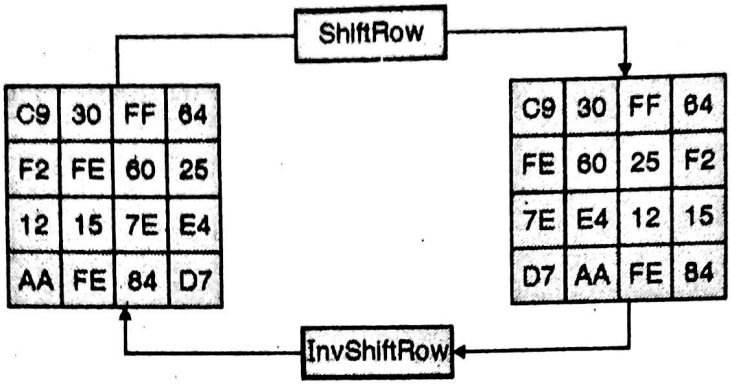


Fig. 3.12 : ShiftRows transformation

3. MixColumns :

Mix Columns performs operation on the state array obtained from ShiftRows column-by-column and each column is multiplied with row of a fixed matrix. This step takes four bytes as an input and produces outputs of four bytes (each input byte affects the output bytes). The four numbers of state arrays of first column are modulo multiplied in Rijandeal's Galios Filed (GF) by a given matrix as shown in Fig. 3.13. In AES MixColumn step along with ShiftRows are primary source for providing complete diffusion to the cipher produced.

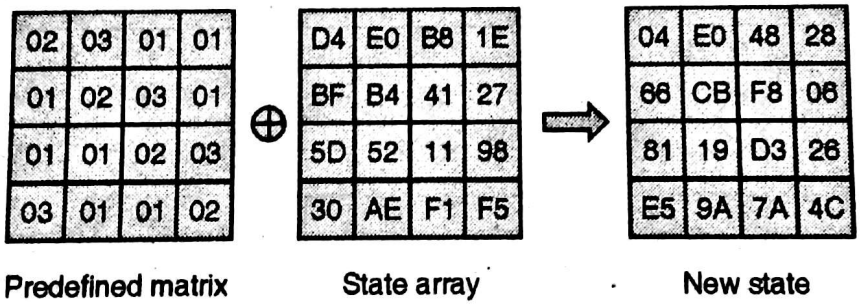


Fig. 3.13 : MixColumns transformation

From Fig. 3.13 on the left hand side, the row of the leftmost matrix is multiply with column of state array (XOR operations) which produces the new state. Perform the same operation on all columns which provides diffusion (mixing data within columns). The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics (modulo multiplied in Rijndael's Galois Filed by a given matrix) as shown. MixColumns step is primary source of diffusion in AES.

4. AddRoundKey :

In the AddRoundKey step, the Round key one generated using Rijndael's key schedule is combined with the new state obtained from MixColumns transformation state.

The round key is added by combining each byte of the state array using bitwise XOR operations. The actual 'encryption' is performed in the AddRoundKey() function, when each byte of state array is XORed with the round key as shown in Fig. 3.14.

04	E0	48	28
66	CB	F8	06
81	19	D3	26
E5	9A	7A	4C

A0	88	23	2A
FA	54	A3	6C
FE	2C	39	76
17	B1	39	05

A4	68	6B	02
9C	9F	5B	6A
7F	35	EA	50
F2	2B	43	49

Fig. 3.14 : AddRoundKey

The same process of AddRoundKey is applied for nine rounds i.e Repeat SubByte, ShiftRows, MixColumns step and XOR with Round key 9 more times.

Except for the last round in each case, all other rounds are identical. Final Round doesn't have MixColumns step it includes only SubBytes, ShiftRows and RoundKey.

Finally an output cipher text will obtain after performing detail steps of AES. A set of reverse rounds are applied (i.e.InvShiftRows, InvSubBytes, AddRoundKey and InvMixcolumns) to transform cipher text back into the original plaintext using the same encryption key called Decryption process of AES.

AES Decryption

Decryption occurs through the function AddRoundKey ( ), plus the inverse AES functions InvShiftRows (), InvSubBytes (), InvMixColumns () and AddRoundKey () does not require an inverse function, as it simply XORs the state with the subkey (XOR encrypts when applied once, and decrypts when applied again).

Q. 12 Compare AES and DES. **Dec. 2014**

Ans. :

Comparison of AED and DES :

Sr. No.	DES	AES
1.	Data encryption standard takes 64-bit plaintext as a input and creates 64-bit Ciphertext i.e. it encrypts data in block of size 64-bits per block.	It allows the data length (plain text size) of 128, 192 and 256 bits.
2.	In DES plaintext message is divided into size 64-bits block each and encrypted using 56-bit key at the initial level.	AES divide plaintext into 16 byte (128-bit) blocks, and treats each block as a 4×4 State array and supporting three different key lengths, 128, 192, and 256 bits.
3.	The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each rounds.	The number of rounds are 10, is for the case when the encryption key is 128 bit long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256.)
4.	DES uses 56-bit keys so that there are 2^{56} possible key combinations which is roughly equal to 7.2×10^{16} keys required	AES is stronger than DES because of key size vary from round to round.

Sr. No.	DES	AES
	to break DES cipher.	
5.	Different versions of DES are double DES and triple DES is added.	AES doesn't have any future version.
6.	DES doesn't use Mix Column, Shift Rows method during encryption and decryption process	AES uses Mix Column, Shift Rows method during encryption and decryption process
7.	DES, double DES and Triple DES (168-bit key) are vulnerable to brute force attacks.	AES also are vulnerable to brute force attacks.

❑❑❑

Chapter 4 : Public Key Cryptography

Q. 1 What is principle of public key cryptography ?

Ans. :

Public key algorithms also called as asymmetric key algorithms.

Two different keys are used during encryption and decryption process (one key for encryption and second key used at the time of decryption). RSA algorithm is the best example of asymmetric key cryptography as shown in Fig. 4.1.

Private key (only known to owner).

Public key(possibly known to everyone).

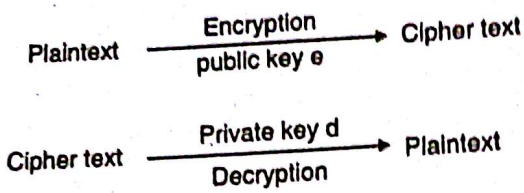


Fig. 4.1

It is easily configurable than secret key.

Q. 2 Write a detail note on : RSA algorithm (Public key algorithm). **Dec. 2013**

Ans. :

Ron Rivest, Adi Shamir and Len Aldeman have developed this algorithm (Rivest-Shamir-Aldeman) in 1978. It is a public-key encryption algorithm. It is a block-cipher which converts plain text into cipher text at sender side and vice versa at receiver side.

The algorithm works as follows :

1. Select two prime numbers a and b where $a \neq b$.
2. Calculate $n = a * b$
3. Calculate $\phi(n) = (a - 1) * (b - 1)$.
4. Select e such that, e is relatively prime to $\phi(n)$ i.e. gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$.
5. Calculate of such that $d = e^{-1} \bmod \phi(n)$ or $ed \bmod \phi(n) = 1$.
6. Public key = {e,n}, private key = {d,n}.
7. Find out ciphertext using the formula,

   $C = P^e \bmod n$ where, $P < n$ and

   C = Ciphertext, P = Plaintext, e = Encryption key and n = Block size.
8. $P = C^d \bmod n$. Plaintext P can be obtain using the given formula.

Where, d = decryption key.

Both sender and receiver know the value of n. In addition, the sender must know encryption key 'e' and receiver must know decryption key 'd'.

Example :

1. Select two prime numbers a = 13, b = 11.
2. $n = a*b = 13 * 11 = 143$.
3. $\phi(n) = (13 - 1) * (11 - 1) = 12 * 10 = 120$.
4. Select e = 13, gcd (13, 120) = 1.
5. **Finding d :**

   $e*d \bmod \phi(n) = 1$

   $13 * d \bmod 120 = 1$

   Do the following procedure till you are not getting a integer numbers

$$d = \frac{(\phi(n) * i) + 1}{e}$$

$$d = \frac{(120 + 1)}{13} = \frac{121}{13} = 9.30 \ (i = 1) \qquad \text{where, } i = 1 \text{ to } 9$$

$$d = \frac{240 + 1}{13} = \frac{241}{13} = 18.53 \ (i = 2)$$

$$d = \frac{360 + 1}{13} = \frac{361}{13} = 27.76 \ (i = 3)$$

$$d = \frac{480 + 1}{13} = \frac{481}{13} = 37$$

Hence **d = 37**

6. Hence public key = {13, 143} and Private key = {37, 143}
7. Encryption :

   Consider any integer as a plaintext (P)

   Such that P < n

   Example : 13 $\because (13 < 143)$

Now, $C = P^e \bmod n$

$C = 13^{13} \bmod 143$

Here to find out $13^{13} \bmod 143$, use the following procedure

$13 \bmod 143 = 13$

$13^2 \bmod 143 = 169 \bmod 143 = 26$

$13^4 \bmod 143 = 26^2 \bmod 143 = 104$

$13^8 \bmod 143 = 104^2 \bmod 143 = 91$

$\therefore C = [(13^8 \bmod 143) * (13^4 \bmod 143) * (13 \bmod 143)] \bmod 143$

$= [91 * 104 * 13] \bmod 143$

$= 52$

8. **Decryption :**

$P = C^d \bmod n$

$= 52^{37} \bmod 143$

Again use above mentioned procedure to find out $52^{37} \bmod 143$. As

$52 \bmod 143 = 52$

$52^2 \bmod 143 = 130$

$52^4 \bmod 143 = (130)^2 \bmod 143 = 26$

$52^8 \bmod 143 = (26)^2 \bmod 143 = 104$

$52^{16} \bmod 143 = (104)^2 \bmod 143 = 91$

$52^{32} \bmod 143 = (91)^2 \bmod 143 = 130$

Hence,

$P = 52^{37} \bmod 143$

$= [(52^{32} \bmod 143) * (52^4 \bmod 143) * (52 \bmod 143)] \bmod 143$

$= [130 * 26 * 52] \bmod 143$

$= 13$

Q. 3 Using the RSA algorithm encrypt the following :

(i) p = 3 , q = 11, e = 7, M = 12

(ii) p = 7 , q = 11, e = 17, M = 25

(iii) Find the corresponding ds for (i) and (ii) and decrypt the ciphertexts. June 2015

Ans.:

Use RSA Algorithm

(i) Consider p as *a* and q as *b* as per our notations for prime numbers.

Step 1 : Prime numbers a = 3, b = 11

Step 2 : n = a * b = 33

Step 3 :

$\phi(n) = (a - 1) * (b - 1)$

$= (3 - 1) * (11 - 1)$

$= 2 * 10$

$= 20$

Step 4 : Select e such that it is relatively prime to $\phi(n)$ i.e. $\gcd(e, \phi(n)) = 1$

$\gcd(e, 20) = 1$

$\gcd(7, 20) = 1$

$e = 7$ is given.

Step 5 : Calculate d such that

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

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

$$7 * d \bmod 20 = 1$$

$$\boxed{d = \frac{(\phi(n) * i) + 1}{e}} \qquad \text{Where I = 0 to 9}$$

Find d such that it is divisible by e.

Consider i = 1 you can continue till d will get integer value, Q(n) = 20 and e= 7

$$d = ((20 * 1) + 1)/7 = 21/7 = 3$$

$$\boxed{d = 3}$$

Step 6 : Public key = {e, n} = {7, 33}

Private key = {d, n} = {3, 33}

Step 7 : Calculate cipher text message for given plain text message.

Plain text message given is M= 12 we consider M as i.e. P = 12

$$C = p^e \bmod n \text{ where } p < n$$

$$= 12^7 \bmod 33$$

$$C = 12$$

Step 8 : Calculate plain text message.

$$P = c^d \bmod n$$

$$= 12^3 \bmod 33$$

$$P = 12$$

$$\boxed{P = 12}$$

When we convert plain text message into cipher text the corresponding cipher text yields the same plain text.

(ii) p = 7 , q = 11, e = 17, M = 25

By using RSA Algorithm,

Step 1 : Prime numbers are 7 and 11 as per our notations a = 7, b = 11

Step 2 : n = a * b = 7 * 11 = 77.

Step 3 :

$$\phi(n) = (a - 1) * (b - 1)$$

$$= (7 - 1) * (11 - 1)$$

$$= 6 * 10$$

$$= 60$$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ(n)) = 1

e is given as 17

gcd (17,60) = 1 (gcd must be 1)

Step 5 : Calculate d such that

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

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

$$17 * d \bmod = 1$$

Using RSA algorithm

$$d = \frac{(\phi(n) * i) + 1}{e} \quad \text{where } i = 1 \text{ to } 100$$

$$= (60*1 + 1/17)$$

$$= \mathbf{3.58}$$

d must be completely divisible by 'e'.

= After putting value of i = 15 into above formula we got value of d

= (60*15 + 1/ 17) = 53

$$\boxed{d = 53}$$

Step 6 : Public key = {e, n} = {17, 77}

Private key = {d, n} = {53, 77}

Step 7 : Calculate cipher text message for given plain text message M = 25.

Plain text denoted as P = 25 (m denoted as p)

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

$$= 25^{17} \bmod 77$$

It can be represented as

$$C = 9$$

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 9 to the receiver then receiver can calculate plain text p.

$$P = C^d \bmod n$$

$$= 9^{53} \bmod 77$$

$$P = 25$$

Decryption process always yields original plain text message

$$\boxed{\therefore P = 25}$$

(iii) Find the corresponding ds for (i) and (ii) and decrypt the ciphertexts

Decryption key for question (i) is d =3 and for question (ii) is d= 53 which will decrypt the message successfully.

There are four possible attacks on RSA as follows,

1. **Brute force attack :** Hacker tries all possible private keys.
2. **Mathematical attacks :** Hackers attacks on n i.e. tries to factorize the product of two prime numbers.
3. **Timing attacks :** It totally depends on running time of decryption algorithm.
4. **Chosen Cipher text attack :**
   Hacker tries to attack on the properties of RSA algorithm.

Q. 4 Define key generation ?

Ans. :

Key generation is the process generating keys using symmetric or asymmetric key cryptography. The key can be generated using random or pseudo-random key bit generator which uses the functions of passwords and PINs. It is standard (ANSI X9.17) way to generate pseudorandom DES keys.

Q. 5 Illustrate Diffie Hellman key exchange algorithm with suitable example.

Ans. :

The **Diffie Hellman** algorithm was widely known as Key exchange algorithm or key agreement algorithm developed by Whitfield *Diffie* and Martin *Hellman* in 1976.Diffie Hellman algorithm is used to generate same (symmetric) private cryptographic key at sender as well as receiver end so that there is no need to transfer this key from sender to receiver.

Remember that Diffie Hellman algorithm is used only for key agreement not for encryption or decryption of message. If sender and receiver want to communicate with each other they first agree on the same key generated by Diffie Hellman Algorithm later on they can use this key for encryption or decryption. Let us start with the algorithm.

Steps of Diffie Hellman Algorithm :

1. The first step is that if Ramesh wants to communicate with Suresh they must agree on two large prime numbers p and q.
2. Ramesh selects another secret large random integer number a, and calculate R such that

$$R = q^a \bmod p$$

3. Ramesh sends this R to suresh.
4. Suresh independently selects another secret large random integer number b, and calculate S such that.

$$S = q^b \bmod p$$

5. Suresh sends the number S to Ramesh.
6. Now Ramesh is calculating his secret key by using $R_K = S^q \bmod p$
7. Suresh is calculating his secret key S_K by using

$$S_K = R^b \bmod p$$

8. If $R_K = S_K$ then Ramesh and Suresh can agree for future communication called as key agreement algorithm.
9. We have $R_K = S_K = K$ hence proved. (K is called symmetric key).

For example :

1. Ramesh and Suresh are agree on two large prime numbers say $p = 17$ and $q = 7$.
2. Ramesh selects another secret large random number 5 i.e. $a = 5$ and calculate R such that

$$R = q^a \bmod p = 7^5 \bmod 17 = 11$$
$$= (7 \times 7 \times 7 \times 7 \times 7) \bmod 17 = 11$$

3. Ramesh sends number R to Suresh.
4. Suresh selects another secret large random number 3. i.e. $b = 3$ and calculate S such that

$$S = q^b \bmod p = 7^3 \bmod 17 = 3$$
$$= (7 \times 7 \times 7) \bmod 17 = 3$$

5. Suresh sends number S to Ramesh.
6. Ramesh now calculates its secret key R_K as follows :

$$R_K = S^a \bmod p = S^5 \bmod 17$$
$$\therefore R_K = 3^5 \bmod 17 = 5$$
$$= (3 \times 3 \times 3 \times 3 \times 3) \bmod 17 = 5.$$

7. Suresh is calculating his secret key S_K as follows :

$$S_K = R^b \bmod p = R^3 \bmod 17 = 11^3 \bmod 17 = 5$$

8. If $R_K = S_K$ then Ramesh and Suresh can agree for future communication.
9. We know that if $R_K = S_K = K = 5$. Hence proved.

Q. 6 If generator g = 2 and n or p = 11 using Diffie Hellman algorithm solve the following :

(i) Show that 2 is primitive root of 11

(ii) If A has public key 9 what is A's private key ?

(iii) If B has public key 3 what is B's private key ?

(iv) Calculate shared secret key. Dec. 2013

Ans. :

(i) To show that 2 is primitive root of 11 :

In general terms, the highest possible exponent to which a number can belong (mod n) is Q(n). Where Q(n) is called as Euler totient function which states that how many numbers are between 1 and n – 1 that are relatively prime to n.

According Euler's theorem :

It states that for every a and n that are relatively prime.

If $a^{\phi(n)} = 1 \bmod n$

For example :

As mention in (i)

$a = 2$ and $n = 11$

Calculate $\phi(n)$ i.e. $\phi(11) = \{ 1 \text{ to } 10 \} = 10$

According to Euler's theorem

$$a^{\phi(n)} = 1 \bmod n$$

$$2^{10} = 1 \bmod 11$$

$$1024 = 1 \bmod 11$$

i.e. $1024 \bmod 11 = 1$ and

$$1 \bmod 11 = 1.$$

Hence 2 is primitive root of 11.

(ii) If 'A' has public key 9 then private key is :

1. Say A as Ramesh and B as Suresh.

   Representing g as a q (i.e. $g = 2 = q$)

   Using Diffie Hellman algorithm

2. Suresh now calculates R such that

$$R = q^a \bmod p \quad [\text{Here } q = 2 \text{ and } p = 11]$$

$$= 2^9 \bmod 11 \quad [a \text{ is 9 public key}]$$

$$R = 6$$

3. Ramesh now sends R to Suresh.

(iii) Suresh has public key 3 (it's random number) Suresh calculates S such that

$$S = q^b \bmod p = [q = 2, p = 11, b = 3]$$

$$S = q^b \bmod p = 2^3 \bmod 11$$

$$S = 8$$

Suresh now sending S to Ramesh.

(iv) Now Ramesh and Suresh calculating their secret keys individually.

1. Ramesh calculates it's secret key R_K as follows :

$$R_K = S^a \bmod p \qquad [S = 8, p = 11, a = 9]$$

$$= 8^9 \bmod 11 = 7$$

2. Suresh calculates it's secrete key S_K as follows :

$$S_K = R^b \bmod p \qquad [R = 6, b = 3, p = 11]$$

$$= 6^3 \bmod 11 = 7$$

Shared secret keys of Ramesh and Suresh are 7.

Hence, $\boxed{R_K = S_K = 7}$

Note : In above example we have solved by using our notations mentioned in Diffie Hellman algorithm. So here A denotes Ramesh, B denotes Suresh, g denotes q and p is same as p. Students can use any notations.

Q. 7 A and B decide to use Diffie Hellman key exchange where p = 13, g = 2, each choose his own secret no. and exchange numbers 6 and 11.

(i) What is common secret key ?

(ii) What are their secret numbers ?

(iii) Can intruder m gain any knowledge from protocol run if he sees p, 9 of and two keys 6 and 11. If yes, show how ? MU - May 2015

Ans. :

According to Diffie Hellman algorithm,

Let us say A as Ramesh and B as Suresh

Also p = 13 and g = 2

Here in our example we are denoting g as q,

$$\therefore p = 13,$$

$$q = 2$$

Secret numbers denoted as, a = 6 and b = 11 by using Diffie Hellman algorithm.

1. Ramesh and Suresh agree on two large prime numbers p = 13 and q = 2.
2. Ramesh selects another secret no. a = 6 and calculate R such that

$$R = q^a \bmod p \; [q = 2, a = 6, p = 13]$$

$$= 2^6 \bmod 13$$

$$R = 12$$

3. Ramesh sends R to Suresh
4. Suresh selects another large random number b = 11 and calculate S such that

$$S = q^b \bmod p \quad [q = 2, b = 11, p = 13]$$

$$= 2^{11} \bmod 13$$

$$S = 7$$

5. Suresh sends S to Ramesh
6. Ramesh now calculates it's secret key R_K as follows :

$$R_K = s^a \bmod p \; [S = 7, a = 6, p = 13]$$

$$= 7^6 \bmod 13$$

$$R_K = 12$$

7. Suresh is calculating his secret key S_K as follows :

$$S_K = R^b \bmod p \; [R = 12, b = 11, p = 13]$$

$$= 12^{11} \bmod 13$$

$S_K = 12$

(i) Shared secret key of Ramesh and Suresh is

$R_K = S_K = 12$ [A and B = 12]

(ii) Secret numbers of Ramesh and Suresh are

R = 12 and S = 7

(iii) If intruder m knows p, g and a, b then what will happen. [Here g = q]

Case I :

Value of p, q, a, b are known to m represented as

Ramesh	m	Suresh
p = 13, q = 2	p = 13, q = 2	p = 13, q = 2

Use Diffie Hellman algorithm,

After selecting large prime numbers, it's time to select random numbers a and b.

The secret random number selected by Ramesh and Suresh are,

Ramesh	m	Suresh
a = 6	a = 8, b = 6	b = 11

Case 2 :

Consider m as intruder selected two random numbers say a = 8 and b = 6 as his own secret key, because he wants to calculate value as R and S, as he intercepted conversion between Ramesh and Suresh

Ramesh	Intruder m	Suresh
$R = q^a \bmod p$	$R = q^a \bmod p$	$S = q^{13} \bmod p$
$= 2^6 \bmod 13$	$= 2^8 \bmod 13$	$= 2^{11} \bmod 13$
$= 12$	$R = 9$	$S = 7$
	$S = q^b \bmod 13$	
	$= 2^6 \bmod 13$	
	$= 12$	

Case 3 :

Following are the values available with Ramesh, Suresh and intruder m

Ramesh	intruder m	Suresh S
R = 12	R = 9, S = 12	S = 7

Case 4 :

Ramesh sending his R = 12 to Suresh but intruder m sending his own R = 9 to Suresh instead of R = 12. Suresh sending his S = 7 to Ramesh, here again intruder m sending his own value of S = 12 to Ramesh. In this case Ramesh and Suresh doesn't aware that which values they are sending and receiving [Intruder m sending his own value Because of his interception]. Following are the new values with Ramesh, Suresh and intruder m.

Ramesh	Intruder m	Suresh
R = 12, S = 12	R = 12, S = 7	S = 7
		R = 9

Case 5 : Based on above values Ramesh, Suresh and Intruder m calculating secret keys.

Ramesh	Intruder m	Suresh
S = 12, a = 6, p = 13	S = 7, R = 12 a = 8, b = 6, p = 13	R = 9, b = 11 p = 13
$R_K = S^a \bmod p$ $= 12^6 \bmod 13$ $R_K = 1$	$R_K = S^a \bmod p$ $= 7^8 \bmod 13$ $= 3$ $S_K = R^b \bmod p$ $= 12^6 \bmod 13$ $= 1$	$S_K = R^b \bmod 11$ $= 9^{11} \bmod 11$ $S_K = 3$

Case 5 : Man-in-the-middle attack

Think what is happening ? Ramesh is thinking that value of his secret key is 1 and Suresh also thinking that value of his secret key is 3. But actual communication is intercepted by intrude m. During real communication between Ramesh and Suresh intruder m sending his own secret keys to Ramesh and Suresh. If Ramesh sending his secret key $R_K = 1$ to Suresh because of **man-in-the-middle attack**. Intruder m sending his secret key $R_K = 3$ to Suresh. In return Suresh is sending his secret key $S_K = 3$ to Ramesh, intruder m sending his secret key $S_K = 1$ to Ramesh.

Both Ramesh and Suresh not aware that communication intercepted by intruder m such type of attack is called as **man-in-the-middle attack**.

Q. 8 State and Prove Fermat's theorem.

Ans. :

Fermat theorem plays an important role in public key cryptography. For this theorem to understand one has to have knowledge of Prime number, Co-prime number, prime factorization and GCD i.e. greatest common divisor that has already been explained in this chapter.

Theorem :

For any prime number p , a is the integer which is not divisible by p then

$$a^{p-1} \equiv 1 (\text{mod } p) \quad \ldots(1)$$

A variant of this theorem is

If p is a prime and a is a co prime to p (i.e gcd(a, p) = 1) then,

$$a^p \equiv a (\text{mod } p) \quad \ldots(2)$$

Basically this theorem is useful in public key RSA and primarily testing.

Let us have a = 3 and p = 5 then as per the above theorem in Equation (1) we have

$3^{5-1} \equiv 3^4 = 81 \equiv 1 (\text{mod } 5)$.

Since on dividing 81 with 5 will have remainder 1.

Hence proof above theorem.

Considering another form of theorem in Equation (2).

Let us have a = 3 and p = 5 then we have

$$a^p = 3^5 = 243.$$

Now we calculate 243 mod 5, we will have result 3.

a mod p = 3 mod 5 = 3

Hence, $3^5 = 3 \bmod 5$.

□□□

Chapter 5 : Cryptographic Hash Functions

Dec. 2012

Q. 1 Explain cryptographic hash function

Ans. :

The process of transforming input message *m* into a fixed size string (called as hash value *h*) is called as hash function and it is denoted by *H*. Here *h* is the output of hashing function applied on input message *m*.

$$h = H(m)$$

Hash function protects the integrity of the message. If attacker tries to modify the original message then the contents of original message may changed it can be identifies by applying Hashing algorithm. The most popular hashing algorithms are MD5 & SHA. Following sections gives details on MD5 and SHA.

Q. 2 Explain cryptographic hash function criteria. Also write short note on : MD5.

Dec. 2012, May 2015

Ans. :

It was developed by Ron Rivest. This algorithm takes an input of arbitrary length and 128 - bit message digest is produced. The input message is produced in 512 - bit blocks. Fig. 5.1 shows processing of a message to produce message digest. Following steps explains the procedure of MD5.

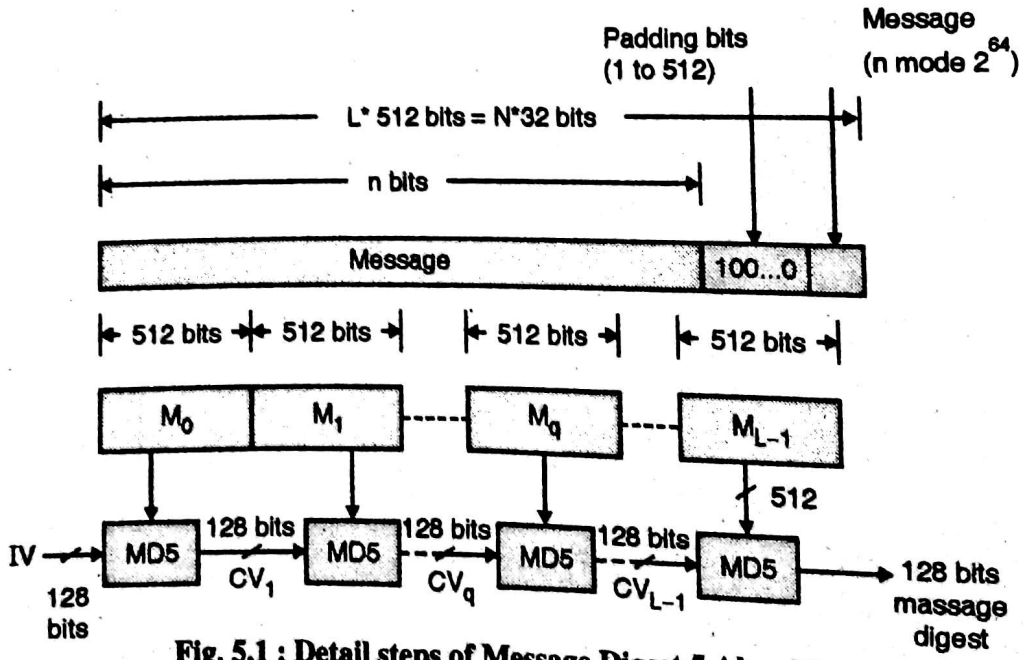


Fig. 5.1 : Detail steps of Message Digest 5 Algorithm

(1) Append padding bits :

The message is padded to make the length of message is 448 mod 512. The length of the padded message is 64 bits less than an integer multiple of 512. The padding message consists a single 1-bit followed by 0 bits. The length of padding bits is in between 1 to 512.

(2) Append length :

64 bits of original message is appended to the result of above step 1. It is appended such that least significant bytes to most significant byte. The output of step 2 yields a message of integer multiple of 512 bits. As $M_0, M_1, \ldots M_q \ldots M_{L-1}$. The total length of expanded message is L * 512 bits.

(3) Initialize MD Buffer :

A 128 - bit buffer is used to store the intermediate as well as final result. A buffer is represented as four 32-bit registers as P, Q, R, S.

P = 67452301

Q = EFCDA1389

R = 98BADCFE

S = 10325476.

It used a little - endian methods. Hence initial values (IV) are represented as,

P = 01 23 45 67

Q = 89 AB CD EF

R = FE DC BA 98

S = 76 54 32 10.

(4) Process Message in 512-bit (16 word of 32 bit) blocks :

It consists of four rounds of processing as shown in Fig. 5.2. These four rounds have similar structure but differ in primitive logical function referred as A, B, C, D.

Each round takes input 512-bit block, processed it and produces 128 bit output. The output of fourth round is added to the first round CV_q to produce CV_{q+1} using addition modulo 2^{32}.

