T.Y. Diploma : Sem. V
[CO/CM]

Computer Security

Time: 3 Hrs.] Prelim Question Paper Solution **[Marks : 100**

Q.1(a) Attempt any THREE of the following : [12]

Q.1(a) (i) Write benefits of VPN. [4]

(A) Benefits of VPN :

1) **Enhanced security :** When you connect to the network through a VPN, the data is kept secured and encrypted. In this way the information is away from hackers' eyes.
2) **Remote control :** In case of a company, the great advantage of having a VPN is that the information can be accessed remotely even from home or from any other place. That's why a VPN can increase productivity within a company.
3) **Share files :** A VPN service can be used if you have a group that needs to share files for a long period of time.
4) **Online anonymity :** Through a VPN you can browse the web in complete anonymity. Compared to hide IP software or web proxies, the advantage of a VPN service is that it allows you to access both web applications and websites in complete anonymity.
5) **Unblock websites & bypass filters** : VPNs are great for accessing blocked websites or for bypassing Internet filters. This is why there is an increased number of VPN services used in countries where Internet censorship is applied.
6) **Change IP address :** If you need an IP address from another country, then a VPN can provide you this.
7) **Better performance :** Bandwidth and efficiency of the network can be generally increased once a VPN solution is implemented.
8) **Reduce costs :** Once a VPN network is created, the maintenance cost is very low. More than that, if you opt for a service provider, the network setup and surveillance is no more a concern.

Q.1(a) (ii) Write a note on Web Server. [4]

(A)

- Web servers are computers that deliver Web Pages. Every web server has an IP address and a possibly domain name.
- For example, if one enters the URL 'http://www.newinformation.com/index.html' in the browser, this sends q request to the Web server whose domain name is 'newinformation.com'. The server then fetches the page names index.html and sends it to the browser.
- Web servers are responsible for storing and exchanging information with other machines or servers.
- A computer can be turned into a web server by installing server software and connecting the machine to the Internet.
- Examples – Apache HTTP server, sunjava system web server, IIS.

Q.1(a) (iii) Write a note on DMZ – DeMilitarized Zone. [4]

(A)

- It is a buffer against outside attack.
- In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ. Those computers on the outside intercept traffic and broker requests for the rest of the LAN, adding an extra layer of protection for computers behind the firewall.
- Traditional DMZs allow computers behind the firewall to initiate requests outbound to the DMZ. Computers in the DMZ in turn respond, forward or re-issue requests out to the Internet or other public network, as proxy servers do. The LAN firewall, though, prevents computers in the DMZ from initiating inbound requests.

- DMZ is a commonly-touted feature of home broadband routers. Broadband routers often implement a DMZ simply through additional firewall rules, meaning that incoming requests reach the firewall directly. In a true DMZ, incoming requests must first pass through a DMZ computer before reaching the firewall.

Q.1(a) (iv) Why e-mails are preferred over snail mail? Enlist fields of RFC-822 for e-mail. [4]

(A) **Reasons** why e-mails are preferred over snail-mail :

- **Speed :** The process of sending a message via email is quicker than snail mail.
- **Convenience :** Email enables people to send messages and information at the touch of a button from whatever location they are presently at. Email messages can be sent 24 hours a day, seven days a week. Business users benefit because messages can be sent to co-workers and other businesses whether the recipient is out of the office or on the phone. Email recipients enjoy the convenience of answering the messages in their own time frame.
- **Different Types of Information Can Be Sent and Received :** Many different types of information can be sent via email including letters, messages, pictures, data files, articles and videos to name a few.
- **Queries Can Be Made Cost Effectively :** Email is preferred over snail mail when needing to obtain information from many different sources to make important decisions. Since sending and receiving email can be free (especially if you use a local library and free email provider), snail mail can be expensive when figuring in copying and postage costs.
- **Privacy and Security :** Email is private unless the sender or recipient choose to share their email address with others. Receiving information through snail mail involves some risk that another person may open the contents of the package before you are able to.