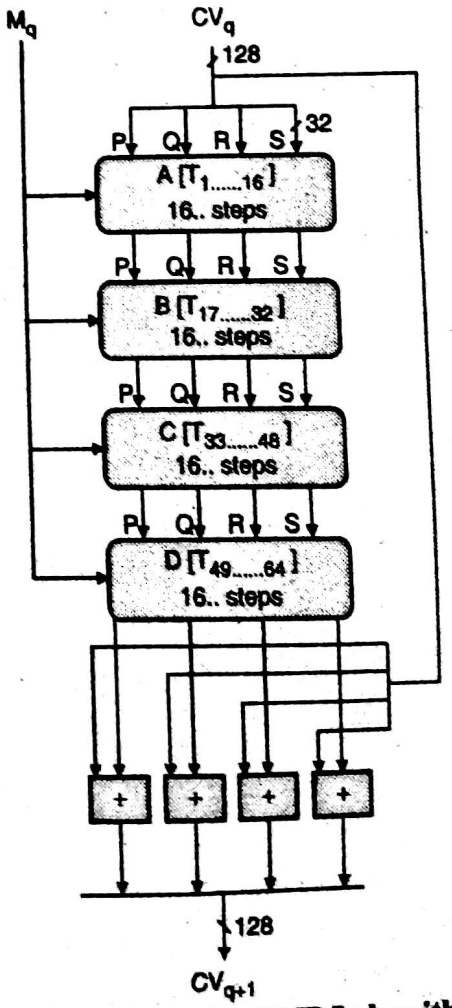


Fig. 5.2 : Four rounds of MD5 algorithm

(5) Output :

After processing all L 512-bit blocks, the 128 bit message digest is produced as a output.

The entire MD5 process can be summarized as follows :

CV0 = IV
CVq+1 = Sum32(CVq, RFd [Mq,RFc [Mq,,RFb [Mq, RFa [Mq, CVq]]]])
MD5Sum = CVL
Where,
IV = the initial value of the PQRS buffer, mentioned in step 3
Mq = the qth 512-bit block of the message
CVq = the chaining variable processed with the q-th block of message
RF = the round function using primitive logical function a, b, c, d.
MD5Sum = the final hash result or message digest
Sum32 = addition modulo 232

Q. 3 Explain cryptographic hash function criteria. Also explain SHA-1 and different steps of working of SHA-1. Dec. 2012 . May 2014

Ans. :

The SHA was developed by NIST in 1993. It is referred as Secure Hash Algorithm-1. SHA - 1 takes an input message of a maximum length less than 2^{64} bits and produced an output of 160 bit message digest. The overall processing of SHA-1 is much similar to MD5. The processing is explained as follows.

(1) Append padding bits :

Padding means addition of bits to the original message. To make length of original massage to a value 64 bits less than multiple of 512. The message is padded to make the length of message 448 mod 512. The length of the padded message is 64 bits less than an integer multiple of 512. The padding message consists of a single 1-bit, followed by many 0 bits as required. The length of padding bits is in between 1 to 512.

(2) Append length :

A block of 64-bit is appended to a message. 64 bits of original message is appended to the result of above step 1 (Original message + Padding). It is appended such that least significant bytes to most significant byte.

(3) Initialize MD5 Buffer :

A 160-bit buffer is used to store the intermediate as well as final result. The buffer is represented as five 32-bit registers as P, Q, R, S, T, as.

P = 67452301
Q = EFCDAB89
R = 98BADCFE
S = 10325476
T = C3D2E1FO

It uses a big-endian method. First four registers are same as MD5. These five registers P, Q, R, S, T are represented as,

P = 67 45 23 01

Q = EF CD AB 89

R = 98 BA DC FE

S = 10 32 54 76

T = C3 D2 E1 FO

(4) Process message in 512-bits (32 bit 16 word) block :

It consists of four rounds of 20-step each as shown in Fig. 5.3. These rounds referred as F1, F2, F3, F4 have similar structure. These rounds used different primitive logical function. Each round takes input 512-bit block processed it and produced 160 bit output. The output of fourth round is added to the first round CV_q to produce CV_{q+1}. Each round also uses an additive constant k_t, where $0 \leq + \leq 79$.

K_1 = 5A 827999

K_2 = 6 ED9EBA1

K_3 = 8F1BBCDC

K_4 = CA62C1D6

(5) Output :

After processing all L 512 bit blocks, the 160 bit message digest is produced as output. The SHA compression function uses a feed forward operation where the chaining variable CVq input of the first round is added to the output obtained (last step) after execution of 80 steps to produce the next chaining variable CVq+1 as shown in Fig. 5.3.

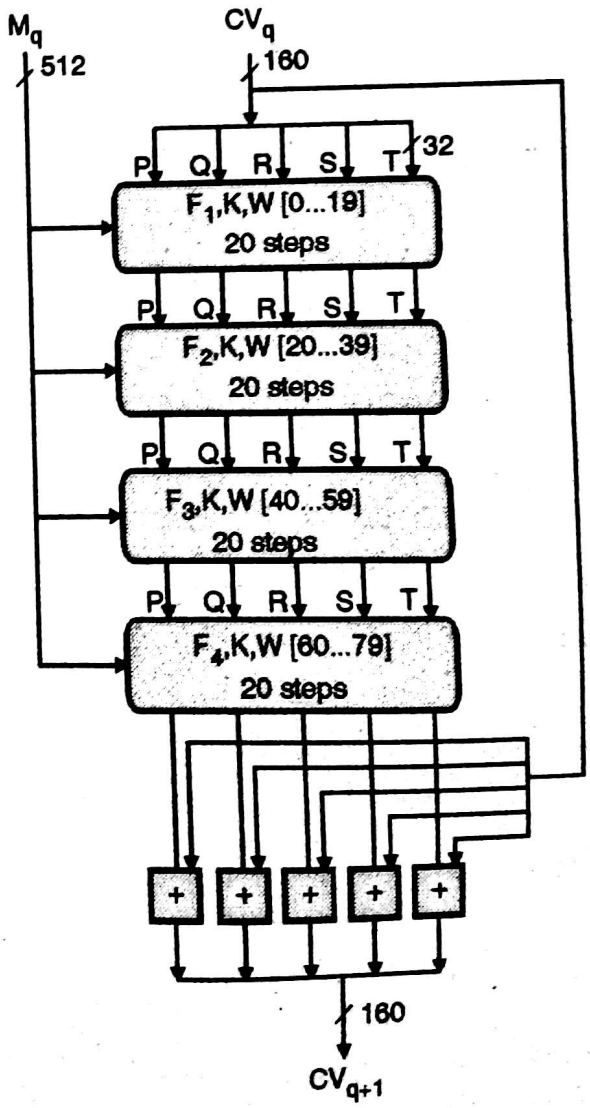


Fig. 5.3 : Four rounds of Secure Hash Algorithm

The entire SHA-1 process can be summarized as follows:

CV0 = IV
CVq+1 = Sum32 (CVq, F4 [M60...79, F3 [M40...59, F2 [M20...39, F1 [M0...19,CVq, K0...19], K20...39] ,K40...59] , K60...79])
SHAr = CVq
where
IV = initial value of the PQRST buffer, used to deal with the first block in a chaining mode
Mq = the qth 512-bit block of the message
CVq = the chaining variable processed with the q-th block of message
F1[_ _ _] = output of the first round consisting of 20 steps
F2[_ _ _] = output of the second round
F3[_ _ _] = output of the third round
F4[_ _ _] = output of the fourth round
Sum32 = addition modulo 232
SHAr = the final hash result or message digest

Q. 4 Compare and contrast SHA-1 and MD-5. Dec. 2012. May 2013

Ans. :

Both are derived from MD4. Both are quite similar. They differ from each other in design goals.

Sr. No.	SHA-1	MD5
1.	It uses a 160-bit message digest. Hence it is stronger against Brute - force attacks than MD5.	It uses a 128 bit message digest. Hence it is weaker than SHA-1 against Brute - force attacks.
2.	SHA-1 is not vulnerable against cryptanalysis.	MD5 is vulnerable against cryptanalysis
3.	SHA-1 is slower than MD5.	MD5 is faster than SHA-1.
4.	It uses big - endian method to represent the message.	It uses a little endian method to represent the message.
5.	SHA has 20 rounds.	MD5 has 64 rounds.
6.	Bit rotation counts for SHA-1 are the same for all rounds.	In MD5 each round has its own bit rotation counts.

Q. 5 Write short note on : Digital signature. Dec. 2012

Ans. :

Digital signatures are essential in today's modern world to verify the sender of a document's and his identity. A digital signature is represented in a computer as a string of binary digits and computer is using a set of rules and regulations (algorithm) to identify the person signing the document as well as the originality of the data can be verified. A digital signature is defined the signature generated electronically from the digital computer to ensure the identity of the sender and contents of the message

cannot be modified during transmission process. Digital signature techniques achieve the authenticity, integrity and non-repudiation of the data over Internet.

Concept of digital signature is that sender of a message uses a signing key (Private Key) to sign the message and send that message and its digital signature to a receiver over insecure communication channel. The receiver uses a verification key (Public Key) of the sender only to verify the origin of the message and make sure that it has not been tampered with while in transit as shown in Fig. 5.4.

Hash value of a message when encrypted with the private key of a person is, his digital signature on that e-Document. Digital signature is an example of asymmetric key cryptography which uses three different algorithms to complete the process.

1. First step is key generation algorithm which generates private key and a corresponding public key.
2. Next step signing algorithm which selects sending message and a private key generated in step 1, to produce a signature.
3. Third step is signature verifying algorithm which verifies the authenticity of sending message and public key.

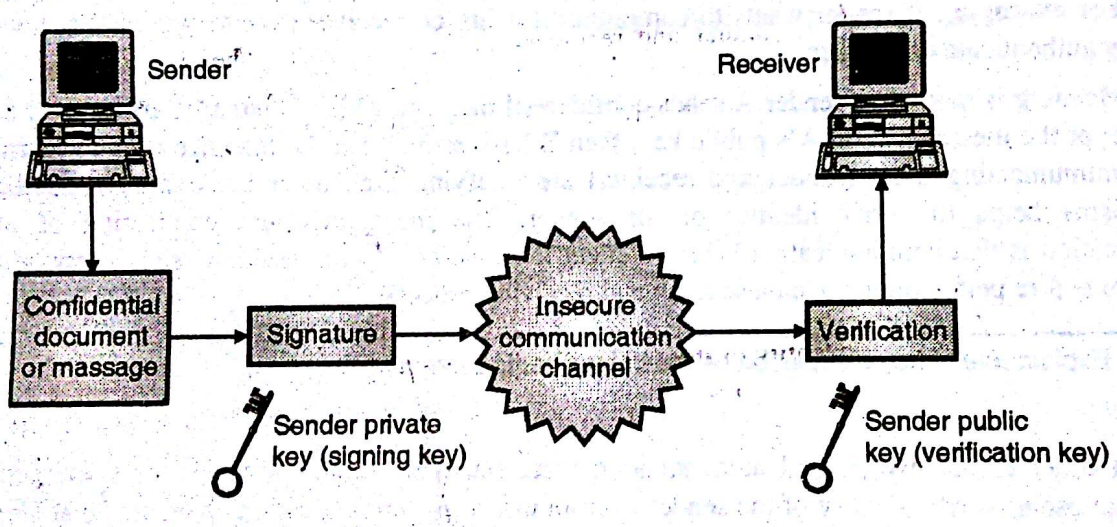


Fig. 5.4 : Digital Signature block diagram

As mentioned above the signature is generated with the help of private key. The private key, which is never shared, is used in signature generation, known to sender only. Public keys, which are known by everyone, can be used to verify the signature of a sender. Every sender and receiver having a private and public key pair, the reason digital signature called public-key cryptography.

Q. 5 Explain different authentication methods and protocols. **Dec. 2012**

Ans. :

Authentication mechanisms help to prove the identity of the sender of the message. Authentication mechanisms ensure that who sends the message i.e. origin of an electronic message is correctly identified.

One-way authentication refers to the authentication of only one end of communication users. For example, One-way authentication follows the flow: If there are two users, user A and B wants to communicate with each other user B authenticates user A, but user A cannot authenticate user B. This process called one-way authentication. Finally the integrity and originality of message is confirmed.

There are different factors of authentication mechanisms used to give strength for authentication. First method is known as **one-factor authentication**. Password is the example of one-factor authentication because it is something that we know. Any operating system first ask for a user name and then for a password. It then looks up the name in a password table and sees if the passwords match. This is known as a **reusable password** since the same password is used for each login.

Second method of authentication is known as **two-factor authentication.** Withdrawing cash from an ATM machine is an example of two-factor authentication. For authentication present the ATM card (something we have) and enter PIN (something we know) or use of **one-time passwords** – a new password must be used for each login.

Q. 6 Explain mutual authentication.

Ans. :

Mutual authentication also called as two-factor authentication. Mutual Authentication *is a* security mechanism used to authenticate sender with the receiver. Sender must prove its identity to a receiver, and the receiver must prove its identity to the sender, before any unwanted threat sent between the sender and receiver.

For example : If sender wants to communicate with the receiver over networks they must first mutually authenticate each other.

Meaning is that when sender A sends confidential message which is intended to receiver B. If B can decrypt the message using A's public key, then B has verified that the message originated from A. Both communicating users (sender and receiver) are verifying each other i.e. mutual authentication mechanisms helps to verify identity of the sender. The most important application of mutual authentication is that communication between client machine and server machine over a network must be secure before performing any data sending and receiving process.

Q. 7 Explain role of key distribution centre in symmetric system.

Ans. :

In order to achieve mutual authentication there must be certain provision of some protocols which suppose to verify identity of the sender over an insecure communication channel. To achieve this goal most of the protocols depends on an authentication server also called **Key Distribution Center (KDC).** If sender A wants to establish a secure communication with receiver B, then A can request for **session key** from Key Distribution Center for communicating with B. If group of people wants to securely communicate with Key Distribution Center then providing every group member a single key called a **master key or secret key**. Authentication servers are capable to delivers good quality session keys and distribute securely to client who requested it.

Authentication server also maintains a table containing a name and a **master key or secret key** of each client. The secret key is used to authenticate client to the authentication server and then for securely transmission of data between client and the authentication server. There are different protocols are used to perform this task but among this the well known protocol called as Needham-Schroeder Protocol.

Q. 8 Explain the Needham/Schroeder Protocol for secret key distribution.

Ans. :

The first mutual authentication protocol was published in 1978 by Needham and Schroeder. This approach was proposed for various purposes that includes secret-key and public key generation and distribution of those keys between sender and receiver.

Needham and Schroeder protocol uses a secret key known to the sender and also to an authentication server. Sender and receiver share a secret key and use it for secure communication with authentication server.

Steps of Needham-Schroeder Secret-key Protocol :

Step 1 : Sender A requests for a **session key** to authentication server for communication with receiver B as shown in Fig. 5.5. The message sent by A to authentication server includes A's secret key Ka, A's network address Na, B's network address Nb and a nonce. A nonce is basically a random number used to demonstrate the freshness of a request denoted by N. The request sent by A to authentication server which is in encrypted format E denoted by,

$$E (Ka, [Na, Nb, N])$$

Step 2 : Authentication server returns a message, containing a newly generated key Kab (used to encrypt communication between sender and receiver), nonce N (to match the response received from authentication server with the request sent), ticket (contains the same shared secret key Kab , as well as the name of the sender A) encrypted with B's secret key Kb and whole these message encrypted with senders private key or secret key Ka to ensure that no one else can read it. The message that authentication server sends back to A can be expressed as :

$$E (Kab, N, \{A, Kab\} Kb, B\} Ka$$

Step 3 : After receiving replay from authentication server, sender decrypt the ticket and sends the ticket **{A, Kab}** to the receiver B. A sends the ticket to B which is not in encrypted format because it was previously encrypted by authentication server using B's secret key Kb.

$$(A, Kab) Kb$$

Step 4 : B decrypts the ticket received from A using the secret key Kb and compares sender identity. B is again encrypting the ticket using shared secret key Kab and generates nonce N1 and sends it back to receiver. This can be represented as

$$E (N1) Kab$$

In this step B got the **session key** (Kab) for communicating securely with A.

Step 5 : Sender is decrypting the nonce N1; using the shared secret key Kab this proved the senders identity. The sender sends response N1+1 encrypted using the shared secret key Kab.

$$E(N1+1) Kab.$$

Step 6 : Now sender A and receiver B can securely communicate with each other using session key generated.

The main weakness of this protocol is that for large networks it is not possible for single authentication server to generate and distribute number of session key which is practically not possible.

Another weakness is that if session key between sender A and receiver B is stolen, and the ticket to B is recorded, attacker can easily copy the contents of a sender A by performing last 3 steps.

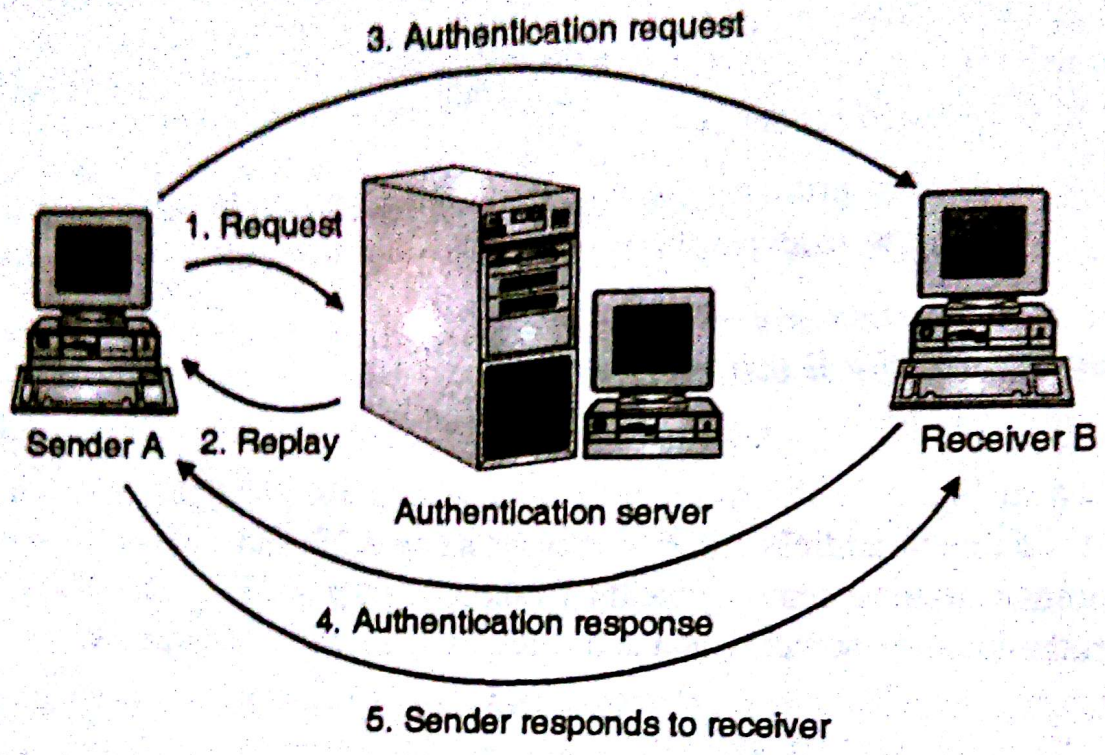


Fig. 5.5 : Needham – Schroeder Secret-key Protocol

Chapter 6 : Authentication Applications

Q. 1 Explain the process of Digital Certificate generation and the process of evaluation of authenticity of Digital certificate. May 2014

Ans. :

Kerberos is also called as authentication protocol. Like when to start in journey we need a confirm ticket then only we can do our journey safely. Kerberos uses the concept of the ticket as a token to prove the identity of the user. Microsoft introduced Kerberos in Windows 2000 server as a default authentication protocol. Kerberos uses the concept of a ticket as a token that proves the identity of a user.

Tickets are digital documents that store session keys. Instead of password, tickets are issued during login session and then can be used in any Kerberos services. For client authentication phase requires two tickets :

Ticket Granting Ticket (TGT), which act an identifier for user and session key. A service ticket to authenticate user to gain access to user for particular service.

The same concept of ticket is used likewise we use railway tickets it has time duration, expiration dates after that ticket become invalid. In Kerberos these ticket includes different contents like time stamps to indicate an, start and expiration time, after time expiration the ticket become invalid. The timestamp is the time set by Kerberos administrator depending upon how much time service is required to the client.

(i) Kerberos Servers

To accomplish the task of secure authentication, Kerberos uses a trusted third party is called a Key Distribution Center (KDC). The Key Distribution Center uses two techniques for authentication :

Authentication Server (AS), which performs user authentication.

Ticket- Granting Server (TGS), which permits/ grants tickets to users.

The role of an Authentication server is to store a database like secret key of the users and its services. The secret key of a user is generated using one-way hash of user provide password. The main aim of the Kerberos is provide centralize authentication of entire network rather than storing the sensitive information at each user machine, the sensitive information will be maintained at particular secure location only.

(ii) Kerberos Authentication

This phase is called as Authentication phase because during this phase only authentication can be done between authentication server, ticket-granting server and service provider.

As shown in Fig. 6.1 first client and authentication server authenticate themselves to each other.

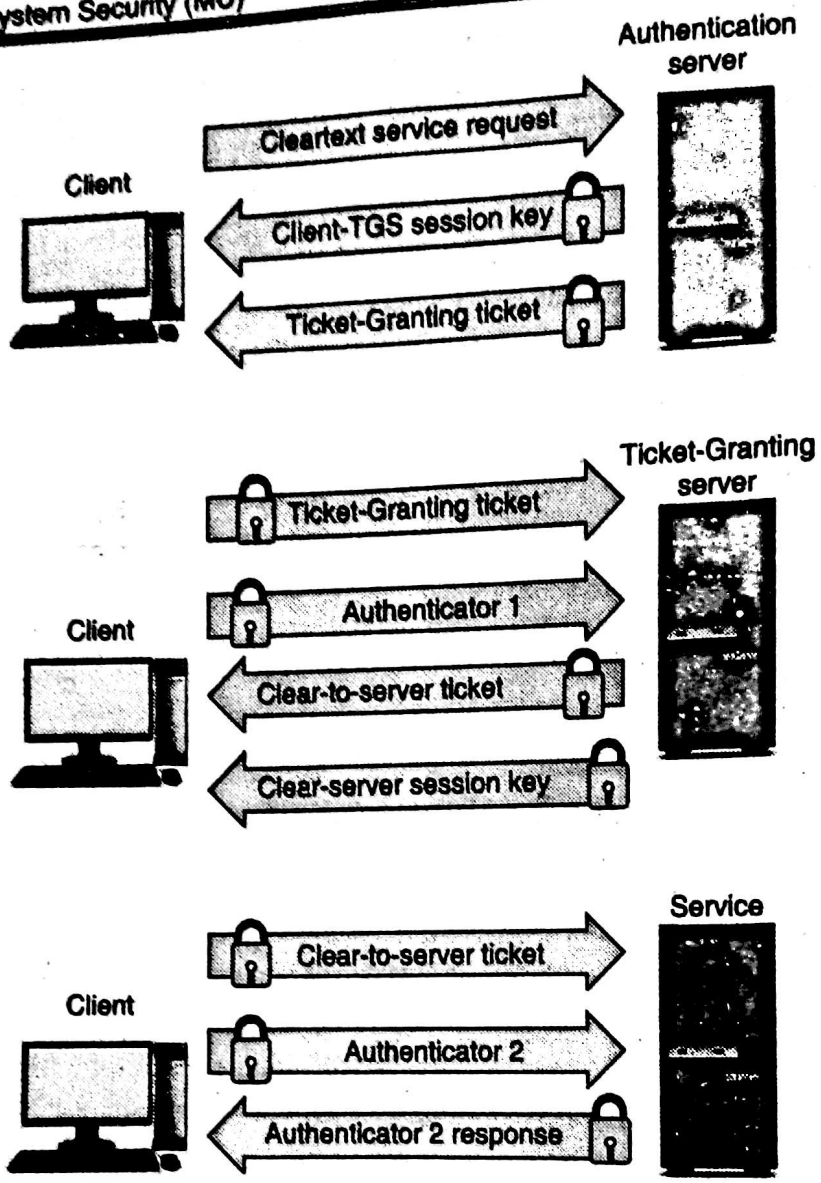


Fig. 6.1 : Kerbaros athentication process

Client and Ticket granting server authenticate themselves. Finally client and requested service provider authenticate themselves to each other regarding which information/ service client wants.

(iii) Authentication Details

During authentication phase user has to provide username and password on the client machine which cryptographically hashed to create a secret key for the client. After client verification done with authentication server, AS will replies the following details to client as shown in Fig. 6.1. The client Ticket Granting Sever (TGS) session key Kt, encrypted using clients secrets key Kc (which now stored in authentication server).

The ticket granting ticket (TGT) encrypted using the secret key of the Ticket granting server. The ticket granting ticket includes the client ticket granting sever session key Kt and its validity period. The client now decrypt the Ticket Granting Server session key Kt using his secret key Kc. To request as service client sends following two message to ticket granting server (TGS). The Ticket Granting Ticket and the name of the service Sr that client wants to request.

Authentication token which includes client ID and time stamp, encrypted using client ticket granting server session key Kt. Upon receiving all the details from client Ticket Granting Server

decrypts the Ticket Granting Ticket using Kt, thus retrieving the client Ticket granting server session key Kt and the validity of the ticket granting ticket. If it is valid then Ticket granting Server sends following messages to the client.

New client server session key Ksc, encrypted using TGS session key Kt. Client to server ticket, encrypted using specific services key Ks, known to Ticket Granting Server only. (Client to server ticket contains the client ID, network address, validity period and the client server session key Ksc). Upon receiving all the details from Ticket Granting server client decrypt the client server session key Ksc, and authenticate him to service Sr by sending following messages. The client server ticket sent by the ticket granting server in previous step. The client ID and the time stamp encrypted suing client server session key Ksc.

The service provider decrypts the client to server ticket using secret key Ks and obtains the client server session key Ksc. With the help of client server session key Ksc, service provider decrypt the client ID and time stamp information. To prove the final identity service providers increment the time stamp by 1 and send it back to the client. The client decrypts and verifies this response using client to server session key Ksc. Once this verification get succeed, now client - server can start. Kerberos protocol was specially design to check the authentication of the client over insecure network.

Q. 2 Does a public key infrastructure use symmetric or asymmetric encryption ? Explain your answer. Dec. 2013

Ans. :

Public Key Infrastructure (PKI) is cryptographic technique used to secure electronic information with the help of certain techniques such as digital certificates and digital signature and transmission of this information securely over internet. PKI consists of certain security policies, software's, and techniques that are required for key generation, key management, secure storage of generated keys, and distribution generated keys. A public key infrastructure is created by combining a number of services and technologies. To complete this technology, there are various components of PKI are required.

Q. 3 List the certifying authorities in India and worldwide. Also list the steps to acquire the digital certificate.

Ans. :

The certification authority (CA) is a trusted unit that helps to issue certificates. A CA takes the certificate request from owner, verifies the requested information according to the terms and conditions of the CA, and uses its private key to apply digital signature to the certificate. Responsibility of the CA is to identify the correct identity of the person who asks for a certificate to be issued, and make sure that the information contained within the certificate is legal and later digitally sign on certificate.

The CA may generate a public key and a private key (a key pair) or the person applying for a certificate may have to generate their own key pair and send a signed request containing their public key to the CA for validation. After the verification from CA it sends certificate for final verification to registration authority (RA).

Q. 4 Explain the process of Digital Certificate generation and the process of evaluation of authenticity of Digital certificate. Dec. 2013, Dec. 2014

Ans. :

Digital certificate is an electronic file that is used to identify people and resources over an insecure channel or a network called Internet. Digital certificate also enable secure, confidential

---

communication between sender and receiver using encryption. For example when we travel to another country, our passport provides a way to establish our identity and gain entry. Digital certificate provide similar identification in the electronic world.

The role of Certification Authority (CA) is to issue certificates with authorized digital signature. Much like the role of the passport office, the role of the CA is to validate the certificate owner's identity and to "sign" the certificate so that it cannot be tampered by unauthorized user. Once a CA has signed a certificate, the owner can present their certificate to people, web sites and network resources to prove their identity for confidential communications over insecure channel.

A standard called as **X.509** defines structure of digital certificate. The International Telecommunication Union (ITU) permitted this standard in 1998. Fig. 6.2 shows structure of X.509 digital certificate. A standard digital certificate typically includes a variety of information pertaining to its owner and to the Certification Authority (a trusted agency that can issue digital certificate) such as :

Certificate version number : Identifies a particular version of the X.509. Current version is X.509 v3.

Certificate serial number : Unique integer number generated by certification authority.

Algorithm for signature identifier : Identifies algorithm used by the certification authority to sign the certificate.

Certificate issuer name : The name of the Certification Authority that issued the certificate.

Validity Details : The validity period (or lifetime) of the certificate (a start and an end date).

Digital Certificate contents
Certificate version number
Certificate serial number
Algorithm for signature identifier
Certificate Issuer name
Validity Details
Name of the certificate owner Public key of certificate owner
Issuer unique identifier
Owner unique identifier
Extensions to certificate
Certification Authority (CA) Digital Signature

Fig. 6.2 : Structure of X.509 Digital certificate

Name of the certificate owner : The name of the owner and other identification information required for identifying the owner such as email id and contact details.

Public key of certificate owner : Certificate owner's public key, which is used to encrypt confidential information of the certificate owner.

Issuer unique identifier : Indentify the CA uniquely i.e. whether single CA signed it or is any CA using same details.

Owner unique identifier : Indentify the owner uniquely if two or more owner has used the same name over a time.

Extensions to certificate : This is an optional field which allows a CA to add additional private information to a certificate. These additional fields are called as extensions of version 2 or 3, respectively.

Certification Authority (CA) Digital Signature : In creating the certificate, this information is digitally signed by the issuing CA. The CA's signature on the certificate is like a tamper-detection seal on packaging any tampering with the contents is easily detected.

Q. 5 Does a public key infrastructure use symmetric or asymmetric encryption ? Explain your answer.

Dec. 2013

Ans. :

Basically PKI is the combinations of all techniques, policies and methods of securely implementing public key encryption.

The name public key encryption indicates it is asymmetric key cryptography; hence PKI also uses asymmetric key cryptography as a basis for encryption

---

Q. 6 Write a detail note on : Email Security. Dec. 2013

Ans. :

We all are aware that most popular use of Internet is to send the email and chatting with the friend's, partner etc. But have you ever think that if we are sending mail to intended person is going in his inbox only? Security concerns have estimated that only about one in every 100 messages is secured against interception and modification attacks. Are we aware that sending an email to business partner or friends in clear text message is going through thousands of machines (between sender and receiver before it reaches to intended recipients?) these machines might read and saved the contents of email for future use?

Many people think that name given in sender of the mail identifies who actually sends it. When you send a message through email, we cannot guarantee that it will be deliver to correct destination or received exactly what you sent. And even there is a no way of knowing that the message is received read and forwarded by attacker.

Because of wide spared problem of email modifications, sending it to wrong destination by intermediate parties, email spoofing, we need a competing solution to overcome and address the issues of authentication, integrity and reliability of the messages between sender and receiver. The public key cryptography play an important role because of two keys used, only intended sender can decrypt the message using his public key as message encrypted using private key of the sender. The solution is called as Pretty Good Privacy (PGP) program/ software which provide the secrecy and non-repudiation of data sent over Internet especially by email.

Pretty Good Privacy (PGP) is a popular open-source freely available software package/ techniques used to encrypt and decrypt email messages over the Internet. PGP is an e-mail security

program written by Phil Zimmermann in 1991, PGP program become a de facto standard for e-mail security used to store the encrypted files so that it can be non-readable by other users or intruders.

This program also be used to send an encrypted digital signature, let the receiver verify the sender's identity and know that the message was not changed or modified while transmission. Once the file is encrypted using PGP program only the intended recipient can decrypt it. Once message content digitally singed by sender, the sender guarantee to the recipients that message or file comes from valid sender and not by attacker. Digital signature functionality of PGP guarantees that the message or file come from the sender and not from an intruder.

❑❑❑

Chapter 7 : Program Security

Q. 1 Explain non-malicious program errors with examples? Dec. 2013

Ans. :

While programming, a programmer can make mistakes/errors. Most of these errors are not intentionally done. Many such kind of errors do not have huge impact on security. Program may produce wrong or incorrect results but it is non-malicious. Following are the three types of non-malicious program errors,

Q. 2 What is buffer overflow in software security ? May 2013, Dec. 2014, May 2015

Ans. :

Attacker can insert malicious data values / instruction codes into overflow space. Array bound checking is not performed by C compiler, pointer limits cannot be defined as well.

Example: int B[15];

Here the array bound is (0 to 14). i.e. B[0].....B[14]. If anything inserted after that bound then the adjacent data is overwritten.

Attacker can overwrite users data, changes users instruction, overwrite OS data, changes OS instructions. Thus can get complete control of a program or OS. This is also known as aliasing. As shown in Fig. 7.1 attacker changes the return address and thus can transfer the control of the program.

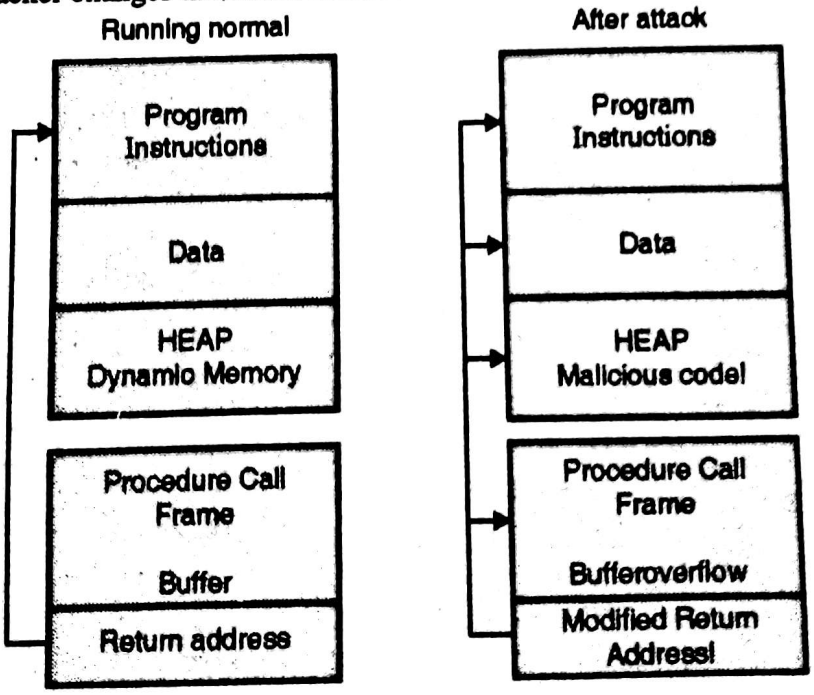


Fig. 7.1 :Buffer overflow attack

Q. 3 What is incomplete mediation in software security ? May 2013, Dec. 2014, May 2015

Ans. :

Due to incomplete mediation serious security threats can be introduced as sensitive data may get exposed and can result in uncontrolled condition.

Example:URL : http://www.onlinestore.com/purchase/total=935.

User can edit the total cost and resubmit the request to the server. URL : http://www.onlinestore.com/purchase/total=035. Such kind of vulnerabilities are very dangerous. Proper care should be taken to avoid such vulnerabilities. Such editing permissions should not available to the user.

Time-of-check to time-of-use errors (TOCTOU) :

This is one of the best examples of RACE condition. RACE condition is very vulnerable to attack.

Example : If two threads are sharing their root and current directories then, Let Thread X's current working directory is /college.

```
Thread X calls open("shadow");
Y calls chdir("/department")
system monitor permits both the calls
open("shadow") executes with /department as working directory
X's call now opens "/department/shadow"
```

Proper locking mechanism can prevent this kind of attack. Time lags should be considered. After checking values it must be locked using digital signatures and certificates. Thus after check data cannot be modified.

Q. 4 What are different types of malicious code ? **Dec. 2013, May 2015**

Ans. :

Malicious software is software where an attacker can get partial or full control of the program. Thus attacker is free to do anything that he / she want to do. Fig. 7.2 shows different types of malicious software's.

Types of malicious software :

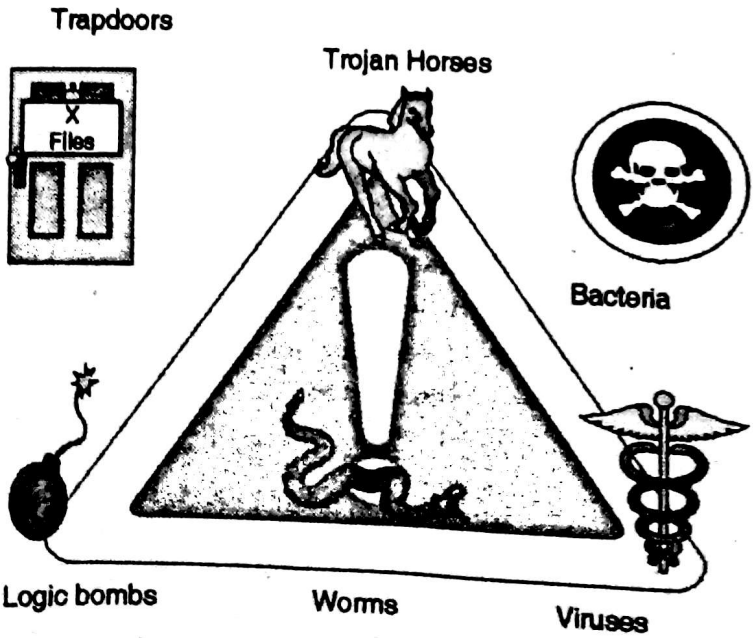


Fig.7.2 : Different types of malicious software's

Trojan horse :

It is a computer program. Along with some useful code or function, some hidden malicious code or function is there which may hamper performance of security mechanisms. Useful information can be stolen by attackers.

Bacterium :

Bacterium is a special kind of virus. Virus is getting attached with different files but bacterium does not get attached to a specific file.

Logic bomb :

Logic bomb is generally used in DOS (Denial of service) attacks. When specified conditions are met it activates malicious program logic. It may damage system resources greatly.

Time bomb :

This gets activated when specified time occurs.

Rabbit :

It is a kind of virus / worms that replicates itself without any limits. The intension is to exhaust resources.

Trapdoor / backdoor:

An intruder can enter into the system by bypassing all security services or mechanisms. Thus intruder knows the flaws or loopholes in the system and can get these loopholes to gain access to the computer.

Virus:

It is a self replicated, hidden computer program. Virus cannot run on its own rather it requires host program to run it and make it active. Malicious logic is written in the program which infects another program. i.e. it becomes the part of another program.

Virus Countermeasures:

(a) Use commercial software from trustworthy sources.
(b) Open only safe attachments.
(c) Keep recoverable system image in safe place.
(d) Use virus scanners often (daily).
(e) Update virus detectors daily as Databases of virus signatures change very often.
(f) Test new software on isolated computers.
(g) Backup executable system files.

Worm :

Worm is also a computer program which can run independently. By propagating a complete working version of itself onto other hosts on a network it can consume computer resources destructively.

Q. 5 What is Malware ? Explain different targeted malicious code ? Dec. 2012, May 2013

Ans. :

This is a computer code which is written to attack a particular system, a particular application and for a particular purpose.

Example :

Trapdoor / backdoor :

An intruder can enter into the system by bypassing all security services or mechanisms. Thus intruder knows the flaws or loopholes in the system and can get these loopholes to gain access to the computer.

Trapdoors are the entry points which are notdocumented but still inserted during code development for testing purpose, for future extensions or for an emergency access if software fails. These loopsholes are purposely kept in the system with good intension.

Major sources of Trapdoors / Backdoors :

During testing of the system stubs, drivers are created. These are temporary functions which then further replaced by actual functions. Sometimes some malicious code is intentionally injected into the system for testing purpose.

(i) Poor error checking conditions.

(ii) Undefined opcodes in hardware processors

Q. 6 Explain Salami and linearization attacks? May 2013

Ans. :

It is series of small attacks which results in large attack. It works on "collect and roundoff" trick. It is a fraudulent practice of stealing money repeatedly. It takes an advantage of rounding operation infinancial transactions. It always rounds down and thus the fractions of amount remained will be transfered into some another account. Thus the transaction will go undetected. Such type of attacks can be easily automated.

Q. 7 Write a short note on covert channel. Dec. 2013, May 2013, May 2015

Ans. :

In covert channel the processes which are not allowed to communicate and transfer the information by security policy can communicate and transfer data using current system objects. Such types of attacks are virtually no detectable by system or administrators. Fig. 7.3 shows channel creation.

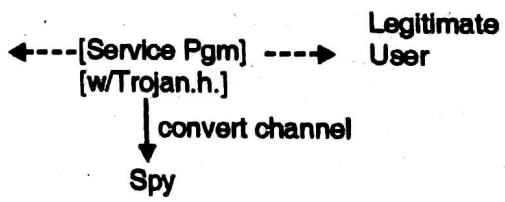


Fig. 7. 3 :Covert channel creation

Q. 8 Write a short note on trojan. May 2015

Ans. :

It is a computer program. Alongwith some useful code or function some hidden malicious code or function is there which may hamper performance of security mechanisms. Useful information can be stolen by attackers.

Rootkits :

A rootkit is a computer malware program installed by an intruder. Intruder installs it by avoiding detection. The purpose is to gain control of the computer system. Basically it is a kind of Trojan horse malwares. System scan cannot detect it. If system is infected with a rootkit, then it becomes very hard to trust infected operating system. The best solution is to shut down the infected system and boot that system by some CD-ROM, Pendrive and clean it.

Following are the types of rootkits :

1. **User Mode :**

User mode rootkits can get administrator privileges. They are automatically activated at system startup. These are detectable rootkits and can be easily removed.

2. **Kernel Mode :**

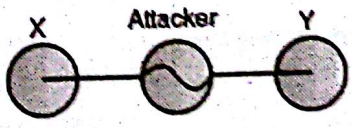
Kernel mode rootkits are installed like an OS hence can corrupt the functionality of complete OS. These Rootkits are very hard to detect. It can be detected only after some event or crash.

3. **Firmware :**

Firmware's are dangerous amongst all. Malcode is created inside a firware. At system startup this malware will be reinstalled. It is very hard to remove.

Man in the middle attack (MITM/MIMA):

Attacker relays and sometimes alters the communication between two parties without knowing to communicating parties.



It is explained as follows :

1. X sends a message to Y, which is intercepted by Attacker:

   X "I want to deposit money in your account. Please send account number"
2. Attacker relays this message to Y; Y cannot tell it is not really from X:
3. Y receives a message from X and responds it with account number.

   Y "My account number is 012345"
4. Attacker again intercepts a message from Y replaces Y's account number with his own account number and relays this to X, claiming that it is Y's message.

Attacker "My account number is 067891"

1. X receives message from Y and gets the account number of Y. Thus X believes that it is Y's account number and deposits money in that account.
2. X and Y both think that it is a secure communication.

□□□

Chapter 8 : Operating System Security

Q. 1 Write a short note on: various ways of memory and address translation. Dec. 2012, Dec. 2014

Ans. :

Due to memory protection the process can access the memory which is allocated to it only. It cannot access the memory which is not allocated to it. Thus it prevents spreading of bugs or malwares in other areas of operating system. Following are the techniques for memory and address protection,

1. Fixed and variable Fence
2. Base/Bound
3. Segmentation
4. Paging
5. Paged Segmentation

1. Fixed and variable Fence :

Fixed Fence :

This technique is used in single user operating system. It prevents the faulty user program spreading in different parts. Thus saves operating system. The fence is created using a fixed and predefined memory address.

Fence separates user area and operating system area. As the memory allocated is fixed, if the allocated memory is not utilized fully then there will be wastage of memory and if needed more memory than allocated it cannot be increased. Fig. 8.1 shows fixed fence.

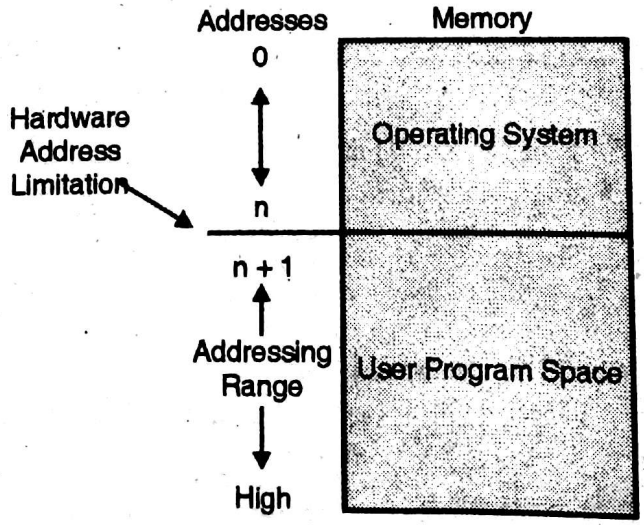


Fig. 8.1 : Fixed fence

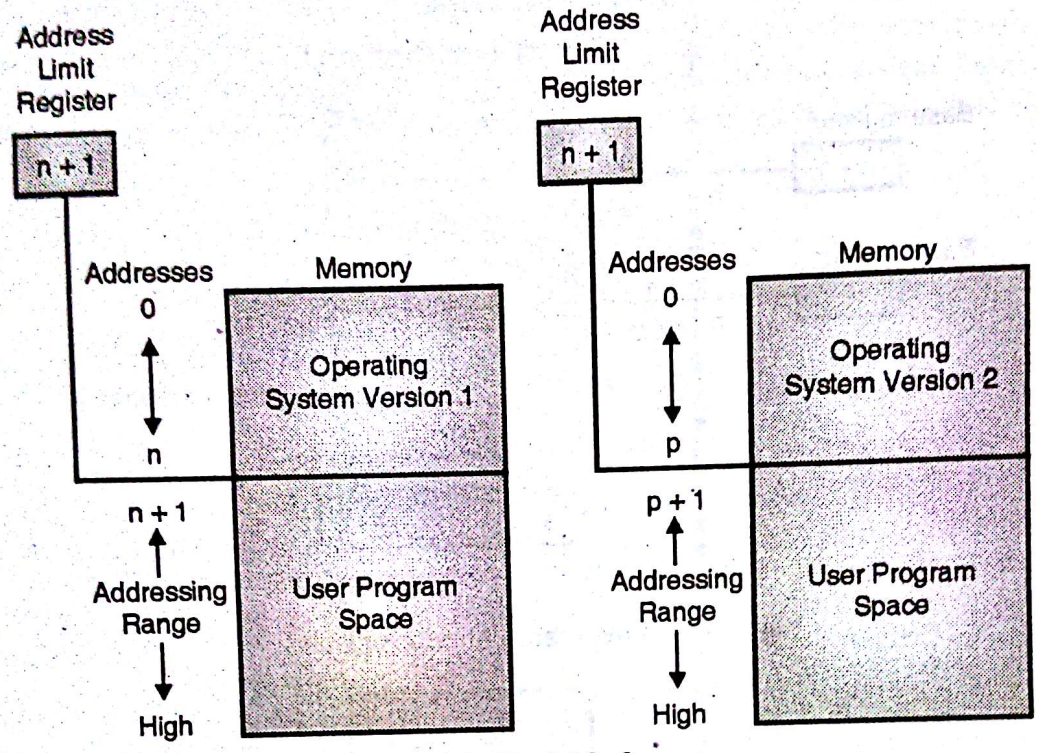


Fig. 8.2 :Variable fence

Variable Fence :

As the name itself indicates the location of the fence can be changed. A fence register is used which contains the end address of the operating system. The address generated by a user program is compared with the fence address. Fig. 8.2 shows variable fence. If the address is greater than fence address then program is executed. If it is less, error will be raised. This approach cannot protect one user from another. It is useful for single user, single operating system only. Relocation technique is used where only starting address of the program is given and based on that starting address all other addresses are automatically updated. Fence register provides the last address. Thus it ensures the security.

2. Base / Bound :

Variable Fence register is also known as base register. All the addresses are derived then with respect to this **base register**. But this base register can have only lower bound i.e. only starting address. It cannot give information about the upper bound. Thus can produce overflow problems. Figs. 8.3 & 8.4 shows pair of base/bound registers.

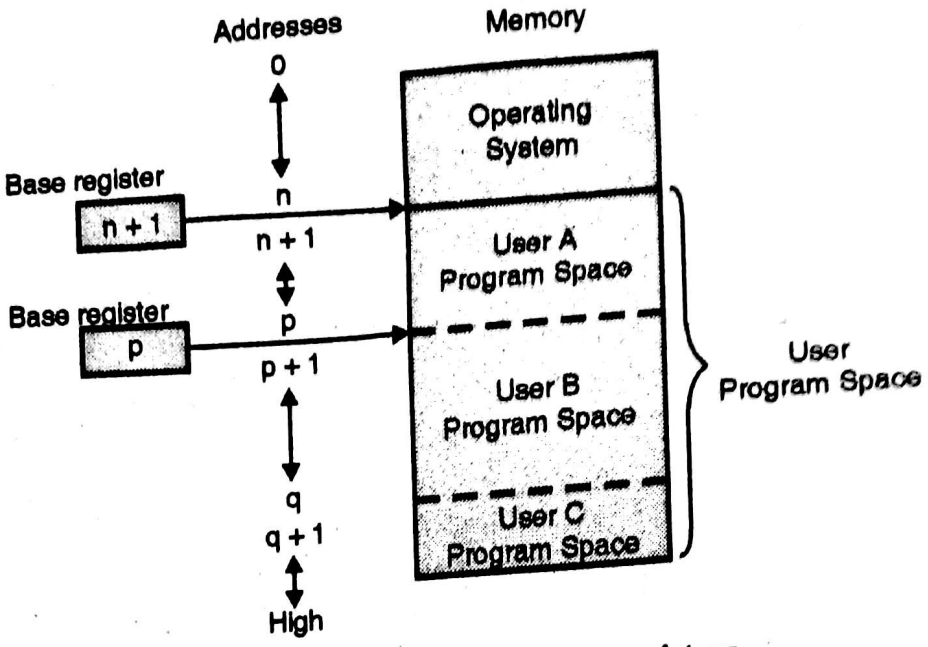


Fig. 8.3 :A pair of base/bound registers

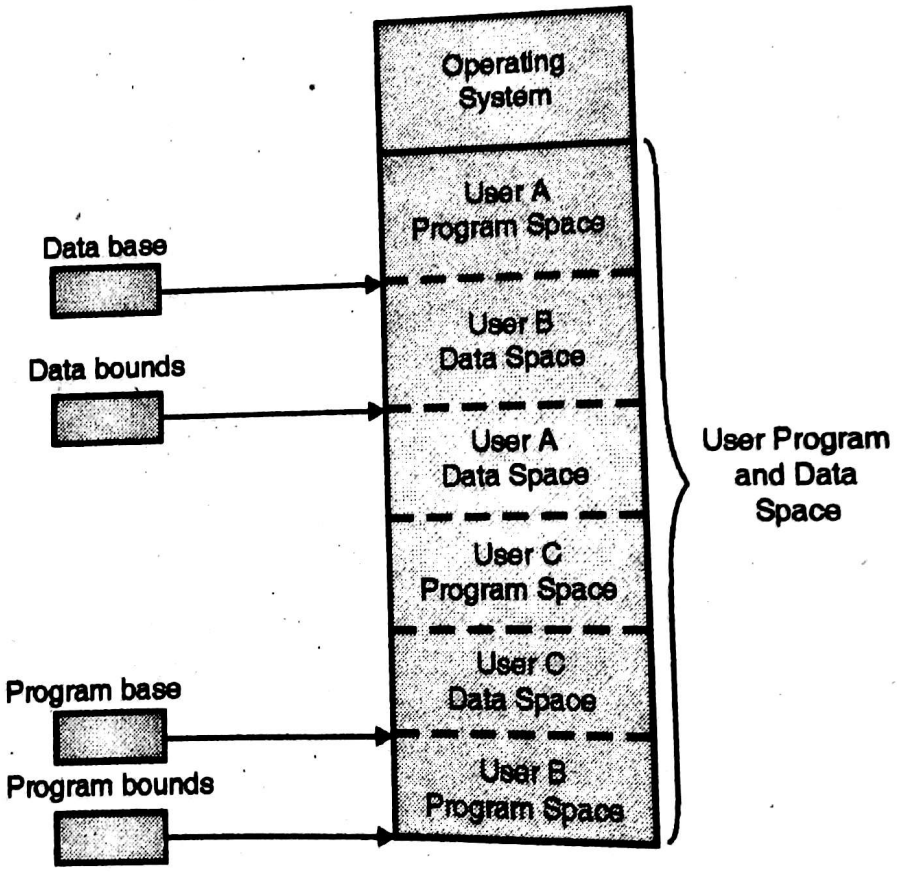


Fig. 8.4 :Two pairs of base/bound registers

To avoid this, an extra register is used called as **bound register**. It stores the upper limit. Thus the program is kept in between upper and lower bounds. Thus it prevents the address modifications by other programs. When execution changes from one users program to another users program i.e. context switching then corresponding fence/base and bound registers are updated so that control can be transferred from one user program address to another user program address.

As shown in above diagram a pair of base / bound registers can be used. One pair can be used to store instructions while other can be used to store data. Thus interface of different users programs can be avoided to certain extent. Tagged Architecture is an alternative way to identify access rights. In this every machine memory word has one or more extra bits. Privileged operating system instructions can only set these bits. For every access these bits are tested. Fig. 8.5 shows targeted architecture.

Tag	Memory Word
R	0001
RW	0137
R	0099
X	
X	
X	
X	
X	
X	
R	4091
RW	0002

Code: R = Read-only RW = Read/Write
X = Execute-only

Fig. 8.5 :Tagged Architecture

3. Segmentation:

Program is divided into separate pieces called as segments. These pieces are having relationship with all code and data in the program. These pieces can have different access rights. Each segment has a unique identity in the system.

<name, offset> pair is used to identify a code or data item within a segment. Name is the segment name and offset is the address within segment. Fig. 8.6 shows logical & physical representation of segments.

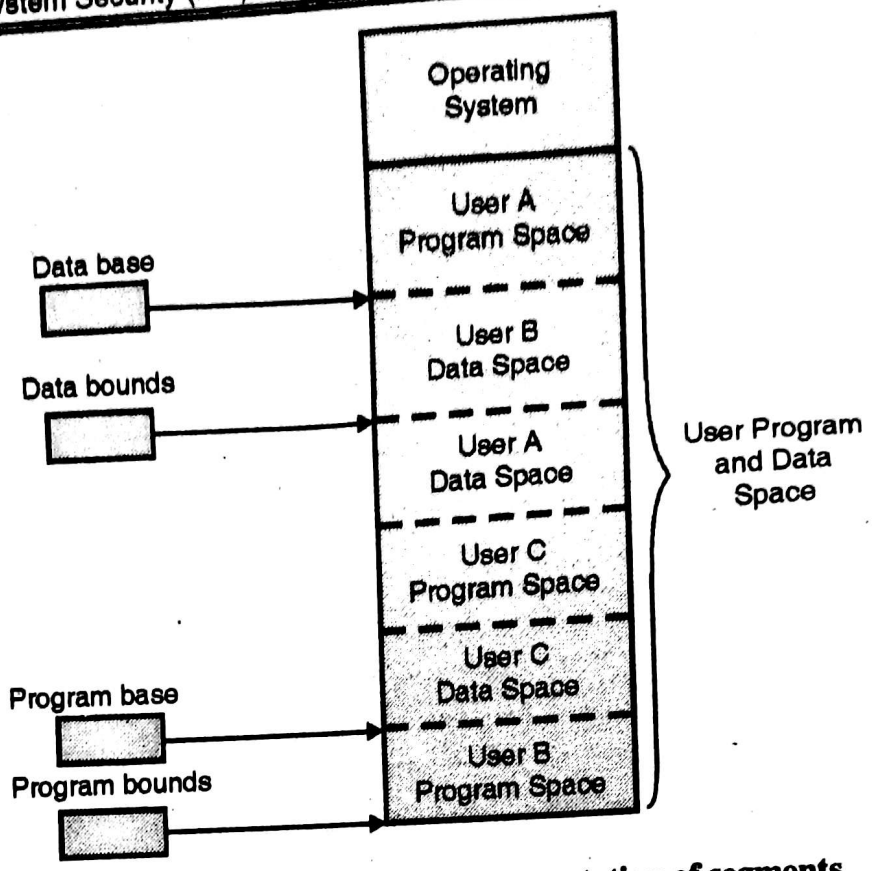


Fig. 8..6 :Logical and physical representation of segments

Segments can be easily relocated anywhere. The operating system stores segment names and their true address into segment address table. These addresses are then translated for program execution. Two processes can share a same segment address table if they belong to the same segment as shown in Fig. 8.7.

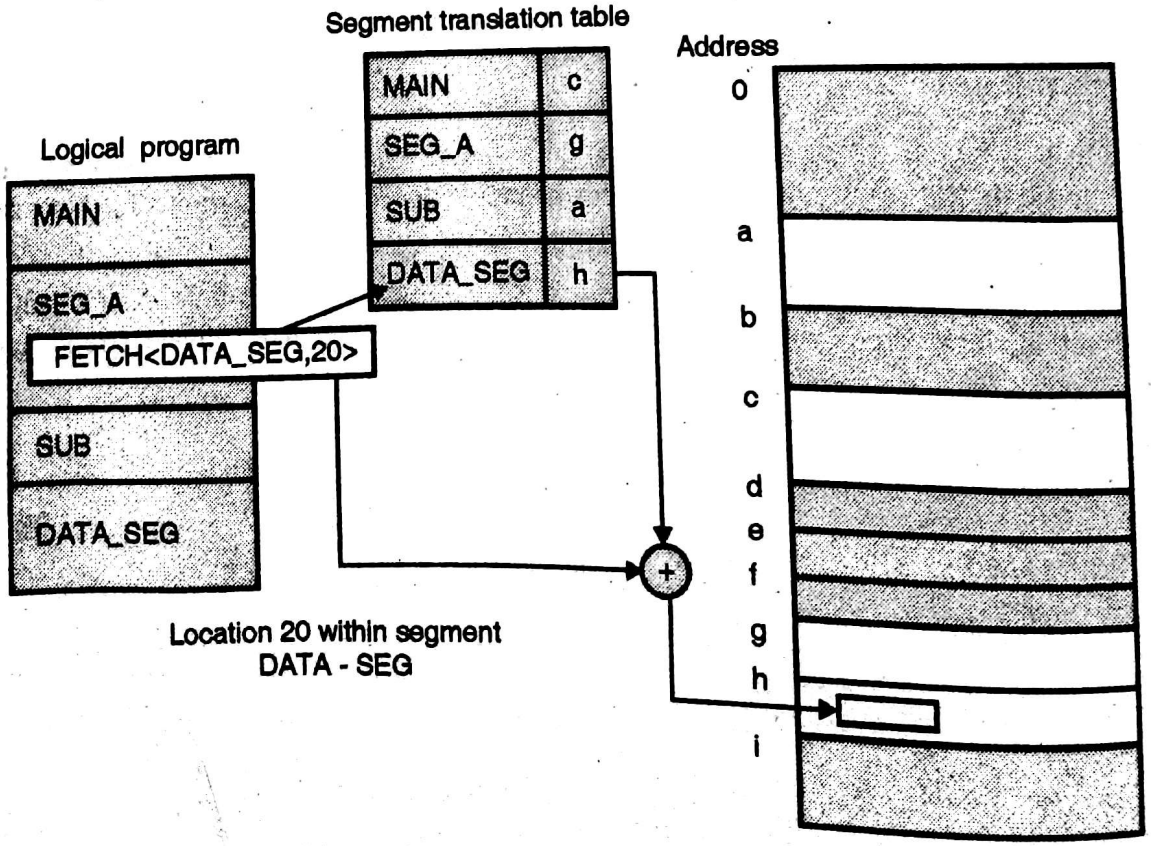


Fig. 8.7 :Segment address translation

4. Paging :

Paging is an alternative to segmentation in which program is divided into equal sized pieces called as pages.

Addressing system and address translation is same as that of segmentation. Operating system maintains the page translation table.