Fields of RFC-822 for e-mail :

- From
- To
- Subject
- Date
- Contents

Q.1(b) Attempt any ONE of the following : [6]

Q.1(b) (i) How PEM is used for email model? [6]

(A)

- PEM is Private Enhanced Mail. It is an email security standard to provide secure electronic mail communication over the internet.
- PEM supports the three main cryptographic functions of encryption, non-repudiation and message integrity.
- The steps in PEM are Canonical Conversion, Digital signature, Encryption and Base-64 Encoding.
  1) **Canonical Conversion :** PEM transforms each email message into an abstract, canonical representation. This means that regardless of the architecture and the operating system of the sending and the receiving computers, the email message always travels in uniform, independent format.
  2) **Digital signature :** This process starts by creating a message digest of the email message using MD@ or MD5 algorithm.

Email message
To : anand@abc.com
From: abhay@xyz.net → Message Digest algorithm → 10101
Subject: Our meeting (MD2 or MD5) 01010
10…
Message digest

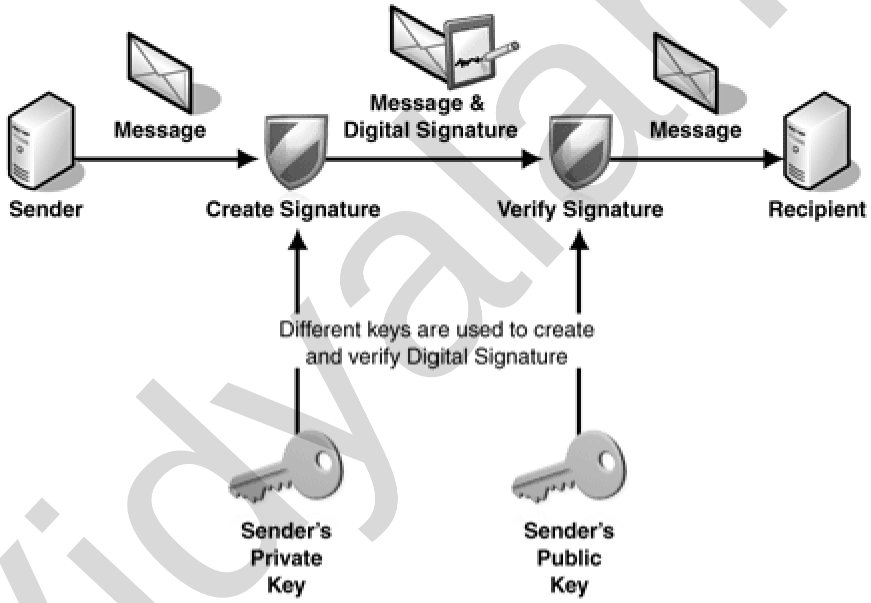
Message Digest creation of the original message :
The message digest thus created is then encrypted with the sender's private key to form the sender's digital signature.

10101
01010 → Encryption with Sender's → Digital signature
10... Private key

3) **Encryption :** In this step, the original email and the digital signature are encrypted together with a symmetric key. For this, DES algorithm is used.
4) **Base-64 Encoding :** In this step, the Base-64 encoding process transforms arbitrary binary input into printable character output. In this technique, the binary output is processed in blocks of 3 octets or 24 bits. These 24 bits are considered to be made up of 4 sets, each of 6 bits. Then their decimal equivalent generated is looked up into the 64-encodind mapping table. The character found at the position specified by the decimal number in this table is then mentioned in the output. Finally, the binary equivalent corresponding to 8-bit ASCII of this character is written.

Q.1(b) (ii) Explain digital signature with advantages and disadvantages. **[6]**

(A)
- Digital signature is the scheme in the context of asymmetric key cryptography.
- If A is the sender of a message and B is the receiver, A encrypts the message with A's private key and sends the encrypted message to B.



- When one encrypts a message with her private key, the intention is not to hide the message (Confidentiality).
- When B receives a message encrypted with A's private key, B can use A's public key to decrypt it which assures B that the message is indeed came from A as the message encrypted with A's private key can only be decrypted with A's public key and only A knows her private key.
- This scheme does not achieve the confidentiality but it achieves Authentication.
- Such a scheme, wherein the sender encrypts the message with her private key, forms the basis of digital signature.

Advantages :

1) Speed : Business no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.

2) Costs : Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.
3) Security : The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed or altered while in transit.
4) Authenticity : An electronic document signed with a digital signature can stand up in court just as well as the other signed paper documents.
5) Tracking : A digitally signed document can easily be tracked and located in a short amount of time.
6) Non-repudiation : Signing an electronic document digitally identifies you as the signatory and that cannot be later denied.
7) Imposter prevention : No one else can forge your digital signature or submit an electronic document falsely claiming it was signed by you.
8) Time-stamp : By time-stamping your digital signatures, you will clearly know when the document was signed.