All pages are of same size hence there is no fragmentation problem. Fig. 8.8 shows Page address translation

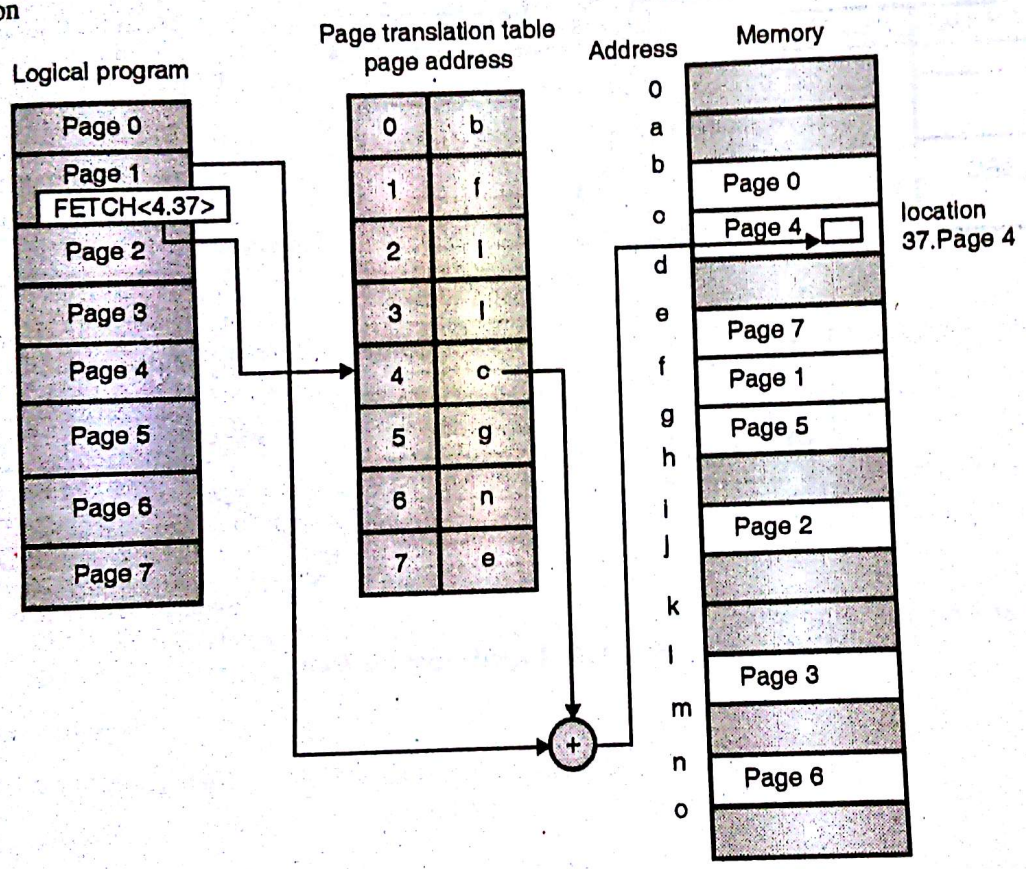


Fig. 8.8 :Page address translation

5. Paged Segmentation :

With paging implementation becomes easy and with segmentation logical security can be improved. Both the techniques are having their own advantages and disadvantages. In paged segmentation both paging and segmentation techniques are combined together.

A programmer can divide the program into segments and then each segment can be further divided into fixed size pages.

Thus paging can be implemented on top of segmentation. As shown in Fig. 8.9 additional hardware is required for additional address translation. Fig. 8.9 shows Paged segmentation

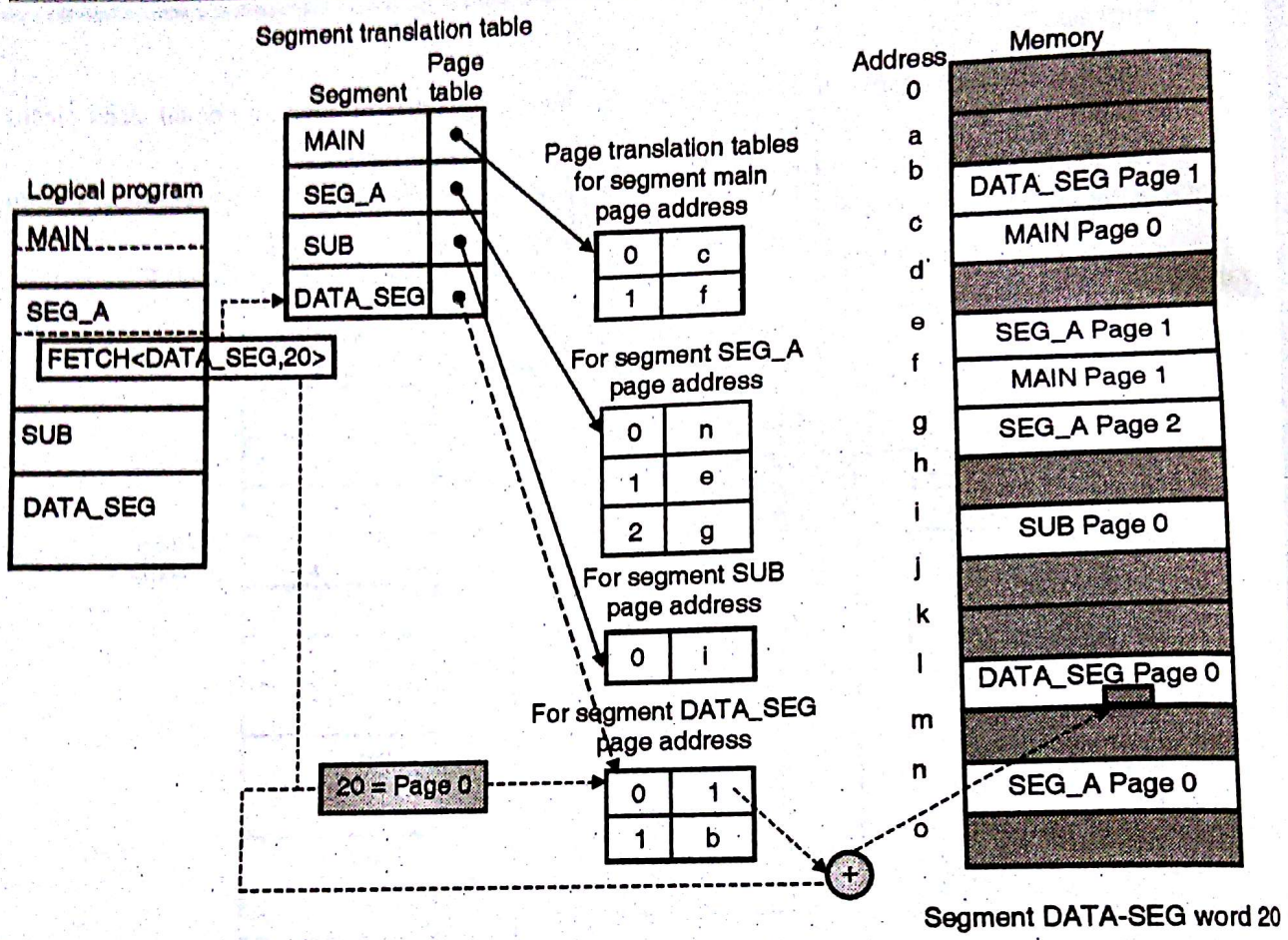


Fig. 8.9 : Paged segmentation

❑❑❑

Chapter 9 : Database Security

Q. 1 What are security requirements of database ?

Ans. :

User authentication :

Only authenticated users should get permission to access permitted data.

Availability :

All the time the permitted data should be available to authorized users.

Access control :

Different users should have different accounts as well as different access rights so that their data can be protected from each other.

Physical database integrity :

In database systems the data is not affected or influenced by physical problems like power failures. Database can be reconstructed after such failures.

Logical database integrity :

The logical structure of the database is fixed. Values manipulation in any field of the database should not affect other fields.

Element integrity :

Accuracy is important. Data should be accurate by all means.

Auditability :

For auditing purpose it is very important to keep track of all the users and their activities.

Q. 2 Explain Multiple level security model. May 2013, Dec. 2013

Ans. :

Different elements may have different security. The security of some element may be different from the other elements of the same row or column. Thus security is implemented for each individual element. For implementing security two levels (i.e. sensitive and non sensitive data) are not good enough. These levels must be increased as per the need of the application security.

Q. 3 Explain multilateral security. May 2013, Dec. 2013

Ans. :

Multilateral security considers different and possibly conflicting security requirements of different parties and strives to balance these requirements.

Q. 4 What is Bell-La Padula ? How Bell-La Padula model works? May 2014

Ans. :

Appropriate access rights and permissions must be granted to individuals before they can see classified information. Confidential information can be seen by those who have permission to see it. They are not trusted to see Secret or Top Secret information. Data flow operates from lower levels to higher levels. It will never be the reverse as shown in Fig. 9.1.

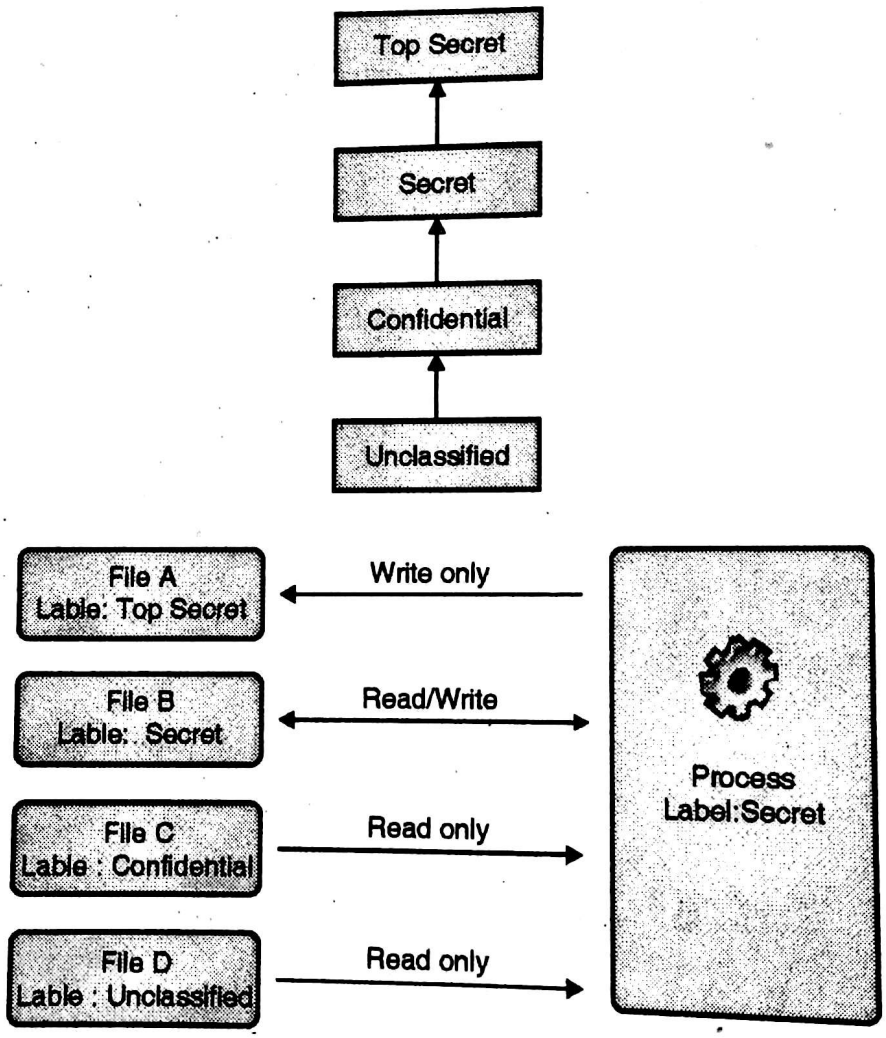


Fig. 9.1

Chapter 10 : IDS and Firewalls

Q. 1 Define intruder.

Ans. :

An *Intruder* is a person who intercepts system availability, confidentiality and data integrity. Intruder's gains unauthorized access to a system with criminal intensions. Intruder may damage that system or disturbs data.

Q. 2 What are the strengths and limitations of Intrusion Detection System ? Describe the different types of IDS. May 2012, May 2013

Ans. :

With the rapid expansion of Internet during recent years, security has becomes an essential issue for computer networks and computer systems.

The main aim of a security system is to protect the most valuable assets (data/secret information) of an organizations like banks, companies, universities and many others, because these organizations have data or secret information in some form, and their security policies are keen for protecting the privacy, integrity, and availability of these valuable information or data.

As these organizations will have different security policies and requirements depending on their vision and missions. Many efforts have been carried out to accomplish this task are security policies, firewalls, anti-virus software even *Intrusion Detection Systems* (IDSs) to configure different services in operating systems and computer networks.

But still detecting different attacks (like denial service attacks, IP spoofing, ping of death, network scanning etc) against computer networks is becoming a crucial problem to solve in the field of cryptography and network security. To overcome all above problems researcher in the field of computer security came with existing but different solution called Intrusion Detection System (IDS). Before discussing on IDS let us understand some key points like what is intrusion? What is intrusion detection and then what is intrusion detection system?

When an attacker or intruder attempts to break into an information system or performs an illegal action such as denial of service attacks, scanning a networks, ping scan, sending many request for connection setup using fake IP address, etc which is legally not allowed, that is called as an *intrusion*. *Intrusion detection* is an important technology that monitors network traffic, events and identifies network intrusions such as abnormal network behaviours, unauthorized network access and malicious attacks to computer systems.

The general example of intrusion detection is when we suffer from some disease and asking doctor what happen to me. Doctor suggests for blood checking and sends blood sample to laboratory for detection. The blood report given by pathologies is just detection of disease (number of platelets count, haemoglobin, etc.) then after checking the entire history of blood report doctor suggests medicine to cure the disease.

Here blood report is intrusion detection where as medicine given by the doctor after checking blood report is called intrusion detection system. Finally how fast patient get relief depends upon the

doctor's education, experience and knowledge, joke apart let us move towards technical definition of IDS.

Intrusion Detection system has some policies or mechanisms to protect computer systems from many attacks. As the use of data transmission and receiving over the internet increases the need to protect the data of these connected systems also increases. Many scientists have different definition of IDS but as per our point of view IDS can be defined as below point.

"An Intrusion Detection System is software that monitors the events occur in a computer systems or networks, analyzing what happens during an execution and tries to find out indications that the computer has been misused in order to achieve confidentiality, integrity and availability of a resource or data."

The IDS will continuously run on our system in the background, and only generate the alert when it detects something suspicious as per its own rules and regulation or attack signature present into it and taking some immediate action to prevent damage.

An Intrusion detection : System examines or monitors system or network activity to find possible attacks on the system or network. Signs of violation of system security policies, standard security practices are analyzed . Intrusion Prevention is the process of detecting intruders and preventing them from intrusive effort to system.

Intruders can be broadly classified into three different types :

1. **Masquerader** :These are unauthorized user typically outsider,try to penetrate the system's protection.
2. **Misfeasor** : These may be authorized or unauthorized person typically the insiders of the organization, who tries to misuse the data.
3. **Clandestine user** : They can be both inside and outside. These types of intruders gain administrative access to the system.

Intrusion detection can be classified into different ways. But mostly it is classified as Active and Passive IDS and Host and Network IDS.

Active and Passive IDS :

An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Intrusion Prevention System (IDPS).

Intrusion Detection and Prevention System (IDPS) is configured to automatically block all suspected attacks without any interference required by any monitor.Intrusion Detection and Prevention System (IDPS) response real time corrective and response to the threats and attacks.

A passive IDS is a system that alerts the operator about the vulnerabilities and analyze network traffic activity. As Passive IDS only analyzes the network, it cannot perform any correction or protection in the network on its own.

Types of IDS technologies :

The types of IDS technologies are differentiated mainly by the types of event they monitor or scrutinize .There are four types of IDS Technologies.

1. **Network based** :The IDS monitors network traffic. It analyze the network activities and protocol activities to identify suspicious activity of the network.
2. **Wireless** :The IDS monitors the wireless network traffic. It analyze the network activities and protocol activities of wireless network.

3. **Network BehaviourAnalyse :**These network behaviour analyze identify the treats that create unusual traffic overflow, DDOS(Distributed Denial of Service) attacks, malwares, and policy violations.

4. **Host Based :**These IDS monitors the host and the event occurs within that host.

Q. 3 Explain Intrusion Detection Techniques.

Ans. :

The categorization of Detection methodologies are : Signature Based, anomaly based, stateful protocol analysis. Most of the IDPS uses these techniques to reduce or make network error free.

(1) Signature Based Detection

It is a process of comparing the signatures of known threat with the events that are been observed. Here the current packet is been matched with log entry of the signatures in the network. Signature is defined as the pattern (structure) that we search inside a data packet. The data packet may contain source address, destination address, protocol, port number etc.

If an attacker adds any malicious code into these data packet he is generating attack pattern or signature. Signature based IDS create databases of such attack pattern for detecting the known or documented attacks. Single signature is used to detect one or more types of attacks which are present in different parts of a data packet. Signature - based IDS used to monitored events occurred in the network and match those events against a database of attack signatures to detect intrusions. It also uses a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks.

For example, we may get signatures in the IP header, transport layer header (TCP or UDP header) and application layer header or payload. Signature based intrusion detection system sometimes also called misuse detection techniques. It checks for the attack pattern with the existing stored database pattern and if match is found then generates the alert.

Signature based IDSs are unable to detect unknown and newly generated attacks because it requires manual updating of each new type of attacks into to the existing database. The most well known example of signature - based IDS is SNORT IDS freely available for attack detection and study purpose.

(2) Anomaly Based Detection

It is the process of comparing activities which are supposed to be normal against observed events to identify deviation. An IDPS uses Anomaly based detection techniques, which has profiles that represent normal activities of user, host, connections or applications.

For example :

Web activities is a normal activity done in a network. Anomaly based IDS works on the notation that "attack behavior" enough differ from "normal behavior" (IDS developer may define normal behavior). Normal or acceptable behaviours of the system (e.g. CPU usage, job execution time etc) if the system behavior looks abnormal i.e. increasing CPU speed, too many job execution at a time then it is assumed that the systems is out of normal activity. Anomaly based detection is based on the abnormal behavior of a host or network.

Database for such type of IDS is the events generated by user, host and network, and the "normal" behavior of the systems. These events (historical data) are collected from the research laboratories which continuously work on normal and abnormal behavior systems over a period of time. Anomaly based IDS checks ongoing traffic, host activities, transactions and behavior in order to identify intrusions by detecting anomalies. Host - based IDS generally uses anomaly based techniques.

This can be done in two ways :

1. **Threshold detection :** Threshold are defined for all users for all group and frequency of all events are measured comparing with threshold.
2. **Profile Based detection :** Profiles of individuals are created and they are matched against the collected statistics for checking the irregular patterns.

May 2013, Dec. 2014

Q. 4 Write a short note on firewall.

Ans. :

A firewall device filters all traffic between intranet and extranet. All the traffic runs through firewall. The main purpose of the firewall is to keep attackers outside the protected environment. For that policies are set in the firewall to decide what is allowed and what is not allowed. Moreover we can decide the allowed places, allowed users, allowed sites, can provide different access rights to different category of the users.

Ex. : Cyberoam through which only educational sites are allowed through college internet and non-educational sites like facebook, twitter can be blocked.

May 2012

Q. 5 What are firewall design principles ?

Ans. :

A firewall is a kind of reference monitor. All network traffic passes through firewall. That's why it is always in invoked condition. A firewall is kept isolated and can not be modified by anybody other than administrator. Generally it is implemented on a separate computer through which intranet and extranets are connected.

Q. 6 List, explain and compare different kinds of firewalls used for network security.

Dec. 2013, Dec. 2014, May 2015

Ans. :

Following are the types of Firewalls,

(i) Packet filtering gateways or screening routers
(ii) Stateful inspection firewalls
(iii) Application proxies
(iv) Guards
(v) Personal firewalls

(i) Packet Filtering Gateway :

It is the most simple and easy to implement firewall. Packet filtering is done on the basis of packets source or destination address or based on some protocol type like HTTP or HTTPs. If the firewall is placed just behind the router then the traffic can be analyzed easily. In the Fig. 10.1 it is shown that how packet filtering gateway can block traffic from network 1 and allow traffic from network 2. Also the traffic using telnet protocol is blocked. Packet filters do not analyze the contents of the packet rather they just check IP address of the packets as shown in Fig. 10. 1.

The biggest disadvantage of the packet filtering gateway is that it requires lot of detailing to set policies.

Example : If port 80 is blocked. If some applications essentially need use of port 80 then in this case we have to provide all the details of those applications for which port 80 is needed.

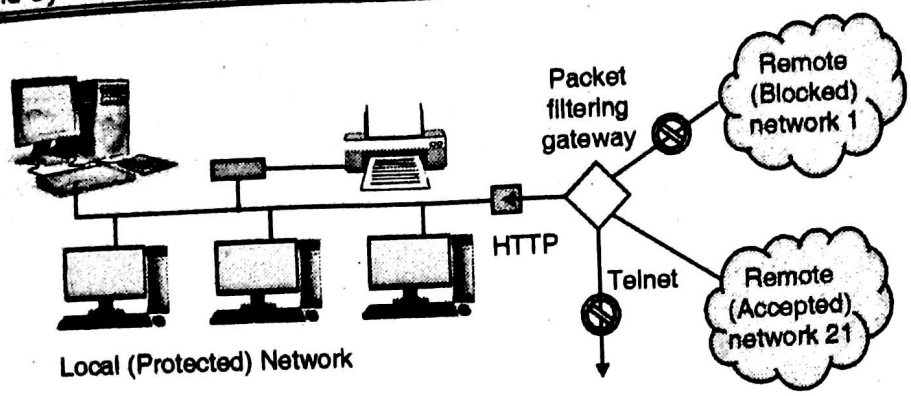


Fig. 10. 1 :Packet Filter Blocking Addresses and Protocols

(II) Stateful Inspection Firewall :

Packet filtering is done one packet at time. Sometimes attacker may use this technique for their attack. Attacker can split the script of attack into different packets so that the complete script of attack cannot be identified by packet filtering firewall.

To avoid this stateful inspection firewall keeps record of states of the packets from one packet to another. Thus sequence of packets and conditions within the packets can be identified easily.

Application Proxy :

Packet filters cannot see inside the packets. From the packet headers they just get IP addresses for filtering. Application proxy is also known as a bastion host. Fig. 10.2 shows firewall proxies.

Example : A college wants to publish a list of selected students. Then they just want students to read that list. No student can change that list. Moreover students can not access more data than the list. Application proxy helps us in this regard. Here it helps us to check only list is displayed on the screen and not more than that. That list should not have any modified contents. Proxies on the firewall can be customized as per the requirements.

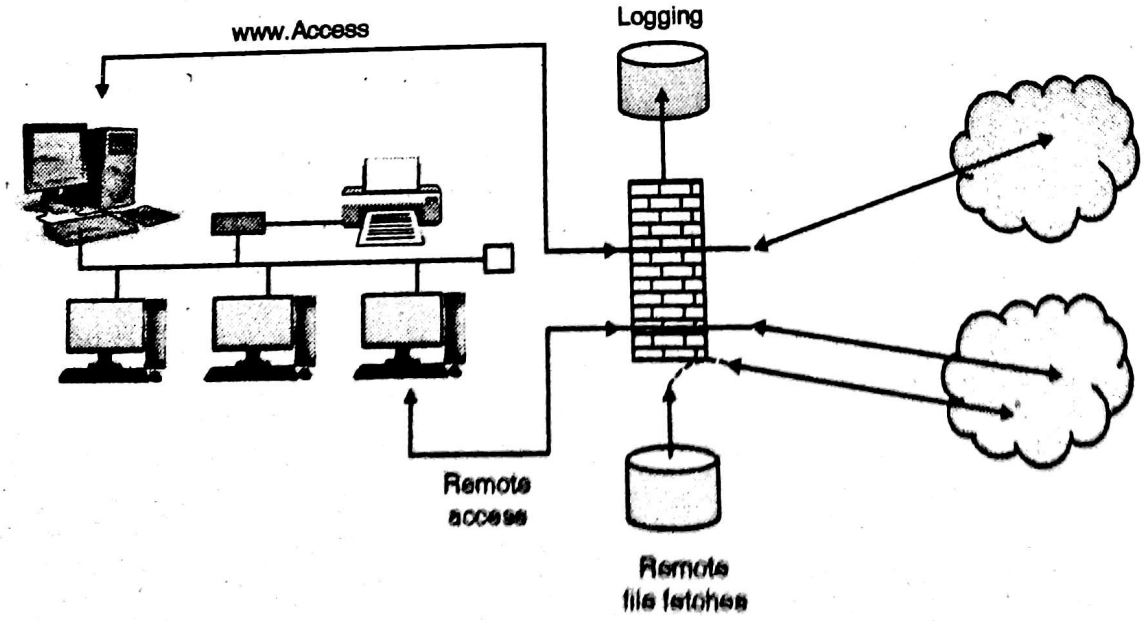


Fig. 10.2 : Firewall Proxies

(iii) Guard :

A guard is kind of complex firewall. It works similar to proxy firewall. Only difference is that guard can decide what to do on behalf of the user by using available knowledge. It can use knowledge of outside users identity, can refer previous interactions, blocked list etc.

Example : In order to increase the speed of the internet a school can set download limit for the students. A student can download only 20mb data per day etc.

Dec. 2012

Q. 7 What is personal firewalls?

Ans. :

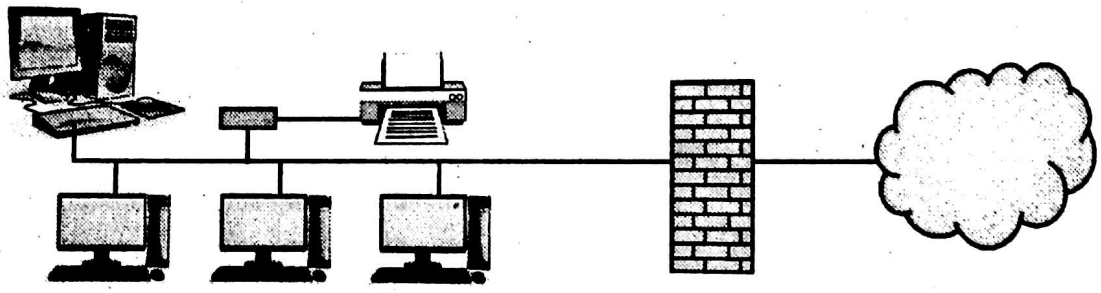
For a personal use to keep separate firewall on a separate machine is quite difficult and costly. So personal users need a firewall capability on lower cost. An application program which can have capabilities of a firewall can solve this problem. It can screen incoming and outgoing traffic on a single host. Symantec, McAfee, Zone alarm are the examples of personal firewalls. Personal firewalls can be combined with antivirus systems.

May 2015

Q. 8 Explain design, configuration and limitations of firewall ?

Ans. :

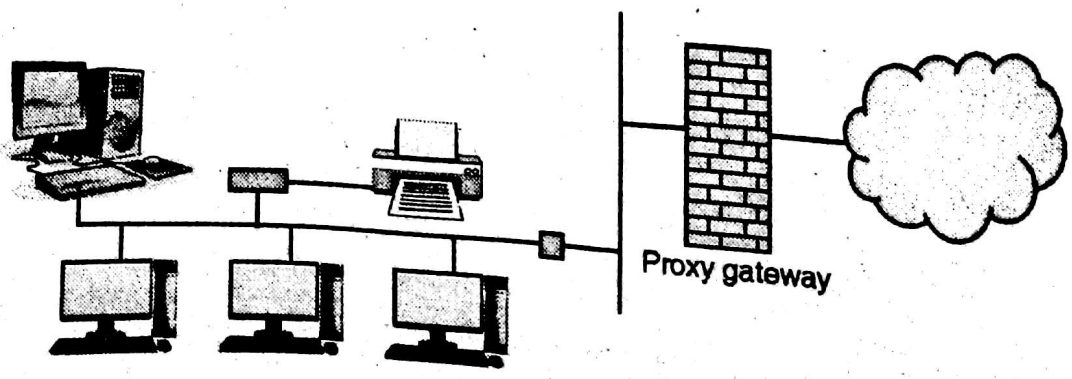
1. Firewall with screening router :



The screening router is placed in between intranet and extranet. It is suitable only if the address screening of the router. The disadvantage of this configuration is that if the screening router is successfully attacked then intranet is directly visible.

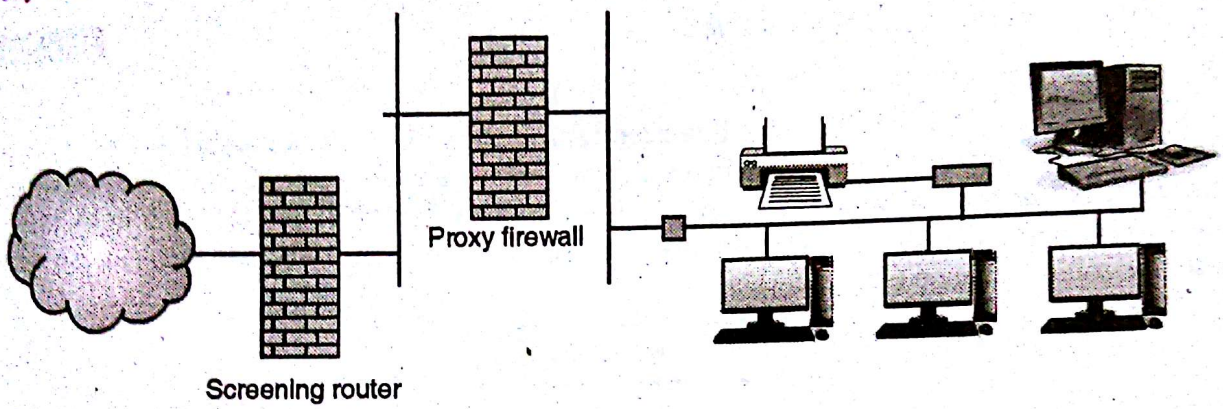
2. Firewall on Separate LAN :

To overcome the problem of the exposure of LAN, a proxy firewall can be installed on its own LAN.



3. Firewall with Proxy and Screening Router :

If screening router is installed behind the proxy firewall, then it ensures the correct address to proxy firewall. In other words it is a double guard protection. If any one fails LAN is not exposed.



❑❑❑

Chapter 11 : IP Security

May 2014

Q. 1 IPSec offers security at network layer.

Ans. :

IPSec is designed by the Internet Engineering task force IETF. It is a collection of protocols which provides security for a packet at network level. IPSec creates authenticated and confidential packets for network layer also known as **IP(Internet Protocol layer).** IPSec provides node to node communication in routing protocols; it provides security to other protocols also which are used for client-server communication in transport layer.

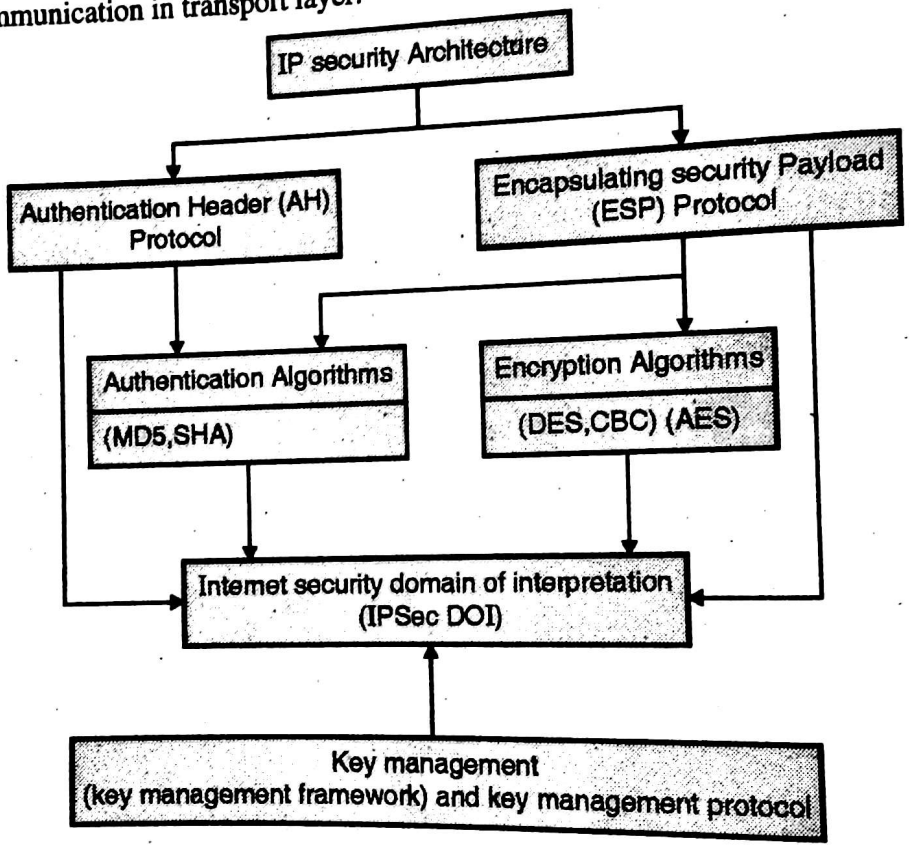


Fig.11.1: IPSec architecture

IPSec defines two protocols as they are backbone of IPSec, are **Authentication Header** (AH) and **Encapsulating Security Payload (ESP)** protocol.

1. Authentication Header (AH):

It defines the AH packet format for processing incoming and outgoing packets. AH helps to ensures that authentication and integrity of the data/packets is protected.

2. Encapsulating Security Payload (ESP):

It defines the ESP packet header, which transmits packets in encrypted and unreadable format. ESP helps to ensure that confidentiality, authenticity and integrity of the data is protected.

3. Authentication algorithms:

Use of MD-5 and SHA with Encapsulating Security Payload to achieve Authentication, integrity and protection of data. Hash is attached to the IP header as an integrity checksum.

4. Encryption algorithms:

Few standard encryption algorithms are implemented in IPSec are DES, AES and CBC because of large key size to secure data.

5. Internet security Domain of Interpretation (DOI):

It contains the supporting database of all IP Security protocols, their parameters, all defined algorithms, key size with lifetime and identity of all approved encryption and decryption algorithms.

6. Key management:

As defined earlier key management is used to generate and distribute the keys required for IPSec protocols.

Q. 2 What are different modes of IPSec ?

Ans. :

IPSec operates in two different modes :

(1) Transport Mode (2) Tunnel Mode

(1) Transport Mode

In Transport mode IPSec protects the data that is delivered from transport layer to network layer or in other words, we can say that, transport mode protects the payload (a packet consist of controlled information and user data) of network layer. It encapsulates the transport layer payload by adding IPSec header and IP Sec trailer and sends this encapsulated packet to network layer.

After that the IP headers of network layer is added to that encapsulated payload. IPSec transport mode is responsible for complete delivery of packet (traffic) from one host to another host or from host to gateways called as end-to-end communications.

For example : Communications between client machine and a server machine, communications between two routers and from router to gateway is also considered as **end-to-end communication.** IPSec transport mode is responsible for secure communications between all these devices.

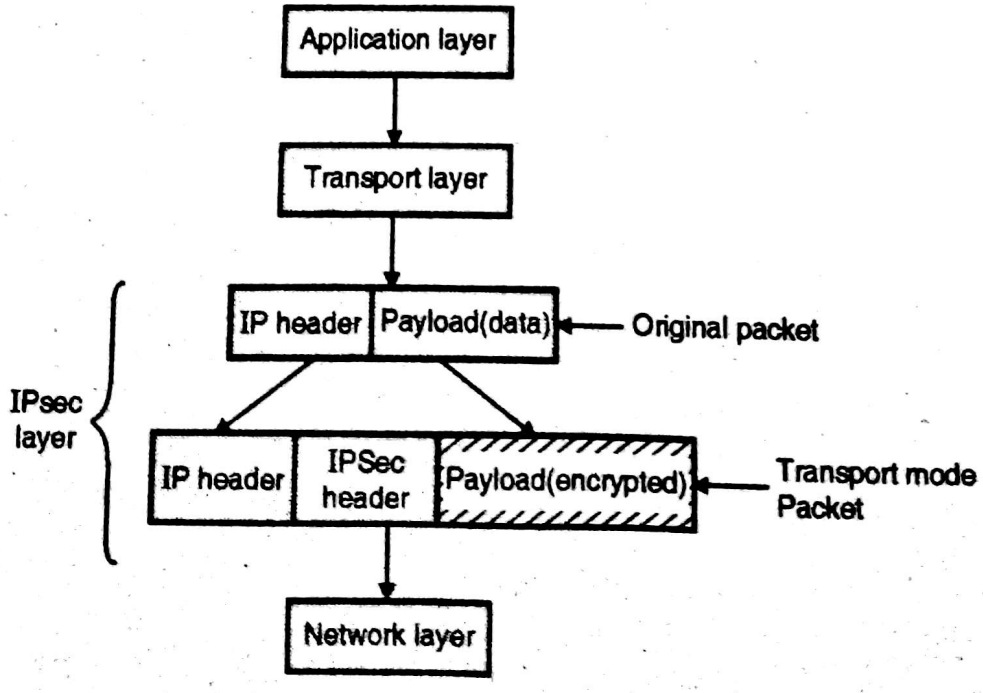


Fig. 11.2 : Transport mode

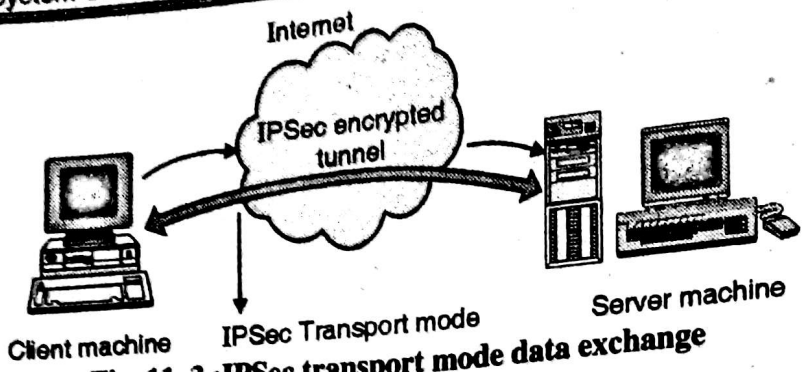


Fig. 11. 3 :IPSec transport mode data exchange

Transport mode helps to protect user data, also known as IP payload through an AH or ESP header. In transport mode payload of IP packet is encrypted by the IPSec headers and trailers but the IP header information, which is remain unchanged as shown in Fig. 11.2. The payload of an IP packet is protected before it is handled by the network layer as shown in Fig. 11.2. Fig. 11. 3 shows how the data exchange (end to end security) take place after encrypting payload.

(2) Tunnel Mode

In tunnel mode, the IPSec protects the entire IP Packet of Network Layer. It takes whole IP packet including the header of that IP Packet and applies the IPSec method to the whole packet and adds new IP header. IPSec tunnel mode is responsible for network-to-network communications, it encrypt the traffic between routers, gateways or host-to-network and host-to-host communications over the Internet and creates a secure tunnel.

IPSec tunnel mode encrypts complete IP packet including IP header and transfer it over network layer (entire original IP packet is encrypted). Tunnel mode binds the original IP packet, encrypts it, adds a new IP header and IPSec header sends it to the other end of IPSec shown in Fig.11.4. Fig. 11.5 shows IPSec tunnel mode during data exchange process.

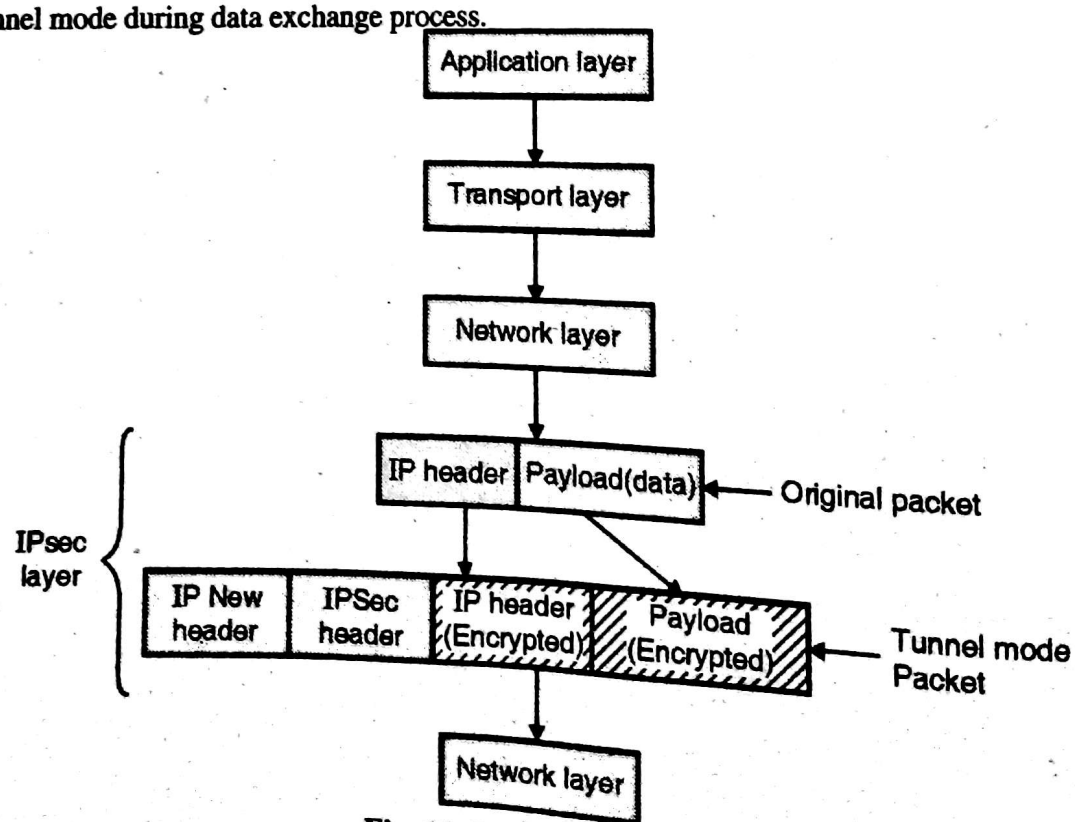


Fig. 11. 4 :Tunnel Mode

Tunnel mode is used on most of the IPSec gateway devices such as firewalls, routers, and connecting remote locations such as branch offices, organizations, and universities securely through a network called **Virtual Private Network (VPN)**.

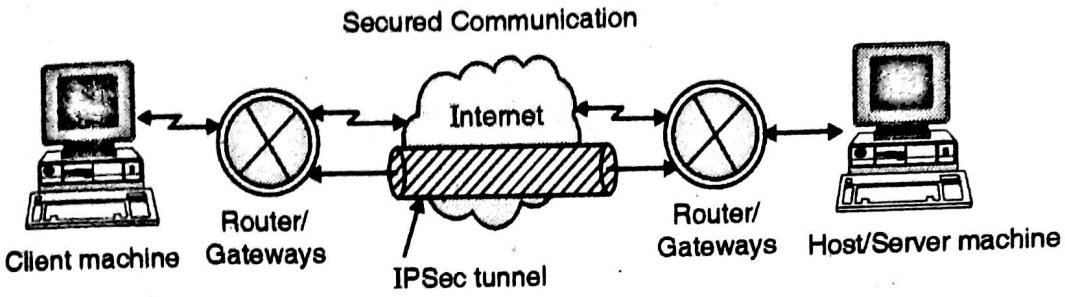


Fig. 11.5 : IPSec tunnel mode data exchange

The IP header after tunnel mode will consist information different from the original IP that was received previously. Tunnel mode is generally used for secure communication between two routers, a host and a router or vice versa.

Q. 3 How AH and ESP are differs while working under transport and tunnel mode ?

Ans. :

Encryption of data and its authenticity is prime concern for secure communication, to avail this two features, IPSec provides two protocols at network layer :

1. Authentication Header
2. Encapsulating Security Payload

(1) Authentication Header

It is designed for authentication, integrity of payload which is carried in IP packet. It is first protocol of IPSec called Authentication Header (AH) protocol designed to provide data authentication (to identify source host), data integrity (if data get modified while in transit) and non-repudiation but doesn't provide data confidentiality (if attacker able to access the contents of a message) because Authentication header does not encrypt the data/ IP packet.

The main functionality of this protocol is protection against replay attacks (sending same data to receiver again and again) and protection against tampering of data over a network. Authentication header is also used to protect the upper-layer or the entire IP packet, with the help of message authentication code (MAC - used to generate fixed length value from message and secret key to provide authentication) using well known hashing algorithms like MD5 or SHA1.

By using Hash function and symmetric key algorithm, message digest is calculated and inserted in authentication data as shown in Fig.11.6 because of this AH protocol provides data authentication and data integrity, but not confidentiality or privacy. The internal fields of authentication header format are shown in Fig. 11. 6. This protocol uses cryptographic checksum which is similar to hash function or message digest, the checksum is inserted in authentication header and placed in location cased on which mode it is using (tunnel mode or transport mode).

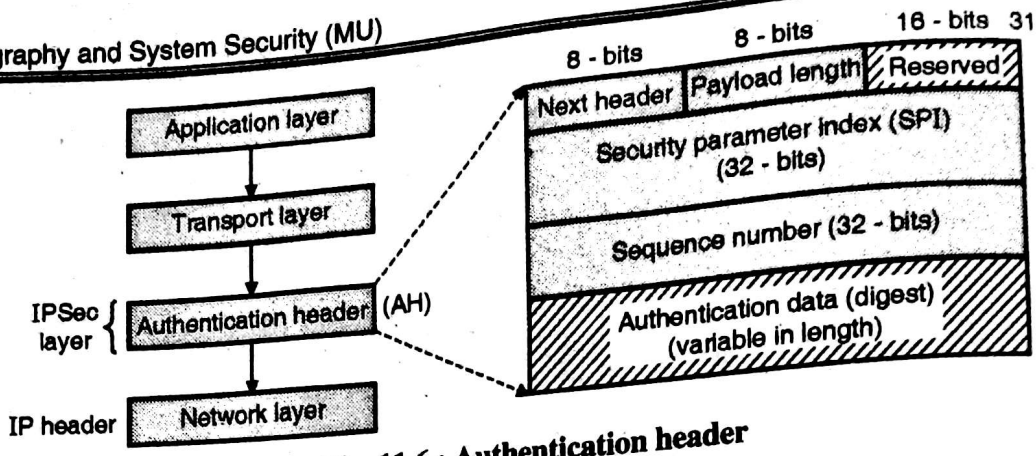


Fig. 11.6 : Authentication header

A brief description of each field:

Next header (8 bits) : The next header is an 8 - bit field which is used to identify the type of payload/ data carried by IP packet.

Payload length (8 bits): The payload header is also an 8 - bit field which defines length of the authentication header.

Reserved (16 bits) : AH contains 16-bit field which is reserved for future use and always set to zero.

Security Parameter Index (SPI) (32 bits): SPI is a 32-bit field used in combination with source IP address, destination IP address and AH security protocol to uniquely identify a security association (SA) for the traffic to which IP packet belongs, we will discuss SA in next bit. This field also defining which different security algorithms and keys were used to calculate the message authentication code (MAC).

Sequence number (32 bits) : It is also a 32 bit field. It prevents the retransmission of datagram which is also known as **replay attack.**

Authentication data : This is variable length field whose length depends upon encryption algorithm used. Authentication data field of AH protocol is the output of hashing algorithm or message digest algorithm. AH protocol performs the integrity check value (ICV) on packet header or MAC is computed over the complete IP packet including the outer IP header to ensure that the data has not been changed during transmission process. As mentioned earlier AH doesn't encrypt the data the reason it doesn't provide confidentiality during transmission.

(2) Encapsulating Security Payload :

One of the most important feature that Authentication Header was unable to provide called data confidentiality (if attacker able to access the contents of a message) because ESP provide encryption on data/ IP packet. As defined earlier ESP is used to encrypt the entire payload of an IPSec packet the reason ESP alone can provide data authentication, protection against replay attacks and data integrity by adding ESP header, ESP trailer and MAC to the packet.

ESP has the same fields as defined in AH, but it integrates these fields in a different way instead of having just a header, it divides these fields into three components: An ESP header, ESP trailer and ESP authentication block as shown in Fig. 11.7.

It is designed for confidentiality and integrity of messages. ESP can be used alone or with combination of AH.ESP adds a header and a trailer to the payload. Following are the steps for adding ESP header and trailer.

Step 1 : In the initial step, ESP trailer is added to IP payload.

Step 2 : Then both Trailer and ESP are encrypted.

Step 3 : After the encryption ESP header is added to the encrypted packet.

Step 4 : Then all encrypted Trailer ESP trailer and ESP header are combine used to form authentication data.

Step 5 : This authentication data is added to the End of Trailer.

Step 6 : Lastly the IP header is added.

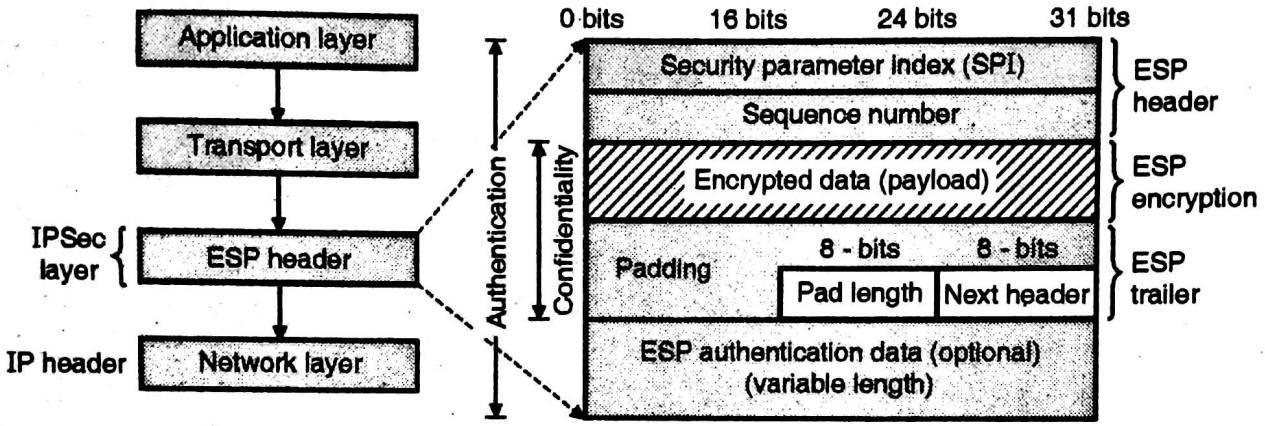


Fig. 11.7 : ESP header, trailer and encryption

The main functionality of ESP is to provide the confidentiality to IP packet by encrypting them. Encryption algorithms (Triple DES, Blowfish, and IDEA etc.) used to combines the data in the packet with a key and transform it into an encrypted form. The encrypted packet now then transmitted to the destination, and decrypts it using the same algorithm.

The detail description of Encapsulating Security Payload (ESP) fields is given below :

1. ESP header :

It is also a 32 bit field. It prevents the retransmission of datagram which is also known as **replay attack as defined earlier.** This field is not encrypted but it's authenticated to perform anti-replay checking before decryption.

2. Encrypted data :

This is variable length filed contains transport layer segment or IP packet which is protected by performing ESP encryption.

3. ESP trailer :

ESP trailer field contains padding (0-255 bytes), pad length 8-bits and next header 8 - bits.

4. Padding (0-255 bytes) :

Padding filed used to expand plain text message to required size or to align the encrypted data by adding padding bits to the actual data which provides confidentiality to traffic flow.

5. Pad length (8 bits) :

This is mandatory field in ESP protocol which used to indicate the number of pad (protection) bytes added into the packet.

6. Next header (8 bits) :

The same bit length as of pad length used to identifies the type of encrypted data in the Payload Data field.

7. ESP authentication data :

This is variable length field whose length depends upon encryption algorithm used. Authentication data field of ESP protocol is the output of hashing algorithm or message digest algorithm, which performs the integrity check value (ICV) on packet header or MAC, is computed over the complete packet including the outer IP header to ensure data has not been changed during transmission process.

Q. 4 How does ESP header guarantee confidentiality and integrity for packet payload? May 2014

Ans. :

One of the most important feature that Authentication Header was unable to provide called data confidentiality (if attacker able to access the contents of a message) because ESP provide encryption on data/ IP packet.

As defined earlier ESP is used to encrypt the entire payload of an IPSec packet the reason ESP alone can provide data authentication, protection against replay attacks and data integrity by adding ESP header, ESP trailer and MAC to the packet.

ESP has the same fields as defined in AH, but it integrates these fields in a different way instead of having just a header, it divides these fields into three components: An ESP header, ESP trailer and ESP authentication block as shown in Fig. 11.8.

It is designed for confidentiality and integrity of messages. ESP can be used alone or with combination of AH.ESP adds a header and a trailer to the payload. Following are the steps for adding ESP header and trailer.

Step 1 : In the initial step, ESP trailer is added to IP payload.

Step 2 : Then both Trailer and ESP are encrypted.

Step 3 : After the encryption ESP header is added to the encrypted packet.

Step 4 : Then all encrypted Trailer ESP trailer and ESP header are combine used to form authentication data.

Step 5 : This authentication data is added to the End of Trailer.

Step 6 : Lastly the IP header is added.

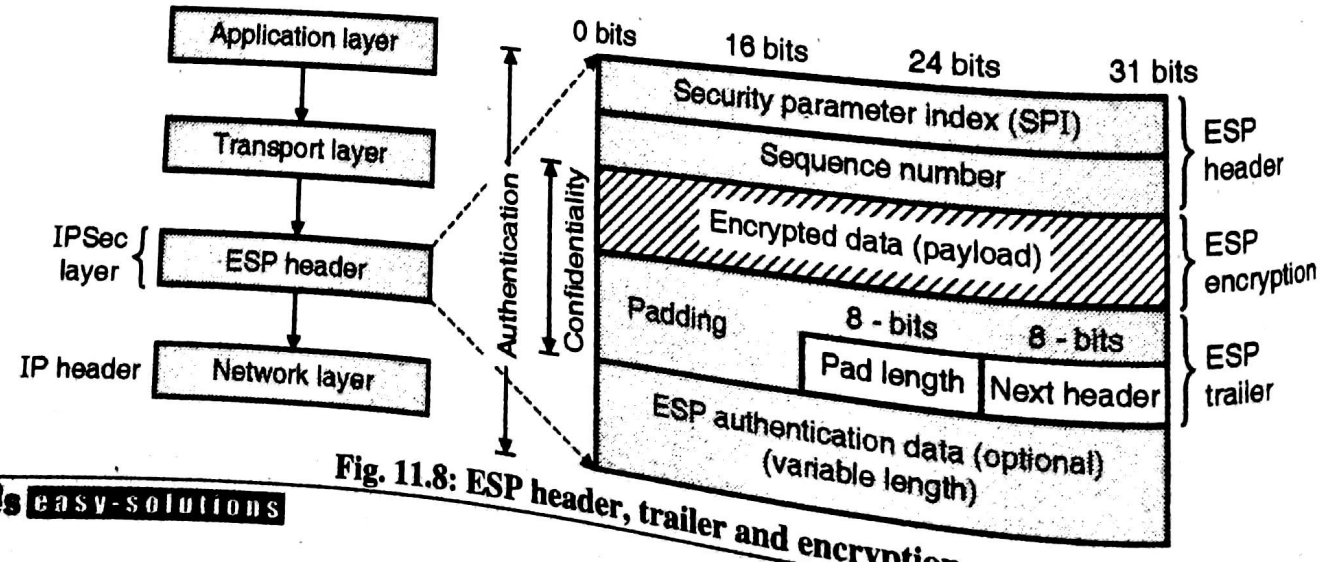


Fig. 11.8: ESP header, trailer and encryption

The main functionality of ESP is to provide the confidentiality to IP packet by encrypting them. Encryption algorithms (Triple DES, Blowfish, and IDEA etc.) used to combines the data in the packet with a key and transform it into an encrypted form. The encrypted packet now then transmitted to the destination, and decrypts it using the same algorithm.

The detail description of Encapsulating Security Payload (ESP) fields is given below:

1. **ESP header:**

It is also a 32 bit field. It prevents the retransmission of datagram which is also known as **replay attack as defined earlier.**

This field is not encrypted but it's authenticated to perform anti-replay checking before decryption.

2. **Encrypted data:**

This is variable length filed contains transport layer segment or IP packet which is protected by performing ESP encryption.

3. **ESP trailer:**

ESP trailer field contains padding (0-255 bytes), pad length 8-bits and next header 8 - bits.

4. **Padding (0-255 bytes):**

Padding filed used to expand plain text message to required size or to align the encrypted data by adding padding bits to the actual data which provides confidentiality to traffic flow.

5. **Pad length (8 bits):**

This is mandatory field in ESP protocol which used to indicate the number of pad (protection) bytes added into the packet.

6. **Next header (8 bits):**

The same bit length as of pad length used to identifies the type of encrypted data in the Payload Data field.

7. **ESP authentication data:**

This is variable length field whose length depends upon encryption algorithm used. Authentication data field of ESP protocol is the output of hashing algorithm or message digest algorithm, which performs the integrity check value (ICV) on packet header or MAC, is computed over the complete packet including the outer IP header to ensure data has not been changed during transmission process. ESP encrypts the data the reason it provide data confidentiality during transmission.

Q. 5 What are benefits of IP security ?

Ans. :

IP Sec operates at the network layer where secure data transmission takes place. For secure access of remote computer over Internet IPSec is used. For securely connecting all branches of bank sectors over internet IPSec protocol is used. For secure communication between same organization which are located at different places.

For connecting to college server any time from any location IPSec protocol is used. Most of the corporate sector allowing employees to performed their task from home and update it to company server at any time from any location or secure access of company server at any time. IPSec now-a-days called as one of the standard of Virtual Private Networks that allow low cost connectivity, secure data transmission between various locations over insecure communication channel. If IPSec is implemented in a *firewall or router*, can provide strong security to the ongoing traffic crossing the network.

Q. 6 Why Secure Socket Layer (SSL) is needed ? What are the different features SSL provides ? Explain how SSL works ? Also explain the services of SSL protocol.

May 2012, Dec. 2013, May 2014

Ans. :

Secure Socket layer invented by Netscape communications in 1994. Secure Socket layer is an internet protocol used for securely exchanging the information between client's web browser and the web server. Secure socket layer ensure the authentication, data integrity and data confidentiality between web browser and web server i.e. it creates a secure tunnel between client and server. The main role of SSL is to provide the security to web traffic in all the way.

The current version of SSL is 3.0. The position of SSL in TCP/ IP protocol suite is shown in Fig. 11.9. SSL is works in between application layer and transport layer the reason SSL is also called as Transport Layer Security (TLS). The data will not be passed directly to transport layer instead it will passed to secure socket layer. Secure Socket Layer will perform encryption to the data received by application layer and add its own encryption information header called SSH i.e. Secure Socket Layer Header. In the receiver's end SSL will remove the SSH header and then pass data to application layer.

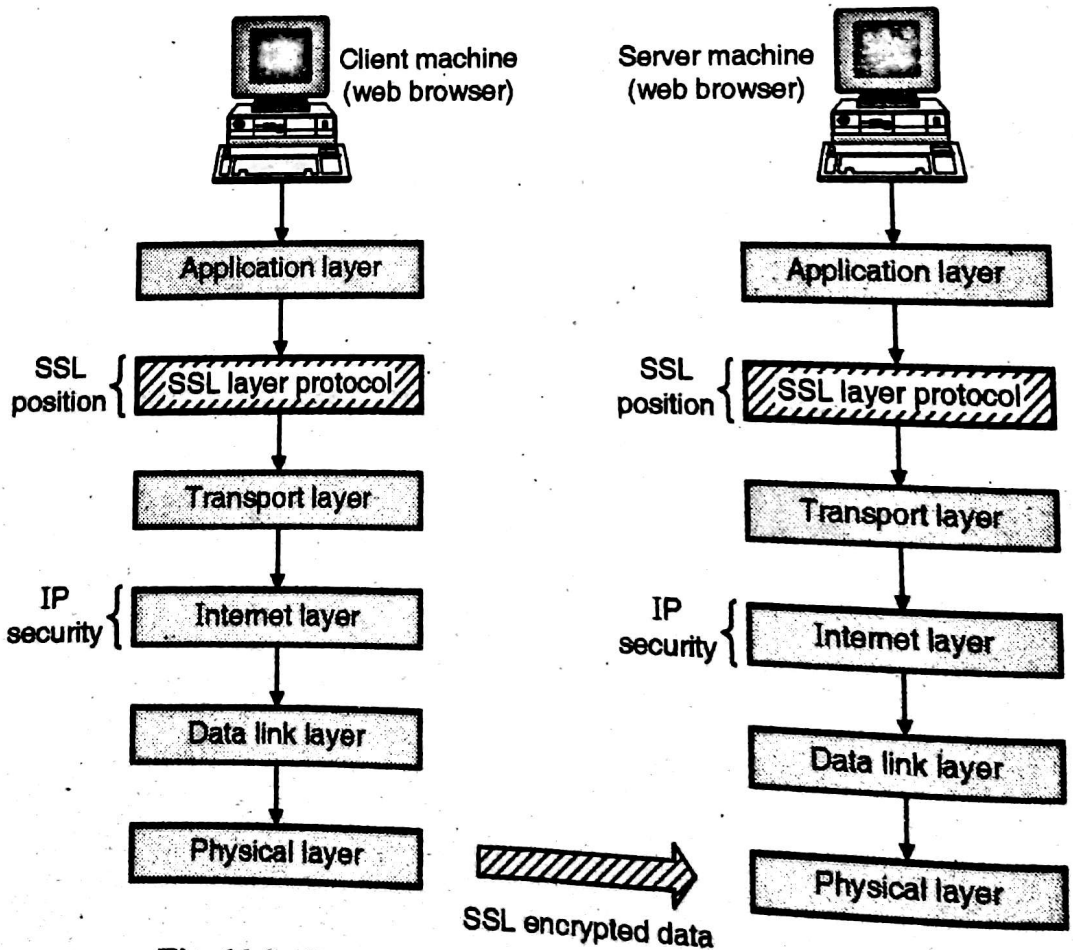


Fig. 11.9 : Position of SSL in TCP/ IP protocol suite

The Fig. 11.9 shows position of SSL protocol in TCP/ IP protocol suite. SSL protocol uses digital certificate and digital signature for securely communication between client machine and server machine. SSL encrypt the data received from application layer of client machine and add its own header (SSL Header) into the encrypted data and send encrypted data to the server side. Upon receiving encrypted data, server removes the SSL header and decrypts the data and sends the decrypted data to application layer as shown in Fig. 11.9.