Disadvantages :

1) Expiry : Digital signatures, like all technological products, are highly dependent on the technology it is based on. Many of these tech products have a short shelf life.
2) Certificates : In order to effectively use digital signatures, both sender and recipient may have to buy digital certificates at a cost from trusted Certification authority.
3) Software : To work with digital certificates, senders and receipients have to buy verification software at a cost.
4) Law : In some states and countries, law regarding cyber and technology based issues are weak or even non-existent. Trading in such jurisdiction becomes very risky for those who use digitally signed electronic documents.

Q.2 Attempt any TWO of the following : [16]

Q.2(a) Explain role of biometrics in security. [8]

(A)

- Biometrics is defined as the unique (personal) physical/logical characteristics or traits of human body. These characteristics and traits are used to identify each human. Any details of the human body which differs from one human to other will be used as unique biometric data to serve as that person's unique identification (ID), such as: retinal, iris, fingerprint, palm print and DNA.
- Biometric systems will collect and store this data in order to use it for verifying personal identity. The combination of biometric data systems and biometrics recognition/ identification technologies creates the biometric security systems. The biometric security system is a lock and capture mechanism to control access to specific data. In order to access the biometric security system, an individual will need to provide their unique characteristics or traits which will be matched to a database in the system. If there is a match, the locking system will provide access to the data for the user. The locking and capturing system will activate and record information of users who accessed the data. The relationship between the biometric and biometric security system is also known as the lock and key system. The biometrics security system is the lock and biometrics is the key to open that lock.
- There are seven basic criteria for biometric security system: uniqueness, universality, permanence, collectability, performance, acceptability and circumvention.
- Uniqueness is considered as the priority one requirement for biometric data. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users.
- For instance, the DNA of each person is unique and it is impossible to replicate.
- Universality is the secondary criteria for the biometric security. This parameter indicates requirements for unique characteristics of each person in the world, which cannot be replicated. For example, retinal and iris are characteristics will satisfy this requirement.

- Thirdly, a permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This parameter will mostly be affected by the age of the user.
- The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification.
- Performance is the next parameter for the system which outlines how well the security system works.
- The accuracy and robustness are main factors for the biometric security system. These factors will decide the performance of the biometric security system.
- The acceptability parameter will choose fields in which biometric technologies are acceptable.
- Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. DNA is believed to be the most difficult characteristic leading to the failure of the verification process.

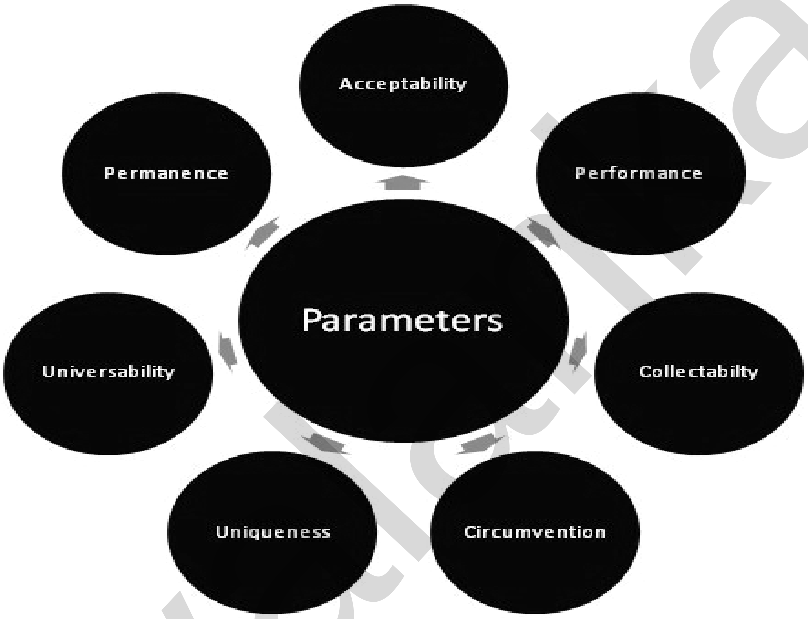


Fig. : Basic Criteria for Biometrics Security System.