SSL is not a single protocol to perform security tasks there are two layers of sub-protocols which support SSL there are the SSL Handshake Protocol, SSL Change Cipher Specification, the SSL Alert Protocol, and the SSL Record Protocol shown in SSL architecture Fig. 11.10. As shown in Fig. 11.10. SSL defines three basic higher-layer protocols namely: SSL Handshake, SSL Change Cipher Specification and SSL Alert protocol.

The role of these three higher-level protocols is the connection establishment, use of required cipher techniques for data encryption and alert (warning, error if any) generation before starting actual data transmission process between client and server.

The SSL Record Protocol is responsible encrypted data transmission and encapsulation of the data sent by the higher layer protocols (handshake, alert, HTTP) also to provide basic security services to higher layer protocols. SSL was designed to make use of TCP protocol to provide a reliable secure process-to-process delivery of entire message/packets. We will discuss how client machine securely communicate with the server machine by using underlying network architecture.

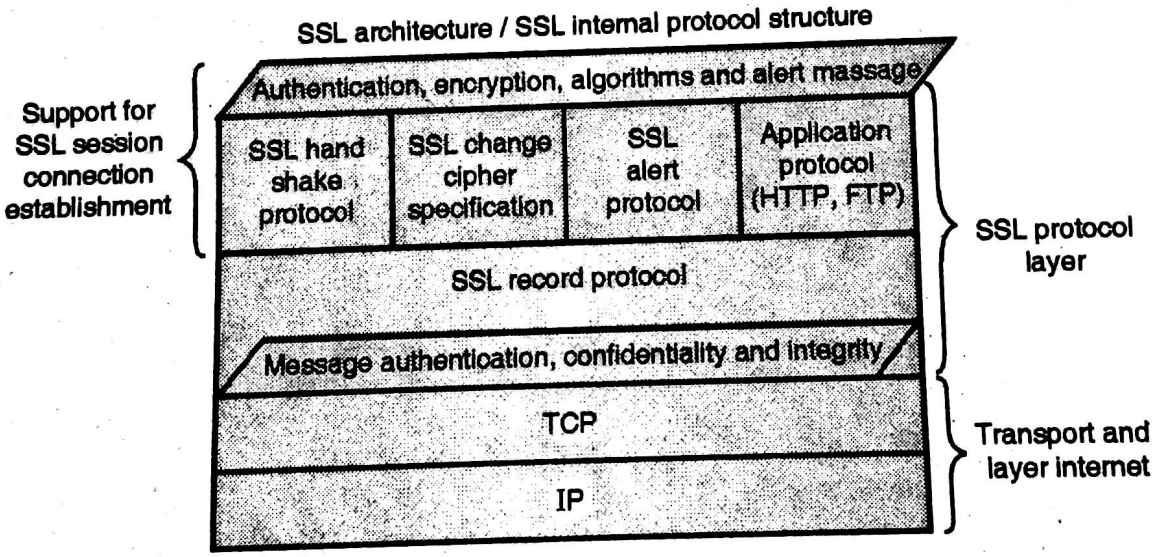


Fig. 11.10 : SSL protocols internal architecture

Working of SSL

SSL has three sub protocols: Handshake protocol, Alert protocol and Record protocol.

Handshake Protocol

As the name suggests when we meet to our friend/colleagues, we have habit to say hi/hello and do the *shake-hands* with each other before starting our actual communication. SSL handshake protocol uses somewhat same ideology but in terms of client and server.

The first sub-protocol of SSL called *handshake protocol* used for secure communication between client and the server using an SSL enabled connections.

In this protocol client authentication to the server is more important that server authentication because server has different options available for client authentication. The details **steps of SSL handshake protocol** are shown in Fig. 11.11.

1. It is used by client and server to start communication using SSL enabled connection.
2. The handshaking is done four phases :
   (a) Establishing security Capabilities.
   (b) Server Authentication and key exchange.
   (c) Client authentication and Key exchange.
   (d) Finalizing and Finishing.

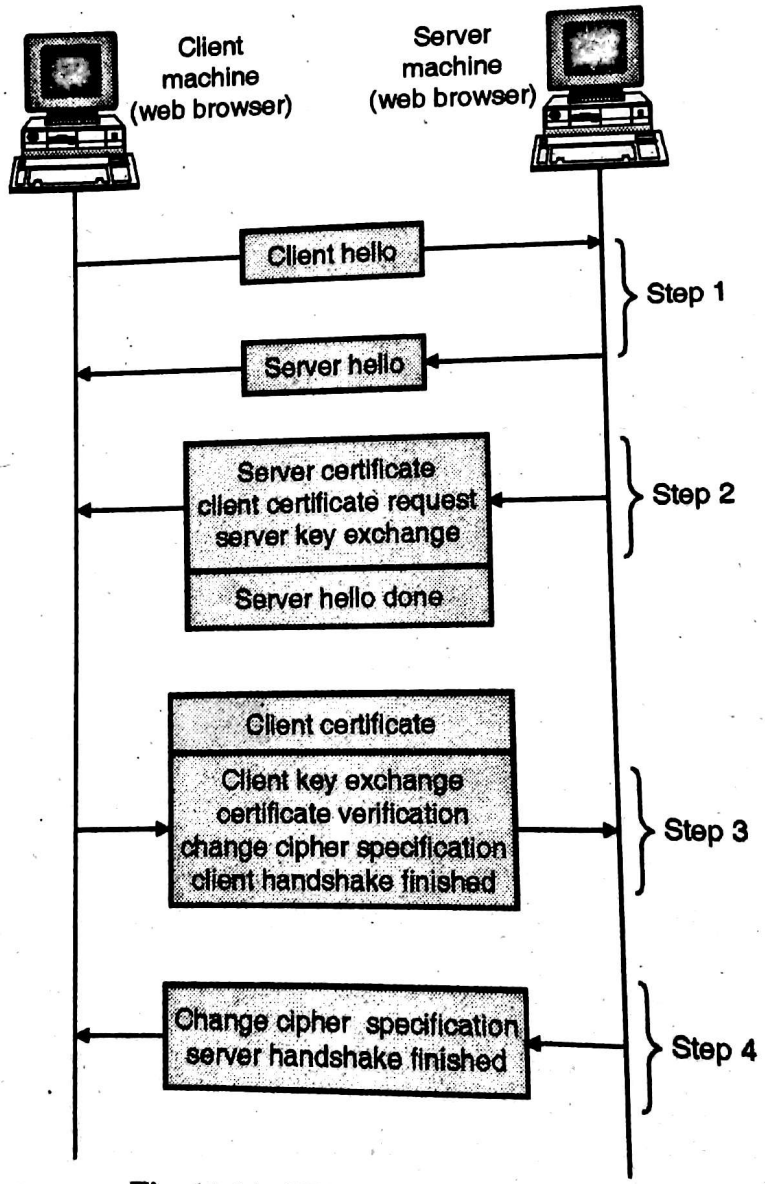


Fig. 11.11 :SSL handshake protocol

Phase 1 : Establishing security capabilities

In this phase logical connections and is established between client and server and establish security capabilities associated with that connections. It consists of two messages , the client hello and

Client hello :

The client hello message contains the following parameters :

(i) The highest SSL version number which the client can support.

(ii) A 32 byte random number that will be used for master secret generation. It contains two subfield that is a 32 bit date time subfield for current time and date of the client's system and a 28 byte random number generator which shows random number generated in client's system.

(iii) A session id that defines the session.

(iv) There is a cipher suite parameter that contains the entire cryptographic algorithm which supports client's system.

(v) A list of compression methods that can be supported by client.

Server :

(i) The SSL version number, the highest among both SSL number of client and server, will be supported by client and other will be supported by server.

(ii) A 32 byte random number that will be used for master secret generation, however this random number is totally independent from the random number of client.

(iii) A session id that defines the session.

(iv) A cipher suite contains the list of all cryptographic algorithms that is sent by the client from which the server will select the algorithm

(v) A list of compression methods sent by the client from which the server will select the method.

Phase 2 :Server authentication and key exchange

In this phase, the server authenticates itself if it is needed. The server sends its certificate, its public key, and also request certificate (digital certificate) from the client.

1. **Certificate :** The server sends a certificate message to authenticate itself to the client. If the key exchange algorithm is Diffie Hellman than no need of authentication.
2. **Server key exchange :** This is optional. It is used only if the server doesn't send its digital certificate to client.
3. **Certificate request :** The server can request for the digital certificate of client. The client's authentication is optional.
4. **Server Hello done :**The server message hello done is the last message in phase 2 .this indicates to the client that the client can now verify all the certificates received by the server . After this hello message done, the server waits for the client's side response in phase 3.

Phase 3 :Client authentication and key exchange

In this phase, the client authenticates itself if it is needed .The client sends its certificate, client key exchange and certificate verify to the server.

Certificate : Client certificate is optional, it is only required if the server had requested for the client's digital certificate. If client doesn't have client's digital certificate it can send no certificate message or an Alert message to the server. Then it is upto server's decision whether to continue with the session or to abort the session.

Client key Exchange : The client sends a client key exchange, the contents in this message are based on key exchange algorithms between both the parties.

Certificate verify : It is necessary only if the server had asked for client authentication. The client has already sent its certificate to the server. But additionally if server wants then the client has to prove that it is authorized holder of the private key .The server can verify the message with its public key already sent to ensure that the certificate belongs to client.

Phase 4 :Finish

The client and server send messages to finish the handshaking protocol. It contains 4 steps. The first two messages are from the client i.e. change cipher specs, finished. The server responds back with change cipher spec and finished.

Change cipher spec : It is a client side message telling about the current status of cipher protocols and parameters which has been made active from pending state.

Finished : This message announces the finish of the handshaking protocol from client side.

Change Cipher spec : This message is sent by server to show that it has made all the pending state of cipher protocols and parameters to active state.

Finished : This message announces the finish of the handshaking protocol from server and finally handshaking is totally completed.

Alert Protocol

SSL uses the Alert protocol for reporting error that is detected by client or server, the party which detects error sends an alert message to other party. If error is serious then both parties terminate the session. Table 11.1shows the types of alert messages.SSL alert protocol is the last protocol of SSL used transmit alerts (warnings, errors, fatal etc.) if any via SSL record protocol to the client or server.

The SSL alert protocol format is shown in Fig. 11.12. Alert protocol uses two bytes to generate alert. First 1 byte indicates two values either 1 or 2. "1" value indicate warning and "2" value indicate a fatal error (if fatal error terminate the session/ connection).

Whereas second 1 byte indicates predefined error code either the server or client detects any error it sends an *alert* containing the error (error occurred during handshaking, error occurred during data processing at server or client side, certificate defeats, etc.)

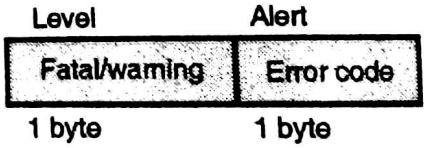


Fig.11.12: SSL alert protocol format

Table 11.1

Alert Code	Alert message	Description
0	close_notify	No more message from sender
10	unexpected_message	An incorrect message received
20	bad_record_mac	A wrong MAC received
30	decompression_failure	Unable to decompress.
40	handshake_failure	Unable to finalize handshake by the sender..
42	bad_certificate	Received a corrupted certificate.
42	Nocertificate	Client has no certificate to send to server.
42	Certificate expired	Certificate has expired.

Record Protocol

After completion of successful SSL handshaking the keen role of SSL record protocol starts now. SSL record protocol is second sub-protocol of SSL also called lower level protocol. As defined earlier the SSL Record Protocol is responsible for encrypted data transmission and encapsulation of the data sent by the higher layer protocols (handshake, alert, HTTP) also to provide basic security services to higher layer protocols. SSL record protocol is basics for data transfer and specially used to build a data path between client and server and encrypt the data path before communication.

SSL record protocol provides different service like data authentication; data confidentiality though encryption algorithms and data integrity through Message Authentication (MAC) to SSL enabled connections. The details steps involved in SSL record protocol and SSL record header format as shown in Fig. 11.13. At this stage all necessary authentication and cryptographic parameters are exchanged between client and server now it's time of secure SSL data transmission through SSL record protocol. As shown in Fig. 11.13.

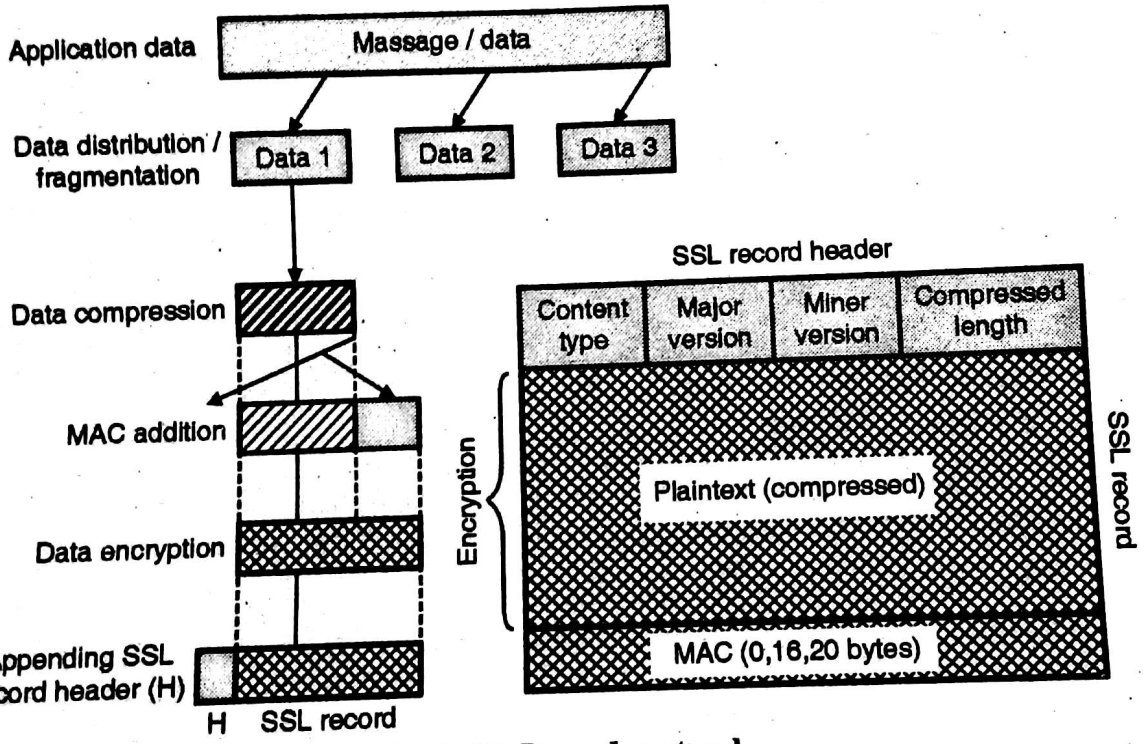


Fig.11.13: Record protocol

SSL record protocol takes application data i.e. actual data that client wants to send over server. Divide this data into the different blocks for each length should not exceed 16384 bytes this process is called as *data distribution* or *data fragmentation*. Data compressed using lossless compression techniques; compression size of data should not exceed 1024 bytes.

After the data fragmentation and compression step the MAC is computed over the data and MAC is then appended to the compressed data (the data is now encapsulated) to form a new encrypted data / payload. The compressed data and MAC again goes through data encryption process. As mentioned earlier SSL record protocol uses symmetric key cryptographic techniques like DES, triple DES, AES, and IDEA because these techniques specially designed to operate on block ciphers.

Finally SSL record header is appended onto each encrypted blocks obtained from encryption process. SSL record header consist of 8-bit content type to which identify nature of the message whether any application data or connection termination or any error message. Next field is Major Version which

is 8-bit field used to indicate latest version of SSL is in use (e.g., 3). Minor Version which is 8-bit field indicates the lowest version of SSL is in use (e.g., 0).

Plaintext (compressed) / compressed length which is 16-bit field indicates the length of the plaintext being compressed. Finally sends SSL layer encrypted data to TCP and IP (Transport and Internet layer) for necessary transmission over network. At the receiver end, the encrypted blocks are decrypted and then checked for data authentication, data confidentiality and data integrity, reassemble these data into single unit, and delivered to the application-layer protocol.

The record protocol provides two services in SSL connection :

(a) Confidentiality :

This can be achieved by using secret key, which is already defined by handshake protocol.

(b) Integrity :

The handshake protocol defines a shared secret key that is used to assure the message integrity. Following are the **operations** performed in Record protocol after connection is established and authentication is done of both client and server.

1. Fragmentation :

The original message that is to be sent is broken into blocks .The size of each block is less than or equal to 2^{14} bytes.

2. Compression :

The fragmented blocks are compressed which is optional. It should be noted that the compression process must not result into loss of original data .

3. Addition of MAC :

The Message authentication code (a short piece of information used to authenticate a message for integrity and assurance of message) for each block is to be calculated using shared secret key.

4. Encryption :

The overall steps including message is encrypted using symmetric key but the encryption should not increase the overall block size.

5. Append header :

After all the above operations, header is added in the encrypted block which contains following fields :

Content type (8 bits) specifies which protocol is used for processing. Major Version (8 bits) specifies the major version of SSL used, for example if SSL version 3.1 is in use than this field contains 3. Minor Version (8 bits) specifies the minor version of SSL used, for example if SSL version 3.0 is in use than this field contains 0. Compressed length (16 bit) specifies the length in bytes of the original plain text block.

Q. 7 Solve TLS.

Ans. : May 2012

It is an extension of secure socket layer. The main aim of TLS is to provide security and data at the transport layer between two web applications. Almost all web browsers and web servers support TLS. It ensures no eavesdropping and tampering of the message.

The TLS protocol consists of two main components : Handshake protocol, to start session and share private key, and Record protocol, to transmit data securely using the shared keys.

Handshake protocol : In the Handshake protocol, both sending and receiving parties acknowledge their protocol versions, agree on cryptographic and compression algorithms, optionally authenticate each other through certificates, and use public-key encryption techniques to generate shared private keys.

Following are the steps :

Step 1 : Clients sends message publicly to containing version of TLS,32-byte random number r_A consisting of a 4-byte timestamp and a 28-byte random number.

A Cipher Suite list in decreasing order of preference for each of the following algorithm families: Public-Key Algorithm (PKA), encryption algorithm used in the Cipher Block Chaining, and compression algorithm (COMPRESS).

Step 2 : Server informs the client about the decided algorithms (after examining the Cipher Suite list sent by the client) along with a 32-byte random number r_B constructed similarly as r_A..

Step 3 : Client replies with a number called pre-master secret s_{pm} using the public key algorithm PKA with public keys retrieved from the server's certificate signed by a Certifying Authority (CA).

Step 4 : Both parties independently calculate the 48-byte long master secret, s_m, to further obtain the keys to exchange data. The master secret is calculated using Pseudorandom Function PRF:s_m = PRF(s_{pm}, "master secret", $r_A||r_B$) It is worth mentioning that in the previous version of TLS the master secret was computed as follows, before MD5 proven to be insecure: MD5(s_{pm}||SHA-1(A||s_{pm}||r_A||r_B)) || MD5(s_{pm}||SHA-1(BB||s_{pm}||r_A||r_B)) || MD5(s_{pm} ||SHA-1(CCC||s_{pm}||r_A||r_B)) Where A, BB, and CCC are strings added for padding.

Step 5 : At this stage, both parties know s_m, s_{pm}, r_A, and r_B. they independently compute the Key Block (KB) that contains all needed private shared keys for this session: KB = P RF(s_m, "key expansion", $r_A||r_B$) KB is then broken into six pieces and labeled as K1, K2, . . . , and K6, before terminating the Handshake phase

Record protocol: Now the client and the server are ready to communicate securely using the key block as a set of security parameters obtained by the Handshake protocol. The Record protocol takes data to be transmitted in one endpoint, fragments the data into manageable blocks, compresses the data, applies a MAC, encrypts by block cipher, and transmits the result. Received data is then decrypted, verified, decompressed, reassembled, and then delivered to higher-level application on the other endpoint. In short, Record protocol ensures that the connection is private via symmetric encryption by sessionunique keys and reliable via integrity check. Suppose the client wants to send data chunk, d.

The client:

1. Compresses the data using the agreed algorithm: d' = COMPRESS(d)
2. Hashes the compressed data for data integrity using K_2: d"= {d' , $HMAC_{K2}$ (d')}
3. Encrypts the data along with its MAC using CBC mode block cipher BCA where the secret key is K_1 and the initialization vector is K_3: d '" = BCA_{K1}(d", K_3)
4. Sends d''' over the public channel

And the server retrieves d from d '":

1. Decrypts the data along with its MAC using BCA_{K1}.
2. Verifies data integrity by computing HMAC of data using K_2 and comparing it with the HMAC computed on the client side

3. Decompresses to retrieve d

The process is reversed when server wants to send data to the client while the last three pieces of the key block is used instead.

Q. 8 Explain Internet key exchange protocol.

Ans. :

Internet Key Exchange protocol is used for managing keys in IPSec network. It allows for automatic creation and managing keys between IPSec peers. It is a hybrid protocol based on three protocols: Oakley, SKEME, and ISAKMP (Internet security association and key management protocol.

ISAKMP :

The internet security association and key management protocol is a framework that defines the formats of payload, the mechanics of implementation of a key exchange protocol, and the exchange of a security association between the parties.

ISAKMP protocol defines the mechanics of implementing a key exchange protocol, and agreement between communicating parties i.e. which are the different features of IPSec protocol has to useetc. and all (simply its negotiation of security association).

ISAKMP provides following features :

It is used to authenticate of remote entity. It manages the secure session between communicating parties by applying different cryptographic techniques. Exchanging required information about key sharing. Negotiation over all data transmission by applying security policies. The reasons ISAKMP establish secure communicating channel between two parties and authenticate them for secure key exchange and negotiation on certain security terms and condition.

Oakley :

It is a key exchange protocol that defines how to obtain authenticated Key for exchange of message between parties. Oakley, within IKE, is used to determine AH and ESP key for each IPsec, by default its uses an authenticated Diffie Hellman key exchange algorithm. Oakley protocol defines the mechanism of key exchange or key agreement protocols in which two parties must agree on key generated before data transmission.

IKE uses different cryptographic techniques and security policies for securely exchanging information between two entities such as Diffie Hellman key exchange, DES, MD5, SHA, RSA algorithm etc.

SKEME :

It is another protocol for exchanging authenticated key between the parties. It uses public key encryption for authentication in key exchange protocol.

Q. 9 Explain different phases of IKE protocol.

Ans. :

IKE has two phases of operations :

Phase 1 : Aggressive mode of exchange : Used to negotiate IKE SA

Phase 2 : Quick mode of exchange : Uses to negotiate IPSec's SA

IKE phase 1 : Aggressive mode of exchange: Uses to negotiate IKE SA

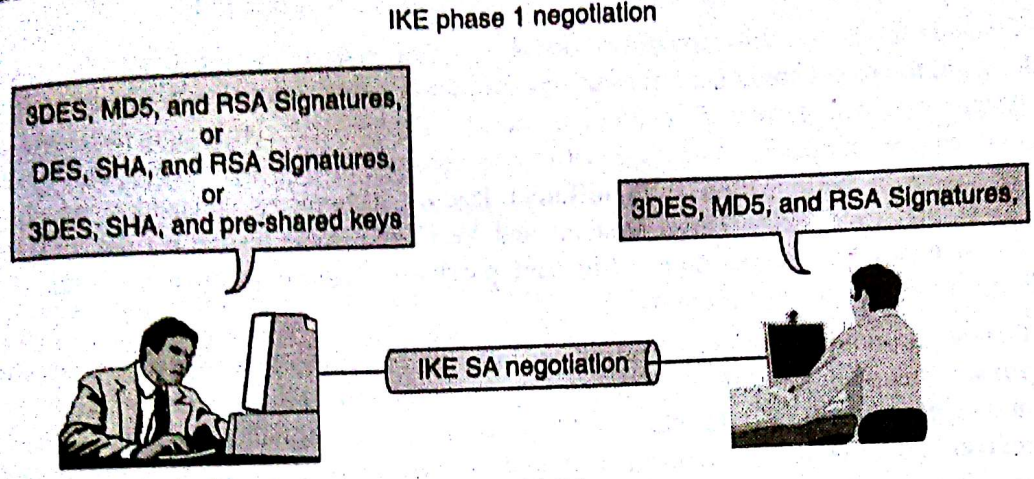


Fig. 11.14

For instance :

As shown in Fig. 11.14 user A and user B want to talk IKE, They must agree on a common IKE protection suite. The initiator (user A) proposes several protection suites and the responder (user B) chooses one of the offered protection suite. The selection is made according to the priorities and the configuration of the responder. In the Fig.11.14, user A proposes three protection suites out of which user B chooses the second protection suite. Both must agree on the same protection suite. If they do not, no common policies may exist and the IKE session may be terminated.

IKE Phase 2: Quick mode of exchange : Uses to negotiate IPSec's SA

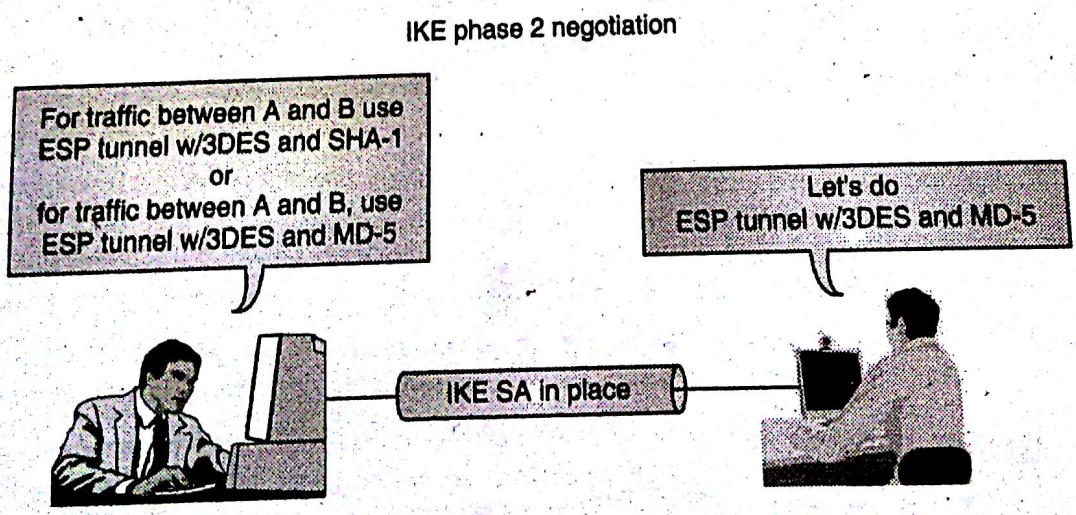


Fig. 11.14

For instance :

As shown in Fig.11.14 user A and user B wish to protect the traffic with IPSec and the IKE SA is already established between them. User A proposes various IPSec security policies and user B chooses one of them (with highest priority according to configuration). After successful negotiation, keying material is exchanged and IPSec SAs are established to protect network traffic.

Q. 10 Explain SET Protocol.

Ans. :

SET stands for Secure Electronic Transaction. It is an encryption & and security specification protocol designed to protect credit card transactions over an insecure channel such as Internet. SET is no payment system it is set of rules & regulations designed to protect credit card payments of users, employee over an open network such as Internet in a secure way. SET was developed in 1996 by VISA and MasterCard, with participation from different leading technology companies, which includes Microsoft, IBM, Netscape, RSA, Terisa Systems and VeriSign. After testing o f the SET in 1998 it declares as a standard for safeguarding credit card purchases made over open networks & made it available to users with following requirements.

SET create a secure communications channel among all parties involved in a transaction. SET provides privacy because the information is only available to sender, receiver & bank or the communication parties' involved in transaction. SET provides confidentially, only sender and his intended receiver should be able to access the contents of a message. It assures to card holder is that is safe and accessible only to the intended recipient. SET provides integrity of the message. Integrity gives assurance that data received exactly as sent by an authorized entity. (No alteration, no modification, no deletion and no intersection etc.).

Q. 11 What are SET participants ?

Ans. :

Following are the components of the Secure Electronic Transaction (SET) which involves in the electronic payment as shown in Fig. 11.15.

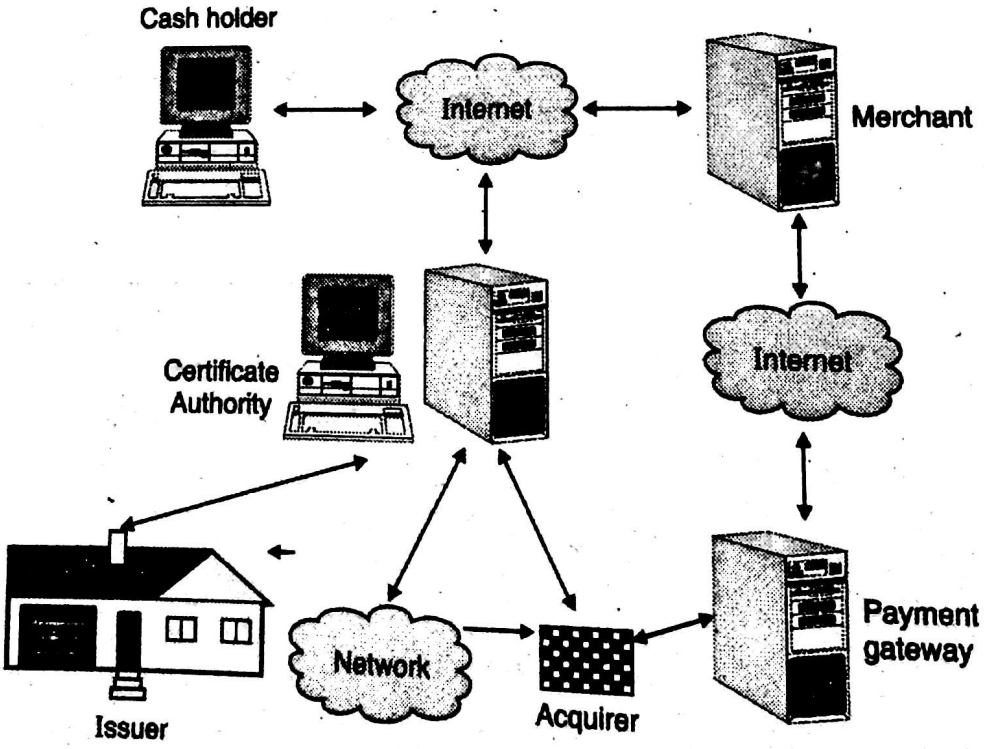


Fig. 11.15

The cardholder :Called as buyer in the transaction who initiates the transaction.