Q.2(b) How DES works? Explain in detail. **[8]**

(A)
- DES is a widely used method of data encryption using a private (secret) key that is difficult to break.
- Both the sender and the receiver must know and use the same private key.
- DES applies a 56 bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds of operations.

How DES works?

1) **Initial Permutation (IP)** : Transposition or replacement between the bits IP replaces the 1st bit of the original plain text block with 58th bit of original plain text block, the 2nd bit with the 50th bit of the original plain text block and so on. This is nothing but jugglery of bit positions of the original plain text.

The idea of Initial Permutation is shown in this table.

Bit position in plain text block	To be overwritten with the contents of this position
1	58
2	50
3	42
...	...
64	7

The complete transposition table is shown below. The table should be read from left to right, top to bottom. For instance, note that 58 in the first position indicates that the contents of the 58th bit in the original plain text block will overwrite the content of the 1st bit position, during IP.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62								64							
57								59							
61								63							

After IP, 64 bit text is divided into two parts(32-32).
They are Left Plain Text(LPT) and Right Plain Text(RPT).

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No. of key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

2) 16 Rounds are performed on these blocks separately.
Each round = 5 steps

Step 1: Key Transformation or Key Compression.
Input = 56 bit key
Output = 48 bits key

Please note for each round, a 56 bit key is available. From this 56-bit key, a different 48-bit sub-key is generated during each round using a process key transformation. For this, the 56-bit key id divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round. For example, if the round number is 1, 2, 9 or 16, the shift is done by only one position. For others, the shift is done by two positions.

After an appropriate shift, 48 of 56 are selected. For selecting 48 out of 56 bits, the table shown below is used. This is compression permutation table, which is used in the same way as we had seen in initial permutation.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Since, the key transformation process involves permutation as well as selection of 48-bit-sub-set of the original 56-bit key, it is called compression permutation. Because of this compression permutation technique, a different subset of key bit is used in each round. That makes DES not so easy to crack.

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

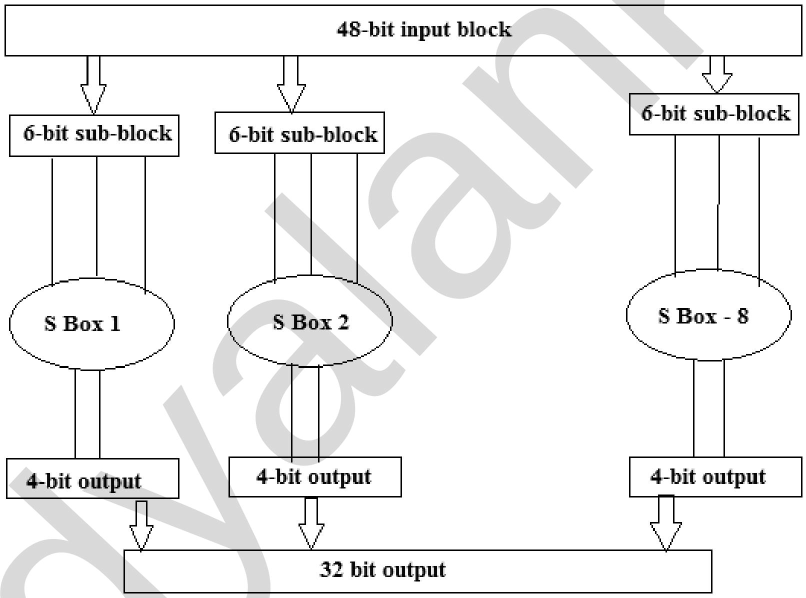
Step 2: Expansion permutation.
During Expansion permutation the RPT(Right Plain Text) is expanded from 32 bits to 48 bits.
The bits are permuted as well as expanded.
PROCESS : It is a 3 step process

1) 32 bits are divided into 8 equal parts 4 bits x 8 data encryption standard algorithm

2) Each 4 bits are transformed into 6 bits. 6 x 8 = 48 bits expansion permutation
   As we can see, the first input bit goes into the second and 48th output position. The second input bit goes to the third output position and so on. Simply, we can find that the output 48 bit sequence would be in the following manner.
3) Finally the 48 bit key(from previous step) and 48 bit RPT are XORed into new 48 bit RPT.