The merchant :Also called seller of goods and services which maintains an account with a bank or acquirer.

The acquirer :Also known as bank or financial institution. The financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

The issuing bank:Bank that maintains the account of the buyer and issues a credit card to the buyer and also sets limit on the amount of purchases.

Certification Authority (CA): Certification Authority (CA) is a trusted unit that helps to issue certificates. A CA takes the certificate request from owner, verifies the requested information according to the terms and conditions of the CA, and uses its private key to apply digital signature to the certificate.

Responsibility of the CA is to identify the correct identity of the person who asks for a certificate to be issued, and make sure that the information contained within the certificate is legal and later digitally sign on certificate.

This is an entity that is trusted to issue X509v3 public-key certificates for cardholders, merchants, and payment gateways.

Payment gateways: It is designated third party that processes merchant payment messages. The merchant exchanges Secure Electronic Transaction messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

Following are the steps of interactions used in SET protocol :

1. **The customer opens the account** :Once the customer obtains a credit card account, such as Master Card or Visa, from the bank which supports electronic payment and Secure Electronic Transaction then customer may proceed for future communication over network.
2. **The customer receives a certificate** :After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank which verifies the customers RSA public key & its expiration date.
3. **Merchants have their own certificates** :A merchant have two public keys one for signing message & another for key exchange The merchant also needs a copy of the payment gateway's public-key certificate.
4. **The customer places an order** : Here customer first browsing through the merchant's Web site to select items and determine the price. The customer now sends its list of items to be purchased to the merchant. Upon receiving list of items from customer merchant returns an order from containing the list of items, their price, a total price, and an order number to the customer.
5. **The merchant is verified** :Along with order number, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid merchant store.
6. **The order and payment is verified** :The customer sends both order and payment information to the merchant, along with the customer's certificate (approved by CA). Customer also confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.
7. **The merchant requests payment authorization** :The merchant sends the payment information to the payment gateway for authentication as well as to check whether customer's available credit is sufficient for this purchase.
8. **The merchant confirm the order** :Upon receiving payment confirmation from customers credit, the merchant sends confirmation of the order to the customer.

9. **The merchant provides the goods or service.** After all verification the merchant provides the goods or service to the customer.
10. **The merchant request payment.** This request is sent to the payment gateway, which handles all of the payment processing.

❑❑❑

Chapter 12 : Non-Cryptographic Protocol Vulnerabilities Phishing

Q. 1 Write short note on phishing attack.

Ans. :

It is an attempt to acquire password credit essential financial data by sending fake email, messages, electronically. There are treated as spam mails. These mails ask for some confidential data by grabbing trust of the user. Phishing mail generally in form of trustworthy email. These are a usually carried out by e-mail spoofing. It is an example of social engineering.

Types of Phishing Attack

1. **Deceptive phishing :**

   Sending bulk of email messages, which make user to click any one of the bulk email such type of attack called as deceptive phishing.

2. **Malware based phishing :**

   Running malicious software on target's or users machine. There malware comes from the email attachments.

3. **Key loggers and screen loggers :**

   These malware track input from keyboard and send information of target through target's keyboard to hacker (attacker) via internet.

4. **Session hijacking :**

   User activities are monitored to get login into the user's system.

5. **Web trojans:**

   They are a kind of pop-ups, when logging into some website. These pop ups usually asks for user's credentials.

6. **System reconfiguration attacks :**

   It is kind of phishing attack where user's PC setting are modified or changed.

7. **DNS based phishing :**

   In this type of phishing the URL requested return to some bogus or fake site which is actually sent by hacker by changing the URL of the requested site of the user.

8. **Content injection phishing :**

   It is an act of inserting some malicious content in the websites which can redirect to some other website or may install malware.

Q. 2 Explain the working of phishing.

Ans. :

Phishing work in following ways :

1. **Planning :**

   The first step is to decide the target and plan how to get through the target's mail. This is generally done using mass mailing.

2. **Setup :**

   Once phisher comes to know whom to spoof or attack using email, they will start creating and delivering message to collect data about the target.

3. **Attack :**

   The phisher starts sending messages, email, which appears to be from a reputed organization.

4. **Collection :**

   Phishers collect the information, that victim enters in the web pages or emails or popup windows which are created by attacker.

5. **Identity theft and forward**

   After gathering information they start misusing information for illegal use.

Q. 3 What is denial of service attack ? Dec. 2012, May 2013

Ans. :

Denial of service and distributed denial of services is a type of attack that causes legitimate users unable to use services or the resource, or services become unavailable to the legitimate users.

Q. 4 What are the way in which on attack can mount a DOS attack on the system ?

Dec. 2012, May 2013

Ans. :

In this attack, the attacker keeps on sending or makes the network or bandwidth overflow by e-mails or spam mail by depriving the victim to access services. It is a continuous effort of attackers to make victim unable to use any internet service or resources. The attacker's main target for websites or services which include financial site bank site or credit card gateway systems.

The targeted network which are root for DOS are mobile phone network or credit card gateway network. Buffer overflow technique is used to make denial service attack. What an attackers does is it takes packet (where is a unit of data) divide into small chunks, the attacker checks for the IP address of the particular network in that packet and floods the network of victim with repeated request. As IP is a fake, from attacker's machine. This acts consumes bandwidth which let other service to fail or unavailable for other user.

A DOS attack do following actions :

1. Flood whole network with unnecessary traffic.

2. Damage connection between two systems so that communication cannot occur.
3. Disrupt services to legitimate users.
4. Prevents individuals to access network services.

Classification of attacks :

(1) Bandwidth attack :

Every website is given particular amount of bandwidth to host (e.g. 50 GB) loading of any websites takes certain amount of time to display whole webpage.

If more visitors load particular websites page or consumes whole 50 GB bandwidth than particular websites can be ban.

The attacker does the same by opening 100 pages of site and keeps on loading and refreshing .Consuming all bandwidths to make the site out of services.

(2) Logic attack :

Attack on the network software to make it vulnerable.

For example : in TCP/IP stack.

(3) Protocol attacks :

This attack, consumes more amount of resources in victims system. It is an attack on the particular features of some protocol that are been installed in the victims systems.

(4) Unintentional Dos attack

Sometimes because of huge popularity among users the particular wets suddenly end up.

Q. 5 What are types of DOS attacks ?

Ans. :

(1) Flood attack :

Attacker keeps on flooding or overloading victim's system with 'n' numbers of ping packets which result into huge traffic which the victim itself cannot handle. It is very simple to launch but difficult handle.

(2) Ping of Death attack :

Sending huge ICMP packet (These packets are used in IP layer or network layer for indicating error message). The attacker sends this huge oversize packet to the victim's system which causes victim's system to crash or freeze resulting in DOS.

(3) SYN attack :

It is a TCP SYN flooding attack, a denial of service attack. In TCP handshaking of network connection is done between sender and receiver through synchronous (SYN) and acknowledgement (ACK) messages. An attacker initiates a TCP connection with server with a SYN message. The server in reply sends an acknowledgement message. (SYN – ACK) message.

The client (attacker) does not respond back with acknowledgement which causes server to wait .Due to which it is unable to connect with other client. This fills up the buffer space for SYN message preventing other for communicate.

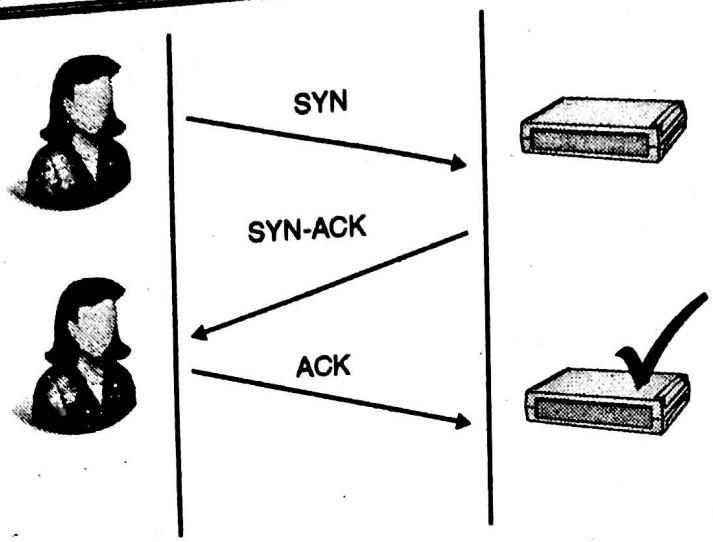


Fig. 12. 1: 3 way handshake

1. Clients sends synchronize (SYN) packet to server.
2. Servers send syn-ack (SYN – ACK) to client.
3. Clients responds back with ACK packet and connect is established client as shown in Fig. 12.1.

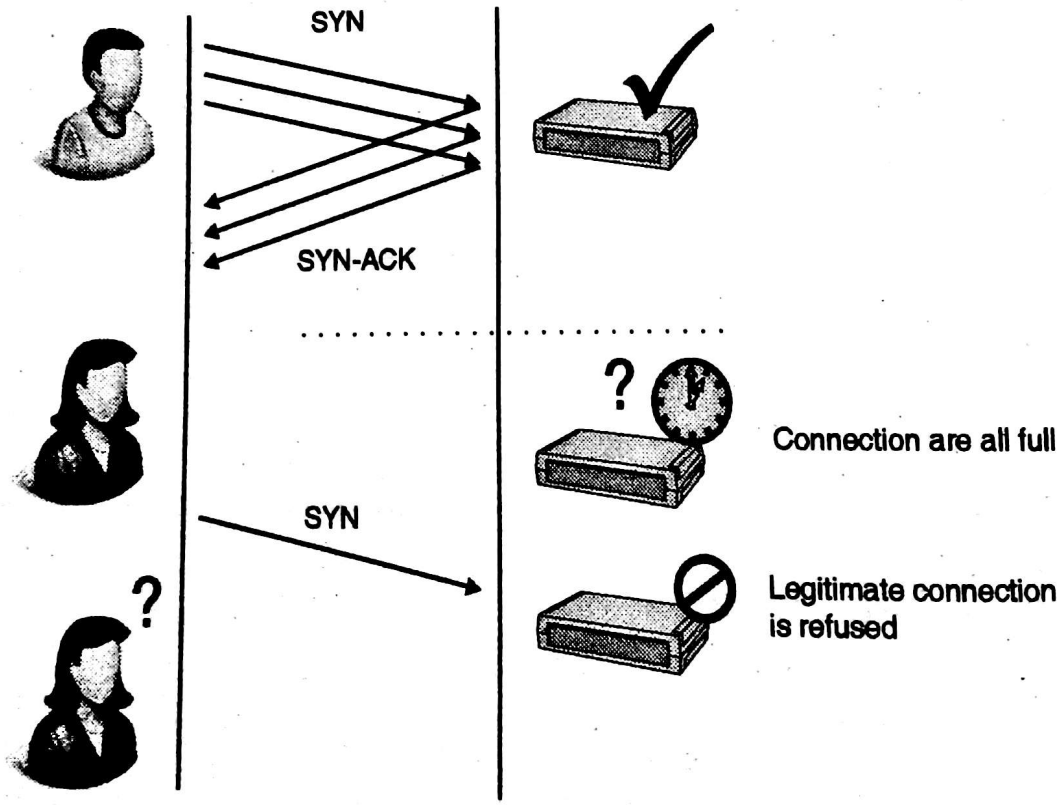


Fig. 12. 2 : Chaotic handshake

1. Client sends multiple SYN packets to all with bad address.
2. **Server send SYN :** ACK packets to in correct address.
3. Legitimate user is denied because server cannot accept additional connection as shown in Fig. 12.2.

4. **Teardrop attack :** It is an attack when packets are overlapped with each other and the receiver is not able to reassemble them, usually corrupted packets are send by attacker to hang or freeze the system.

5. **Nuke :** It is an attack of sending invalid ICMP packet to the target which slow down the affected computer till it is completely stop.

6. **Smurf attack :**It is an attack in which IP address broad casting is done. A Smurf program is used to make network inoperable. It builds a packet which seems to originate from another address. This packet contains ICMP ping. The echo responses are sent back to victim. Maximum ping and echo make network unusable.

The various tools used for DOS attack or Jolt2, Nemesy, Targa etc.

Q. 6 What are the way in which on attack can mount a DDOS attack on the system ? Dec. 2012

Ans. :

Distributed denial of service, it is where an attacker uses your own computer to attack on another computer. It takes advantage of loopholes and security vulnerability to take control on for computer to send vulnerability spam or send huge data to other computers. The systems which are used for attacking victim computer are called as Zombie systems. Various tools to launch DDOS attack are Trinoo, Tribe flood, shaft etc.

Measures to protect from DOS/DDOS attack are :

Implementing filters on routers. Disable unused network services. Examine the physical security routinely. Maintain regular backup schedules and policies. Maintain password policies. Using fault tolerant network configuration. Tools for detecting DOS/DDOS attacks Zombie Zapper, find – DDOS, remote intrusion detector (RID).

Q. 7 Explain methods used to commit session hijack. Dec. 2012 , May 2014

Ans. :

In session hijacking, the hacker takes over the control over the TCP session between two machines whereas in spoofing the attacker pretends to be the authenticate user and gain access to other machine.

Steps in session hijacking :

(i) Sniff the network, by placing itself between victim and target's network.

(ii) Monitor the packet flow between two machines.

(iii) Predict the SYN sequence number.

(iv) Kill the connection to the victim's machine.

(v) Take over the session.

(vi) Start injecting packets to the target server.

Types of Session Hijacking

1. **Active :** In active attack ,attacker finds the active session and takes over.

2. **Passive :** With passive attack, an attacker hijacks a session observes and analyses the session.

Session Hijacking Levels

1. **Network level :** It can be defined as the interception of the packets during transmission between client and server in a TCP and UDP session. It is particularly attractive to hackers providing critical information to the attacker which is used to attack application level session.

   Ex. :TCP/IP session hijacking

   IP Spoofing

   Packet Sniffer (Man-in middle attack)

2. **Application level :**It is about gaining control on HTTP user session by obtaining session's id, after gaining control it creates a new unauthorized access.

   Ex. : Sniffing

   Brute Force attack

   Misdirect trust.

   Various tools of session hijacking are :Wireshark, Juggernaut, IP watcher etc.

Session Hijacking : Detection

It can be detected in two ways:

1. **Manual method :**by using packet sniffing software.
2. **Automatic method :** Using IDS(Intrusion Detection system) and IPS(Intrusion Prevention System)

Session Hijacking : Prevention

It can be prevented if proper encryption is done, antivirus software is used and proper secure connection is established.

Q. 8 What is mean by buffer overflow ?

Ans. :

It is also known as buffer overrun. It deviates from a standard, where the process stores data in buffer overruns the buffer's boundary and overwrites adjacent memory locations. Buffer overflow can be triggered by inputs that are designed to execute code or alter the way the program operates. Bound check can prevent buffer overflow.

The languages which are commonly associated with buffer overflow are : C and C++, as it provides no built in protection against accessing or overwriting data in any part of memory. Buffer overflow occur when a process tries to store data in buffer then it was intended to hold.

Q. 9 What are types of buffer overflow ?

Ans. :

1. **Stack based buffer overflow :** When program writes in memory address, on program's call stack outside the intended data structure, then stack overflow occurs. The condition where Buffer being overwritten is allocated on the stack (i.e., is a local variable or a parameter to a function).
2. **NOP (No Operation) :**It is an assembly language instruction command that effectively does nothing at all. NOP enables developer to force memory alignment to act as a place holder to be

replaced by active instruction later on in program development. NOP opcode can be used to form an NOP slide, which allows code to execute when exact value of instruction pointer is indeterminate. Fig. 12.3 shows NOP operation.

3. **Heap buffer overflow :** In Buffer overflow ,the overflow occurs when an application copies more data into buffer then the buffer was designed to contain. The heap space is dynamically allocated by new(),malloc(),calloc() dynamically allocated in runtime.

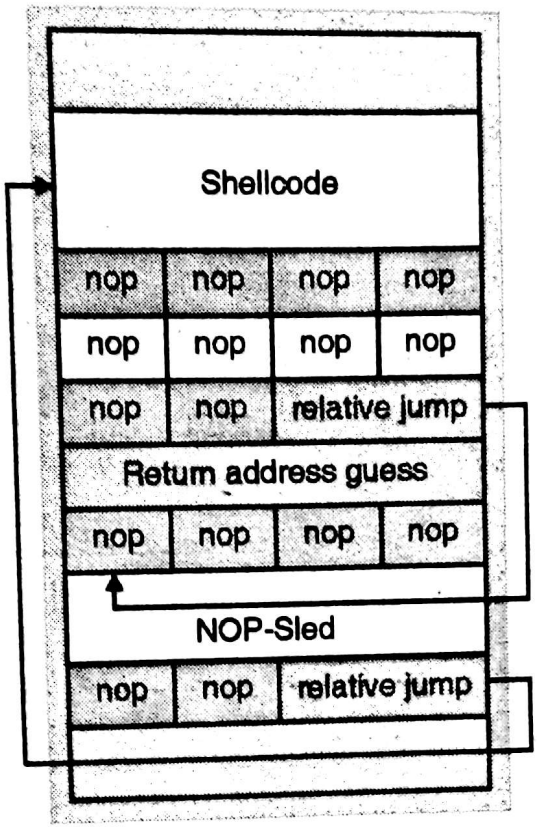


Fig. 12.3 : NOP operation

Q. 10 What is SQL injection ? Give example. Dec. 2012, Dec. 2014

Ans. :

It is a source code injection technique in which malicious SQL statements are inserted into entry field of database to dump data base content. Attacker targets the database organization where confidential data is stored.

Its main focus is to get information from the database server stored in database table by sending malicious query since database can be accessible by query.

When legitimate user enters an additional database via web form, the attacker sends its own command through same web form field. The attackers before proceeding always checks whether organization's database has any loop is it vulnerable or not.

Steps for SQL injection :

(1) The attacker looks for login pages search pages or feedback pages or pages that display HTML commands like POST or GET.

(2) Attacker checks the source code of the web page by right click on web page and view source.

(3) It checks term <form> tag everything insides <form> tag </form >have potential of getting vulnerabilities.

(4) The attacker puts single quote under the text which accepts username and password. If response is an error message such as "a" = 'a' (something like) then website is vulnerable.

(5) Attacker than uses SQL command such as SELECT to retrieve data or INSERT command to add information to database.

Benefits for attacker using SQL injection :

(1) Obtain basic information about website or organization.

(2) May gain access to database by obtaining username, password from SELECT command FROM command where command.

(3) Can add new data to the database by executing INSERT command.

(4) Can modify data in the database by UPDATE command.

Prevention against SQL injection : .

SQL injection attacks happen because of poor website coding and poor administration of website.

Following steps help to prevent SQL injection attack :

(1) Replace all single quotes to two single quotes.

(2) Check the user input of any character and string that should not be malicious.

(3) Numeric value should also be checked.

(4) If there is SQL error it should be modified immediately but not be displayed to outsiders.

(5) SQL server 2000 which is a default server should never be used.

(6) Both database server and web server be reside in different machine

❑❑❑

Cryptography and System Security

Statistical Analysis

Chapter No.	Dec. 2015	May 2016
Chapter 1	05 Marks	10 Marks
Chapter 2	11 Marks	05 Marks
Chapter 3	15 Marks	–
Chapter 4	20 Marks	05 Marks
Chapter 5	05 Marks	15 Marks
Chapter 6	10 Marks	–
Chapter 7	12 Marks	05 Marks
Chapter 8	05 Marks	05 Marks
Chapter 9	–	05 Marks
Chapter 10	05 Marks	05 Marks
Chapter 11	15 Marks	05 Marks
Chapter 12	22 Marks	10 Marks
Repeated Questions	-	30 Marks

Dec. 2015

Chapter 1 : Introduction [Total Marks - 05]

Q. 1(c) Define the goals of security and specify mechanisms to achieve each goal. **(5 Marks)**

Ans. : **Please refer Q. 5 of Chapter 1.**

Chapter 2 : Basics of Cryptography [Total Marks - 11]

Q. 1(a)(I) Define with examples : Substitution cipher. **(3 Marks)**

Ans. : **Please refer Q. 3 of Chapter 2.**

Q. 1(a)(II) Define with examples : Poly-alphabetic cipher. **(3 Marks)**

Ans. : Polyalphabetic cipher :

Monoalphabetic cipher substitutes one letter of the alphabet with any random letter from the alphabet, but draw back in monoalphabetic is that these are fairly easy to break or this can make the cryptanalysis attacker straight forward to guess the pattern. So to make it more harder to break the concept of polyalphabetic cipher arises it is a way to use **more than one** alphabet and switching between them systematically.

Procedure of polyalphabetic cipher :

1. Pick a keyword (for our example, the keyword will be "MEC").
2. Write your keyword across the top of the text you want to encipher, repeating it as many times as necessary.
3. For each letter, look at the letter of the keyword above it (if it was 'M', then you would go to the row that starts with an 'M'), and find that row in the Vigenere table.

ROW																									
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

4. Then find the column of your plaintext letter (for example, 'w', so the twenty-third column).
5. Finally, trace down that column until you reach the row you found before and write down the letter in the cell where they intersect (in this case, you find an 'T' there).

Example :

Keyword : MECMECMECMECMECMECMECM

Plaintext : weneedmoresuppliesfast

Ciphertext : IIPQIFYSTQWWBTNUIUREUF

Thus, the urgent message "We need more supplies fast!" comes out:

IIPQIFYSTQWWBTNUIUREUF

Q. 2(c) Encrypt "The key is hidden under the door" using Playfair cipher with keyword "domestic". **(5 Marks)**

Ans. : Keyword-domestic :

Keyword is domestic. In the first step all letters are to be filled in that matrix from left to right, the letters which are already been placed is not be placed again in that matrix. After filling up of the given letter, fill rest of the space in the matrix with the remaining letters alphabetically with no repetitions. The letters I and J will be considered as one letter. So If I is already placed then no need to place J in rest of the matrix.

d	o	m	e	s
t	i	c	a	b
f	g	h	k	l
n	p	q	r	u
v	w	x	y	z

By using Playfair cipher (Use following steps to encrypt given word or message) we want to encrypt the plain text message "The key is hidden under the door" using keyword domestic.

1. The plaintext received is to be broken in pair of two letters, if duplicate letter put x
2. Th, ek, ey, is, hi, dx, de, nu, nd, er, th, ed, ox, or
3. If both letters are same or only one letter is left then put X with that alphabet.
4. If both pair alphabet appear in same row replace the letter with the immediate right alphabet (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
5. If both letters appear in same column replace it with alphabet immediate below to that letter (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
6. If none of the condition explained above meet, then replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.
7. Refer above matrix for the same.

th → Step 6 → cf
ek → Step 5 → ar
ey → Step 5 → ae
is → Step 6→ bo
hi → Step 6 → gc
dx → Step 6 → mv
de → Step 4 → os
nu → Step 4 → pn
nd → Step 5 → vt
er → Step 5 → ay
th → Step 6 → cf
ed → Step 4 → so
ox → Step 6 → mw
or → Step 6 → ep

The plain text message "The key is hidden under the door" encrypted as :
cf, ar, ae, bo, gc, mv, os, pn, vt, ay, cf, so, mw, ep.

Chapter 3 : Secret Key Cryptography [Total Marks - 15]

Q. 4(a) Explain working of DES detailing the Fiestel structure. **(10 Marks)**

Ans. : Please refer Q. 1 of Chapter 3.

Q. 6(v) Write in brief about : Key generation in IDEA. **(5 Marks)**

Ans. : International Data Encryption Algorithm (IDEA) :

It is a block cipher algorithm designed by Xuejia Lai and James L. Massey of ETH-Zürich in 1991. It is a modified version of Data encryption Standard algorithm. It operates on 64-bit plaintext and ciphertext blocks and key used is of 128 bit. It was used in Pretty Good Privacy PGP v2. Total 8 numbers of rounds are done using 6 keys in each round. Like this 48 keys are there and in last round another 4 keys (6*8= 48 + 4=52) are used for both encryption and decryption. The operations performed in this process are i)XOR ii) Addition iii) Multiplication

1. Key generation process :

The 128 bit keys are divided into 8 sub parts i.e. 16 bit in each subpart. Then this 128 bit key is cyclic shifted to the left by 25 positions and generates a new 128 bit key. Similarly this 128 bit key is divided into 8 sub blocks which will be used in next round. The same process is repeated from which 52 keys are generated. Table 1 show sub blocks of key generation.

Table 1 : Encryption of the key sub-blocks

Round 1	$Z_1^{(1)}\ Z_2^{(1)}\ Z_3^{(1)}\ Z_4^{(1)}\ Z_5^{(1)}\ Z_6^{(1)}$
Round 2	$Z_1^{(2)}\ Z_2^{(2)}\ Z_3^{(2)}\ Z_4^{(2)}\ Z_5^{(2)}\ Z_6^{(2)}$
Round 3	$Z_1^{(3)}\ Z_2^{(3)}\ Z_3^{(3)}\ Z_4^{(3)}\ Z_5^{(3)}\ Z_6^{(3)}$
Round 4	$Z_1^{(4)}\ Z_2^{(4)}\ Z_3^{(4)}\ Z_4^{(4)}\ Z_5^{(4)}\ Z_6^{(4)}$
Round 5	$Z_1^{(5)}\ Z_2^{(5)}\ Z_3^{(5)}\ Z_4^{(5)}\ Z_5^{(5)}\ Z_6^{(5)}$
Round 6	$Z_1^{(6)}\ Z_2^{(6)}\ Z_3^{(6)}\ Z_4^{(6)}\ Z_5^{(6)}\ Z_6^{(6)}$
Round 7	$Z_1^{(7)}\ Z_2^{(7)}\ Z_3^{(7)}\ Z_4^{(7)}\ Z_5^{(7)}\ Z_6^{(7)}$
Round 8	$Z_1^{(8)}\ Z_2^{(8)}\ Z_3^{(8)}\ Z_4^{(8)}\ Z_5^{(8)}\ Z_6^{(8)}$
Output Transform	$Z_1^{(9)}\ Z_2^{(9)}\ Z_3^{(9)}\ Z_4^{(9)}$

2. Encryption :

The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in Fig. 1-Q. 6(v).

The first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$. The results are then processed, where two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order.

The process described above for round one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 216 and multiplication modulo 216 + 1 to form the resulting four 16-bit ciphertext blocks.

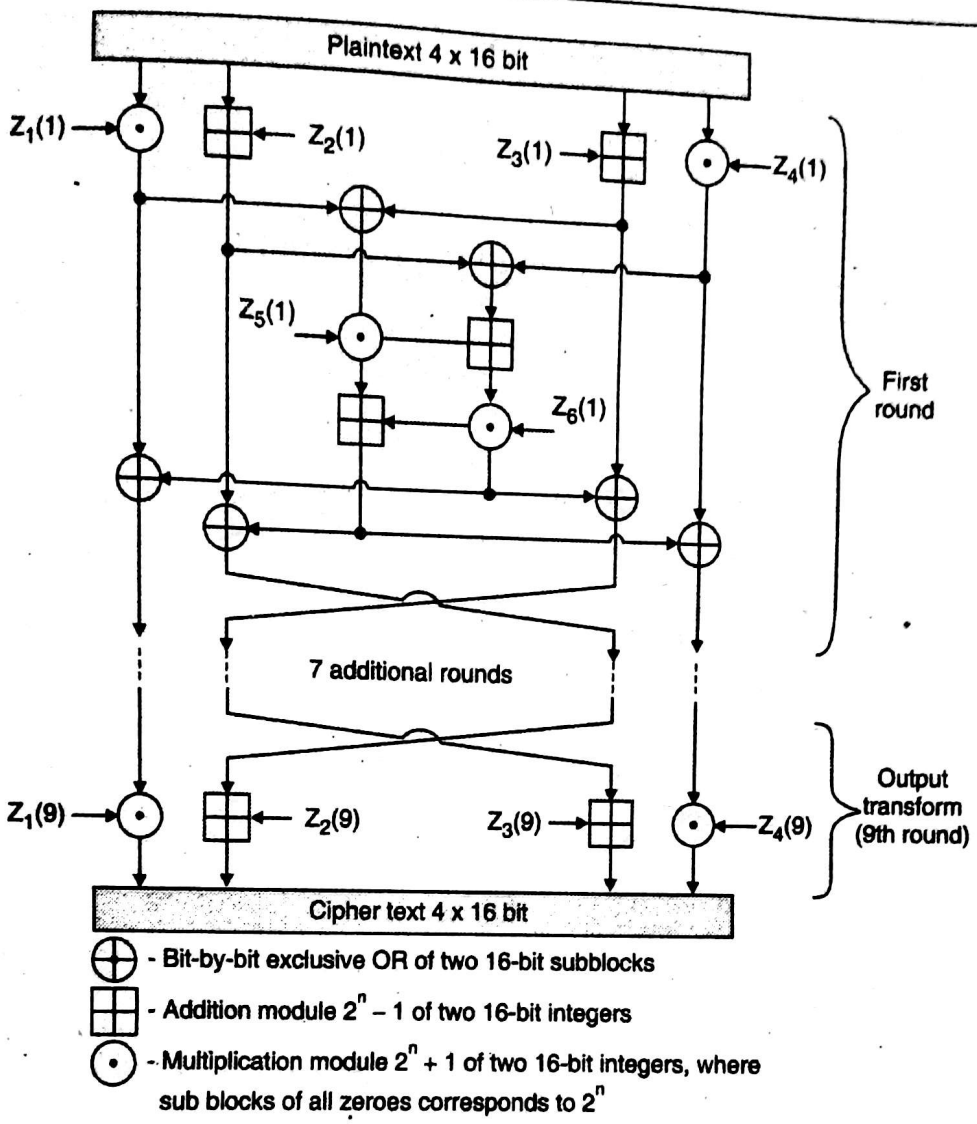


Fig. 1-Q. 6(v) : The IDEA structure

3. Decryption :

Table 2 : Decryption of the key sub-blocks

Round 1	$Z_1^{(9)-1}\ Z_2^{(9)}\ Z_3^{(9)}\ Z_4^{(9)-1}\ Z_5^{(9)}\ Z_6^{(9)}$
Round 2	$Z_1^{(8)-1}\ Z_2^{(8)}\ Z_3^{(8)}\ Z_4^{(8)-1}\ Z_5^{(8)}\ Z_6^{(8)}$
Round 3	$Z_1^{(7)-1}\ Z_2^{(7)}\ Z_3^{(7)}\ Z_4^{(7)-1}\ Z_5^{(7)}\ Z_6^{(7)}$
Round 4	$Z_1^{(6)-1}\ Z_2^{(6)}\ Z_3^{(6)}\ Z_4^{(6)-1}\ Z_5^{(6)}\ Z_6^{(6)}$
Round 5	$Z_1^{(5)-1}\ Z_2^{(5)}\ Z_3^{(5)}\ Z_4^{(5)-1}\ Z_5^{(5)}\ Z_6^{(5)}$
Round 6	$Z_1^{(4)-1}\ Z_2^{(4)}\ Z_3^{(4)}\ Z_4^{(4)-1}\ Z_5^{(4)}\ Z_6^{(4)}$
Round 7	$Z_1^{(3)-1}\ Z_2^{(3)}\ Z_3^{(3)}\ Z_4^{(3)-1}\ Z_5^{(3)}\ Z_6^{(3)}$
Round 8	$Z_1^{(2)-1}\ Z_2^{(2)}\ Z_3^{(2)}\ Z_4^{(2)-1}\ Z_5^{(2)}\ Z_6^{(2)}$
Output Transform	$Z_1^{(1)-1}\ Z_2^{(1)}\ Z_3^{(1)}\ Z_4^{(1)-1}$

The computational process used for decryption of the ciphertext is essentially the same as in encryption process. Here only 16 bit key sub blocks are generated during decryption. Each of the 52, 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption. The key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process as shown in Table 2.