Step 3: S-Box Substitution.
Input: 48 bits new RPT (XORed from previous step)
Output: 32 bits (after substitution)

The substitution is performed by eight substitution boxes called S-Boxes. Each of the eight S-boxes has a 6-bit input and 4 bit output.
S-box 1 gives --> First 4 bits of Output.
S-Box 2 gives --> Second 4 bits of data and so on.
Given, 8 S-boxes which are 4 x 16 table which we will use for fetching each 4 bit data is shown below :



S-Box 1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-Box 2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

PROCESS:
1) Divide 48 bit input into eight 6 equal bits.
2) 4 rows
   16 columns

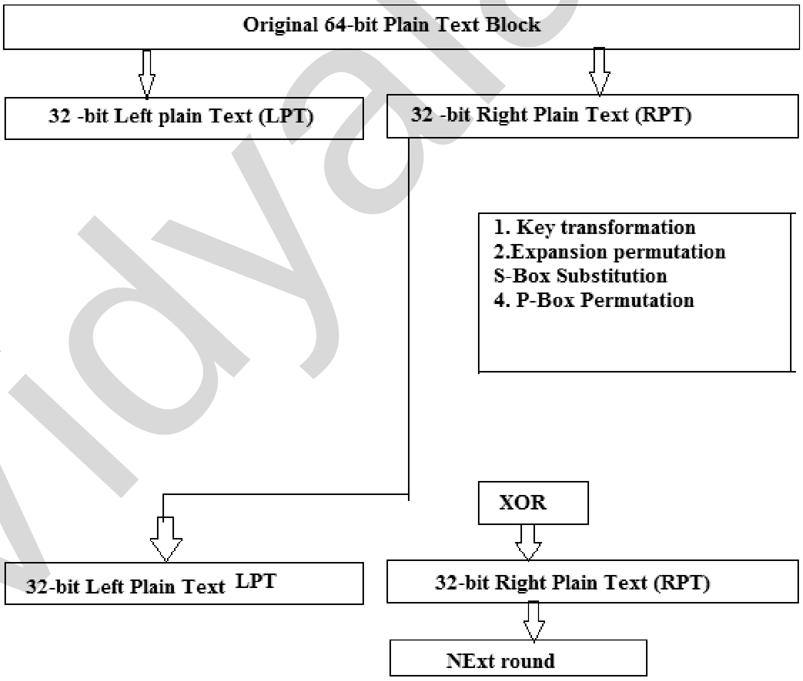
3) See the number (i.e 0-15) from the S-Box 2[3][6], and that is 4 and in binary form that is 0100 4 bit of output from S-Box 2
   Please note that 3 denotes 4th row while 6 denotes 7th row.
4) Similarly from all 8 boxes give
   8 x 4
   32 bit O/P

Step 4: P-Block Permutation
Input: 32 bit RPT(after S-box substitution)
Output: 32 bit RPT(after P-box permutation)
It involves straight forward permutation or transformation.
The permutation table for P-Box Permutation is shown below:

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

As we know how to use the transposition table, the 16 in the first block position indicates that the bit at position 16 of the original input moves to bit at position 1 in the output and so on.

Step 5: XOR and Swap
We have performed all these operations only on the 32 bit right half portion of the 64-bit original plain text. The left half portion (32 bit) was untouched so far. At this juncture, the left half portion of the initial 64-bit plain text block (LPT) is XORed with the output produced by P-Box permutation. The result of this XOR operation becomes the new right half (RPT). The old RPT becomes the new left half, in a process of swapping.


Original 64-bit Plain Text Block
32 -bit Left plain Text (LPT)
32 -bit Right Plain Text (RPT)
1. Key transformation
2.Expansion permutation
S-Box Substitution
4. P-Box Permutation
XOR
32-bit Left Plain Text LPT
32-bit Right Plain Text (RPT)
NExt round