Chapter 4 : Public Key Cryptography [Total Marks - 20]

Q. 2(a) In an RSA system the public key (e,n) of user A is defined as (7,119). Calculate ϕ_n and private key d. What is the cipher text when you encrypt message m = 10, using the public key ? **(10 Marks)**

Ans. :

By using RSA algorithm :

In the problem statement Public key (e,n) = (7,119) is given, means we don't need to select e & n. if we select following prime numbers which results n = 119 as shown below.

Step 1 : Prime numbers are 7 and 17 a = 7, b = 17

Step 2 : $n = a * b = 7 * 17 = 119$.

Step 3 : $\phi(n) = (a - 1) * (b - 1) = (7 - 1) * (17 - 1) = 6 * 16 = 96$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ(n)) = 1
e = 7 as per problem statement.

Step 5 : Calculate d such that

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

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

$$7 * d \bmod 96 = 1$$

Using RSA algorithm

$$d = ((\phi(n) * i) + 1)/7 \text{ where } i = 1 \text{ to } 100 = \mathbf{(96*1 + 1)/7 = 13.85}$$

d must be completely divisible by 'e'.

$$= \mathbf{((96*2) + 1)/7} = 21.57 = \mathbf{((96*3) + 1)/7} = 48.28 = \mathbf{((96*4) + 1)/7} = 55$$

$$\mathbf{d = 55}$$

Step 6 : Public key = {e, n} = {7, 119}
Private key = {d, n} = {55, 119}

Step 7 : Calculate cipher text message for given plain text message m = 10.
Plain text denoted as p = 10 (m denoted as p)

$$C = P^e \bmod n = 10^7 \bmod 119 = 10000000 \bmod 119$$

$$C = 73$$

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 40 to the receiver then receiver can calculate plain text p.

$$P = C^d \bmod n = 73^{55} \bmod 119$$

Now represent $40^{55} \bmod 119$ as mention above it will results p as 10.
Because decryption process always yields original message / plain text

$$\therefore \quad P = 73^{55} \bmod 119 = 10$$

$$\mathbf{P = 10}$$

There are four possible attacks on RSA as follows,

1. **Brute force attack :** Hacker tries all possible private keys.
2. **Mathematical attacks :** Hackers attacks on n i.e. tries to factorize the product of two prime numbers.
3. **Timing attacks :** It totally depends on running time of decryption algorithm.
4. **Chosen Cipher text attack :** Hacker tries to attack on the properties of RSA algorithm.

Q. 3(a) Explain how a key is shared between two parties using Diffie Hellman key exchange algorithm. What is the drawback of this algorithm? **(10 Marks)**

Ans. : **Please refer Q. 5 of Chapter 4.**

Chapter 5 : Cryptographic Hash Functions [Total Marks - 05]

Q. 3(b)(i) Differentiate between : MD-5 and SHA. **(5 Marks)**

Ans. : **Please refer Q. 4 of Chapter 5.**

Chapter 6 : Authentication Applications [Total Marks - 10]

Q. 2(b) Give the format of X 509 digital certificate and explain the use of a digital signature in it. **(5 Marks)**

Ans. :

Public key certificate/ digital certificate :

Digital certificate is an electronic file that is used to identify people and resources over a insecure channel or a networks called Internet. Digital certificate also enable secure, confidential communication between sender and receiver using encryption. For example when we travel to another country, our passport provides a way to establish our identity and gain entry. Digital certificate provide similar identification in the electronic world. The role of Certification Authority (CA) is to issue certificates with authorized digital signature. Much like the role of the passport office, the role of the CA is to validate the certificate owner's identity and to "sign" the certificate so that it cannot be tampered by unauthorized user. Once a CA has signed a certificate, the owner can present their certificate to people, web sites and network resources to prove their identity for confidential communications over insecure channel.

A standard called as **X.509** defines structure of digital certificate. The International Telecommunication Union (ITU) permitted this standard in 1998. Fig. 1-Q. 2(b) shows structure of X.509 digital certificate. A standard digital certificate typically includes a variety of information pertaining to its owner and to the Certification Authority (a trusted agency that can issue digital certificate) such as :

1. **Certificate version number :** Identifies a particular version of the X.509. Current version is X.509 v3.
2. **Certificate serial number :** Unique integer number generated by certification authority.
3. **Algorithm for signature identifier :** Identifies algorithm used by the certification authority to sign the certificate.
4. **Certificate issuer name :** The name of the Certification Authority that issued the certificate.
5. **Validity Details :** The validity period (or lifetime) of the certificate (a start and an end date).

Digital Certificate contents
Certificate version number
Certificate serial number
Algorithm for signature identifier
Certificate Issuer name
Validity Details
Name of the certificate owner Public key of certificate owner
Issuer unique identifier
Owner unique identifier
Extensions to certificate
Certification Authority (CA) Digital Signature

Fig. 1-Q. 2(b) : Structure of X.509 Digital certificate

6. **Name of the certificate owner :** The name of the owner and other identification information required for identifying the owner such as email id and contact details.
7. **Public key of certificate owner :** Certificate owner's public key, which is used to encrypt confidential information of the certificate owner.
8. **Issuer unique identifier :** Indentify the CA uniquely i.e. whether single CA signed it or is any CA using same details.
9. **Owner unique identifier :** Indentify the owner uniquely if two or more owner has used the same name over a time.
10. **Extensions to certificate :** This is an optional field which allows a CA to add additional private information to a certificate. These additional fields are called as extensions of version 2 or 3, respectively.
11. **Certification Authority (CA) Digital Signature :** In creating the certificate, this information is digitally signed by the issuing CA. The CA's signature on the certificate is like a tamper-detection seal on packaging any tampering with the contents is easily detected.

Q. 5(b) How does PGP achieve confidentiality and authentication in emails ? **(5 Marks)**

Ans. : Electronic mail security : pretty good privacy :

1. PGP Authentication :

1. Ramesh has (private/public) key pair *(Rd/Re)* and he wants to send a digitally signed message *m* to Suresh.
2. Ramesh hashes the message using SHA-1 to obtain *SHA(m).*
3. Ramesh encrypts the hash using his private key *Rd* to obtain ciphertext *c* given by

$$c = \text{encrypt}_{Rd}(\text{SHA}(m))$$

4. Ramesh sends the pair *(m,c)to Suresh*
5. Suresh receives *(m,c)* and decrypts *c* using Ramesh's public key *Rd* to obtain signature *S*

$$S = \text{decrypt}_{Rd}(c)$$

6. He computes the hash of *m* using SHA-1 and if this hash value is equal to S then the message is authenticated.

Suresh is sure that the message is correct and that is does come from Ramesh. Furthermore Ramesh cannot later deny sending the message since only Ramesh has access to his private key *Rd* which works with respective public key *Rd.*

2. **PGP confidentiality :**

1. Ramesh wishes to send Suresh a confidential message *m*.
2. Ramesh generates a random session key *k* for a symmetric cryptosystem.
3. Ramesh encrypts *k* using Suresh's public key *Be* to get
$$k' = encrypt_{Be}(k)$$
4. Ramesh encrypts the message *m* with the session key *k* to get ciphertext *c*
$$c = encrypt_{k}(m)$$
5. Ramesh sends Suresh the values *(k',c)*
6. Suresh receives the values *(k',c)* and decrypts *k'* using his private key B_d to obtain *k*.
$$k = decrypt_{Bd}(k')$$
7. Suresh uses the session key *k* to decrypt the ciphertext *c* and recover the message *m*
$$m = decrypt_{k}(c)$$

Public and symmetric key cryptosystems are combined in this way to provide security for key exchange and then efficiency for encryption. The session key *k* is used only to encrypt message *m* and is not stored for any length of time.

3. **PGP authentication and confidentiality :**

The schemes for authentication and confidentiality can be combined so that Ramesh can sign a confidential message which is encrypted before transmission. The steps required are as follows :

1. Ramesh generates a signature *c* for his message *m* as in the Authentication scheme
$$c = encrypt_{Rd}(SHA(m))$$
2. Ramesh generates a random session key *k* and encrypts the message *m* and the signature *c* using a symmetric cryptosystem to obtain ciphertext *C*
$$C = encrypt_{k}(m,c)$$
3. He encrypts the session key *k* using Bob's public key
$$k' = encrypt_{Be}(k)$$
4. Ramesh sends Suresh the values *(k',C)*
5. Suresh recieves *k'* and *C* and decrypts *k'* using his private key *Bd* to obtain the session key *k*
$$k = decrypt_{Bd}(k')$$
6. Suresh decrypts the ciphertext *C* using the session key *k* to obtain *m* and *c*
$$(m, c) = decrypt_{k}(C)$$
7. Suresh now has the message *m*. In order to authenticate it he uses Ramesh public key Re to decrypt the signature *c* and hashes the message *m* using SHA-1.
$$If \quad SHA(m) = decrypt_{Re}(c)$$

Then the message is authenticated.

Chapter 7 : Program Security [Total Marks - 12]

Q. 1(a)(iii) Define with examples : Salami attack. **(2 Marks)**

Ans. : It is series of small attacks which results in large attack. It works on "collect and roundoff" trick. It is a fraudulent practice of stealing money repeatedly. It takes advantage of rounding operation in financial transactions. It always rounds down and thus the fractions of amount remained will be transfered into some another account. Thus the transaction will go undetected. Such type of attacks can be easily automated.

Q. 1(b) With the help of examples explain non-malicious programming errors. **(5 Marks)**

Ans. : Please refer Q. 1 ,Q. 2 and Q. 3 of Chapter 1.

Q. 6(iv) Write in brief about : Viruses and their types. **(5 Marks)**

Ans. : Types of virus :

(1) **Boot sector viruses :** It infects the storage media like dislects and hard drives. All disks or hard serves contain sector and the first sector is called as Boot Sector. This boot carries Master Boot Record which is used to read and load operating system. The virus infect itself sector while rebooting system Boot sector also spreads other computers if same disk is shared to other system.

(2) **Program virus :** A program virus gets active when program containing these virus gets opened (.bin, .exe, .ove), once if gets open it starts copying itself and infect other program.

(3) **Multipartite virus :** It is combination/hybrid of boot sector and program virus. It infects the program files. When this virus is active it will affect boot sector also after booting or starting up it will affect other computer also.

(4) Stealth virus : "Dubbed Brain" the first computer virus was a stealth virus it tries to disguise itself, so that antivirus software may not able to recognize it. It alters the file size, concealing file's memory and so on.

(5) **Polymorphic virus :** It keeps on changing it patterns or signature to get undetected. Usually it acts like a 'chamleon'. These are not actual virus, it is a virus which hides actual virus of the system.

(6) **Macro virus :** Applications such as MS word, excel sheets has macro supportive language. These virus infects victim every documents once it get into victims systems.

(7) **Active X and Java control :** All web browser need java control active X enable to function properly. Awareness is needed about managing and controlling settings of browser to check for enabling or disabling popups, downloading files and sounds, since these can invite virus which can affect computer by downloading unwanted software.

Chapter 8 : Operating System Security [Total Marks - 05]

Q. 6(I) Write in brief about : Operating System Security. **(5 Marks)**

Ans. :

Operating system security :

Memory and address protection :

Due to memory protection the process can access the memory which is allocated to it only. It cannot access the memory which is not allocated to it. Thus it prevents spreading of bugs or malwares in other areas of operating system. Following are the techniques for memory and address protection,

1. Fixed and variable Fence
2. Base / Bound
3. Segmentation
4. Paging
5. Paged Segmentation

File protection mechanism : In multiuser operating systems users must be protected from each other so that they will not be able to modify each other's files. Following are the ways for providing security in multiuser operating systems :

All-None System (ANS) : In earlier IBM operating system all the files were by default public. So any user could have access to any other users files. But certain files in the system are very important and it must be locked with passwords by an administrator. However to provide access rights

administrator passwords are required which again limits access to that files. All none system thus provides either full access or no access. But this approach is unacceptable due to following reasons,

Lack of trust : Every time it is not possible to trust other users. It is assumed that all the users are using system with good intension. But this assumption is not justified anywhere.

Too course : It is hard to provide selective rights to selective users.

Rise of sharing : Due to time sharing concept users always interacts with each other.

Complexity : Every time human intervention is required.

File listings : File lists are maintained for users. But interactive user may browse other files also.

Group protection : Due to so many drawbacks of All None system a new modified approach is introduced where groups of authorized users are created. Then access is given to these authorized users groups. This scheme also has following disadvantages,

Group affiliation : One member cannot be a member of two groups. i.e. one person one group.

Multiple personalities : A single person may have two accounts to get involved into two different groups.

All groups :

Limited sharing : Files can be shared to only within groups or to the world.

Single access permissions : Using passwords the single or multiple files can be locked. But again this scheme has drawbacks like forget password, attempts to provide a correct password, leaked password etc.

Per object and per user protection : In the groups different objects can be assigned to different users. New users when created their access rights to different objects are also specified also.

User authentication : Authentication is basically performed for two different reasons :

1. To check whether a requesting user is having permission to perform an operation.
2. To perform an audit trial i.e. who performed what operation.

Authorization :

Authorization is the process by which an entity such as a user or a server gets permission to perform a restricted operation.

Following are the commonly used authentication techniques :

1. **Local user authentication :** Verification by the operating system itself. Based on the type of the user different access permissions are given. **Ex :** Administrator, Guest.
2. **Network host authentication :** Verification of remote server in order to check whether it is safe to submit data or not. **Ex :** Digital certificates on the websites.
3. **Remote user authentication :** Verification of a user by some remote servers. **Ex :** User verification by sending username and password.

Chapter 10 : IDS and Firewalls [Total Marks - 05]

Q. 3(b)(ii) Differentiate between : Firewall and IDS. **(5 Marks)**

Ans. : Difference Firewall and Intrusion Detection System :

Sr. No.	Firewall	Intrusion Detection System
1.	A firewall device filters all traffic between intranet and extranet.	Only network intrusion detection system monitors the inside & outside network traffic.
2.	Different types of firewalls are : Packet filtering gateways Stateful inspection firewalls Application proxies	Different types of IDS are : Network based IDS Host based IDS Active & Passive IDS
3.	All network traffic passes through firewall.	All network traffic doesn't passes through IDS. It monitors the malicious activities inside the packet.
4.	Firewall blocks the traffic or packet by using port numbers or using certain policies.	IDS block the packet by using well known signatures or using set of rules.
5.	Traffic increases because of more number of policies set in the firewall. Ultimately it affects on speed of a network.	Increase in network traffic does not affects on the speed of IDS.
6.	Well known firewalls are Sonicwall Symantec, McAfee.	Well known IDS are SNORT & SAX2

Chapter 11 : IP Security [Total Marks - 15]

Q. 5(a) List the functions of the different protocols of SSL. Explain the handshake protocol. **(5 Marks)**

Ans. : Please refer Q. 6 of Chapter 11.

Q. 5(c) Differentiate between the transport mode and tunnel mode of IPSec and explain how authentication and confidentiality are achieved using IPSec. **(10 Marks)**

Ans. : Please refer Q. 1 and Q. 2 of Chapter 11.

Chapter 12 : Non-Cryptographic Protocol Vulnerabilities Phishing [Total Marks - 22]

Q. 1(a)(iv) Define with examples : Session hijacking. **(2 Marks)**

Ans. : Please refer Q. 7 of Chapter 12.

Q. 4(b) What is a Denial of service attack. What are the different ways in which an attacker can mount a DOS attack on a system? **(10 Marks)**

Ans. : Please refer Q. 3, Q. 4 and Q. 5 of Chapter 12.

Q. 6(ii) Write in brief about : Buffer overflow attack. **(5 Marks)**

Ans. : Please refer Q. 8, Q. 9 of Chapter 12.

Q. 6(iii) Write in brief about : IP spoofing. **(5 Marks)**

Ans. :

IP spoofing :

In this attack, attacker establishes a large number of "half-open" connections using IP spoofing. The attacker first sends SYN packets with the spoofed (faked) IP address to the victim in order to establish a connection. The victim creates a record in a data structure and responds with SYN/ACK message to the spoofed IP address, but it never receives the final acknowledgment message ACK for establishing the connection, since the spoofed IP addresses are unreachable or unable to respond to the SYN/ACK messages. Although the record from the data structure is freed after a time out period, the attacker attempts to generate sufficiently large number of "half-open" connections to overflow the data structure that may lead to a segmentation fault or locking up the computer.

In session hijacking, the hacker takes over the control over the TCP session between two machines whereas in spoofing the attacker pretends to be the authenticate user and gain access to other machine.

Steps in session hijacking :

1. Sniff the network, by placing itself between victim and target's network.
2. Monitor the packet flow between two machines.
3. Predict the SYN sequence number.
4. Kill the connection to the victim's machine.
5. Take over the session.
6. Start injecting packets to the target server.

Types of session hijacking :

1. **Active :** In active attack , attacker finds the active session and takes over.
2. **Passive :** With passive attack, an attacker hijacks a session observes and analyses the session.

Session hijacking levels :

1. **Network level :** It can be defined as the interception of the packets during transmission between client and server in a TCP and UDP session. It is particularly attractive to hackers providing critical information to the attacker which is used to attack application level session.

   Ex. : TCP/IP session hijacking

   IP Spoofing

   Packet Sniffer (Man-in middle attack)

2. **Application level :** It is about gaining control on HTTP user session by obtaining session's id, after gaining control it creates a new unauthorized access.

   Ex. : Sniffing

   Brute Force attack

   Misdirect trust.

   Various tools of session hijacking are : Wireshark, Juggernaut, IPwatcher etc.

Session Hijacking : Detection

It can be detected in two ways :

1. **Manual method :** by using packet sniffing software.
2. **Automatic method :** Using IDS(Intrusion Detection system) and IPS(Intrusion Prevention System)

Session Hijacking : Prevention

It can be prevented if proper encryption is done, antivirus software is used and proper secure connection is established.

❑❑❑

May 2016

Chapter 1 : Introduction [Total Marks - 10]

Q. 1(b) List with examples the different mechanisms to achieve security. **(5 Marks)**

Ans. : **Please refer Q. 5 of Chapter 1.**

Q. 3(a) What is access control ? **(5 Marks)**

Ans. : Access control :

Access Control is the ability to limit and control the access to the host systems. It prevents unauthorized use of a resource. The service used to prevent unauthorized use of a resources i.e. complete control over who can access to resources, under what conditions access can occur and what are different accessing methodology.

For example : It controls the access of resources which is to be made available only to legitimate user. Secondly it looks to the conditions of accessing the resource or network and what is allowed to be done to the resources.

Chapter 2 : Basics of Cryptography [Total Marks - 05]

Q. 1(b) Explain with examples, keyed and keyless transposition ciphers. **(5 Marks)**

Ans. : **Please refer Q. 4 of Chapter 2.**

Chapter 3 : Secret Key Cryptography [Total Marks - 15]

Q. 2(b) Explain working of DES. **(10 Marks)**

Ans. : **Please refer Q. 4(a) of Dec. 2015.**

Q. 6(v) Write in brief about : IDEA. **(5 Marks)**

Ans. : **Please refer Q. 6(v) of Dec. 2015.**

Chapter 4 : Public Key Cryptography [Total Marks - 05]

Q. 1(c) Elaborate the steps of key generation using RSA algorithm. **(5 Marks)**

Ans. : **Please refer Q. 2 of Chapter 4.**

Chapter 5 : Cryptographic Hash Functions [Total Marks - 10]

Q. 3(b) What is a digital signature. Explain any digital signature algorithm in detail. **(10 Marks)**

Ans. : **Please refer Q. 5 of Chapter 5.**

Chapter 6 : Authentication Applications [Total Marks - 15]

Q. 4 (b) Explain working of Kerberos. **(10 Marks)**

Ans. : **Please refer Q. 1 of Chapter 6.**

Q. 6(l) Write in brief about : Email security. **(5 Marks)**

Ans. : **Please refer Q. 6 of Chapter 6.**

Chapter 7 : Program Security [Total Marks - 05]

Q. 1(a) Explain software flaws with examples. **(5 Marks)**

Ans. : **Please refer Q. 1, Q. 2 and Q. 3 of Chapter 7.**

Chapter 8 : Operating System Security [Total Marks - 05]

Q. 5(b) What are the various ways for memory and address protection. **(5 Marks)**

Ans. : **Please refer Q. 1 of Chapter 8.**

Chapter 9 : Database Security [Total Marks - 05]

Q. 3(a) How does the Bell La Padula model achieve access control. **(5 Marks)**

Ans. : The Bell-La Padula Model (BLP) :

Bell-La Padula is an extension of the Access Matrix model with classified data. This model has two components, Classification and Set of categories. Bell-La Padula model shows how to use Mandatory Access Control to prevent the Trojan Horse.

Two main properties of this model for a secure system are :

1. **Simple security** means : A subject at a given security level may not read an object at a higher security level (**no read-up**).
2. **Star property** means : A subject at a given security level must not write to any object at a lower security level (**no write-down**).

This model guarantees secrecy by preventing unauthorized release of information.

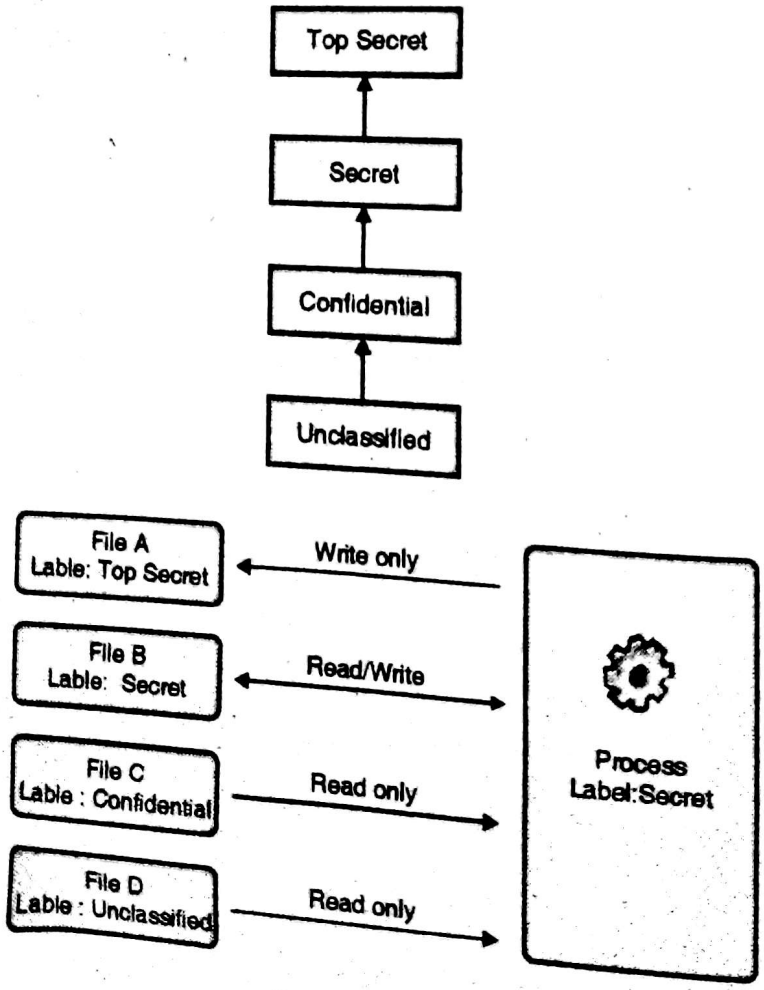


Fig. 1-Q. 3(a)

Appropriate access rights and permissions must be granted to individuals before they can see classified information. Confidential information can be seen by those who have permission to see it. They are not trusted to see Secret or Top Secret information. Data flow operates from lower levels to higher levels. It will never be the reverse as shown in Fig. 1-Q. 3(a). Even if someone has all the necessary official approvals (such as a security clearance) to access certain information they should not be given access to such information unless they have a need to know that is, unless access to the specific information necessary for the conduct of one's official duties. Bell-LaPadula is a simple linear model. Access levels can be defined and thus information flow can be controlled as shown in figure 1-Q. 3(a). All the security levels of objects are static. Because of this restrictions at different levels certain operations are outside the context of protection system becomes very difficult to perform.

Chapter 10 : IDS and Firewalls [Total Marks - 15]

Q. 5(c) Explain the significance of an intrusion detection system for securing a network. Compare signature based and anomaly based IDS. **(10 Marks)**

Ans. : **Please refer Q. 3(b) of Dec. 2015.**

Q. 5(a) What is a firewall? What are the firewall design principles ? **(5 Marks)**

Ans. : **Please refer Q. 8 of Chapter 10.**

Chapter 11 : IP Security [Total Marks - 10]

Q. 6(ii) Write in brief about : SSL handshake protocol. **(5 Marks)**

Ans. : **Please refer Q. 5(a) of Dec. 2015.**

Q. 6(iii) Write in brief about : IP Sec protocols for security. **(5 Marks)**

Ans. : **Please refer Q. 1 of Chapter 11.**

Chapter 12 : Non-Cryptographic Protocol Vulnerabilities Phishing [Total Marks - 15]

Q. 4(a) Compare packet sniffing and packet spoofing. Explain session hijacking attack. **(10 Marks)**

Ans. :

Sr. No.	packet sniffing	packet spoofing
1.	Sniffing is the most effective technique which is used to attack over the network and gain over the network	spoofing is the technique to get the identity of another computer with the special privileges so as to get over to the network
2.	Sniffing is a passive security attack.	Spoofing is the active security attack.
3.	Sniffing does not interrupt and alters the data.	Spoofing does interrupt and alters the data.

Sr. No.	packet sniffing	packet spoofing
4.	Sniffing word comes from the word "sniff the ether" where "ether" is Ethernet network	Spoofing follows the term "masquerade". Masquerade means fooling the other machines on the network into accepting the other user into real or original network.
5.	Sniffing can be used in the good and bad manner.	Spoofing is done with the help of sniffing because with the help of sniffing it is more effective.

(5 Marks)

Q. 6(iv) Write in brief about : Denial of service attacks.

Ans. : Please refer Q. 4 of Chapter 12.

❑❑❑

Dec. 2015

Q. 1 (a) Define the following with examples :
i) Substitution cipher, ii) Poly-alphabetic cipher,
iii) Salami attack iv) Session hijacking **(10 Marks)**

(b) With the help of examples explain non-malicious programming errors. **(5 Marks)**

(c) Define the goals of security and specify mechanisms to achieve each goal. **(5 Marks)**

Q. 2 (a) In an RSA system the public key (e,n) of user A is defined as (7,119). Calculate ϕ_n and private key d. What is the cipher text when you encrypt message m = 10, using the public key ? **(10 Marks)**

(b) Give the format of X 509 digital certificate and explain the use of a digital signature in it. **(5 Marks)**

(c) Encrypt "The key is hidden under the door" using Playfair cipher with keyword "domestic". **(5 Marks)**

Q. 3 (a) Explain how a key is shared between two parties using Diffie Hellman key exchange algorithm. What is the drawback of this algorithm? **(10 Marks)**

(b) Differentiate between : i) MD-5 and SHA ii) Firewall and IDS. **(10 Marks)**

Q. 4 (a) Explain working of DES detailing the Fiestel structure . **(10 Marks)**

(b) What is a Denial of service attack. What are the different ways in which an attacker can mount a DOS attack on a system? **(10 Marks)**

Q. 5 (a) List the functions of the different protocols of SSL. Explain the handshake protocol. **(5 Marks)**

(b) How does PGP achieve confidentiality and authentication in emails? **(5 Marks)**

(c) Differentiate between the transport mode and tunnel mode of IPSec and explain how authentication and confidentiality are achieved using IPSec. **(10 Marks)**

(20 Marks)

Q. 6 Write in brief about (any four) :
i) Operating System Security, ii) Buffer overflow attack,
iii) IP spoofing, iv) Viruses and their types,
v) Key generation in IDEA.

❑❑❑

May 2016

Q. 1 (a) Explain software flaws with examples **(5 Marks)**

(b) List with examples the different mechanisms to achieve security **(5 Marks)**

(b) Explain with examples, keyed and keyless transposition ciphers **(5 Marks)**

(c) Elaborate the steps of key generation using RSA algorithm **(5 Marks)**

Q. 2 (a) A and B decide to use Diffie Hellman algorithm to share a key. They chose p = 23 and g = 5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. **(10 Marks)**

(b) Explain working of DES. **(10 Marks)**

Q. 3 (a) What is access control? How does the Bell La Padula model achieve access control. **(10 Marks)**

(b) What is a digital signature. Explain any digital signature algorithm in detail. **(10 Marks)**

Q. 4 (a) Compare packet sniffing and packet spoofing. Explain session hijacking attack. **(10 Marks)**

(b) Explain working of Kerberos. **(10 Marks)**

Q. 5 (a) What is a firewall? What are the firewall design principles? **(5 Marks)**

(b) What are the various ways for memory and address protection **(5 Marks)**

(c) Explain the significance of an intrusion detection system for securing a network. Compare signature based and anomaly based IDS. **(10 Marks)**

Q. 6 Write in brief about (any four) : **(20 Marks)**

i) Email security,

ii) SSL handshake protocol,

iii) IP Sec protocols for security,

iv) Denial of service attacks,

v) IDEA

□□□