3) Final Permutation

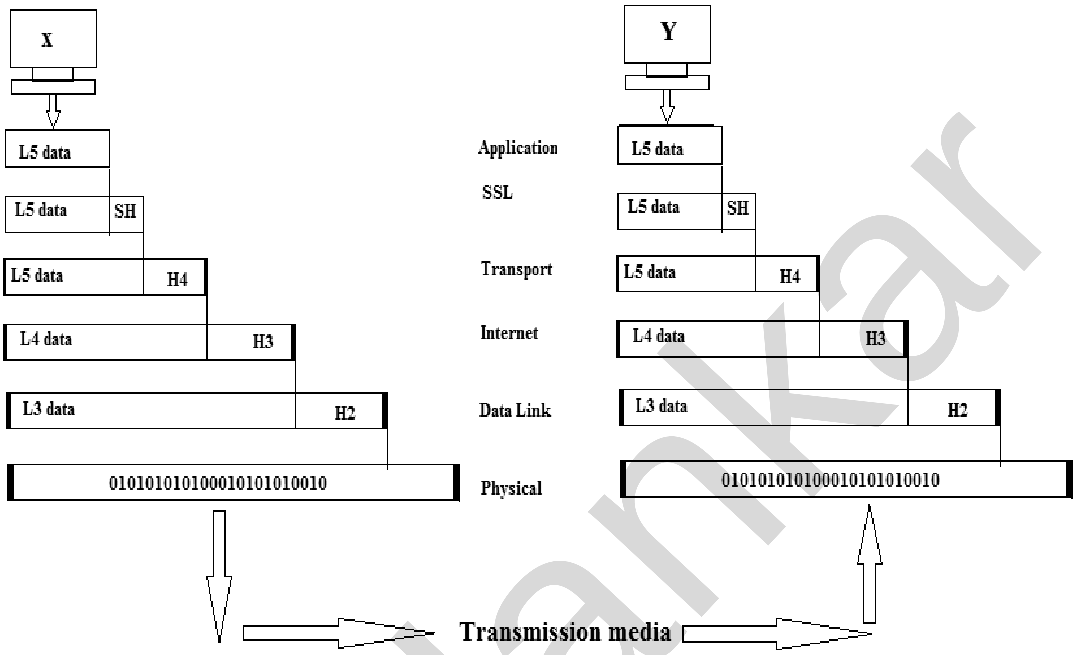
After 16 rounds, final permutation is performed on 64 bit XORed and swapped O/P. It is a simple permutation and the table is:

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	3	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	30	18	58	26	33	1	41	9	49	17	57	25

So, the output of the final permutation is the 64 bit encrypted block.

Q.2(c) Describe SSL Protocol. At which layer of OSI it works. Draw and explain in brief SSL Protocol Stack. [8]

(A)
- SSL – Secure Socket Layer is an Internet protocol for Secure exchange of information between a web browser and a web server.
- SSL has three sub-protocols, namely Handshake Protocol, the Record Protocol and the Alert protocol.
- The objectives of SSL are authentication and confidentiality.
- SSL layer is located between the Application layer and the Transport layer of OSI.

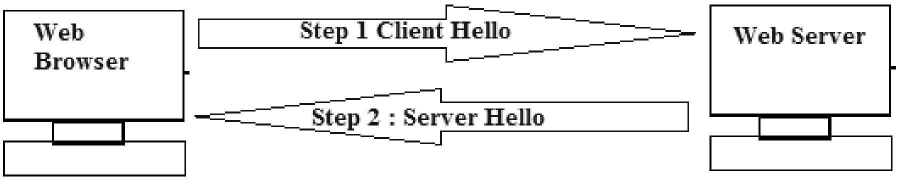


- The application layer of the sending computer (X) prepares the data to be sent to the receiving computer(Y). Unlike what happens in the normal case, the application layer data is not passed directly to the transport layer. Instead, it is passed to the SSL layer. Here, the SSL layer performs encryption on the data received and also adds its own encryption in formation header called as, SSL Header (SH) to the encrypted data.
- Then the SSL layer data (L5) becomes the input for transport layer. It adds its own header (H4) and passes it on the Internet layer and so on. Finally when the data reaches the physical layer, it is sent in the form of voltage pulses across the transmission media.
- Exactly opposite process happens at the receiver's end. The SSL layer at the receiver's end removes the SSL header (SH), decrypts the encrypted data and gives the plain text data back to the application layer of the receiving computer.
- Thus only the Application layer data is encrypted by SSL. The lower layer headers are not encrypted.
  SSL has three sub-protocols, namely Handshake Protocol, the Record Protocol and the Alert protocol. These three protocols constitute the overall working of SSL.

The Handshake Protocol :
- This protocol of SSL is the first sub-protocol used by the client and the server to communicate using SSL-enabled connection.

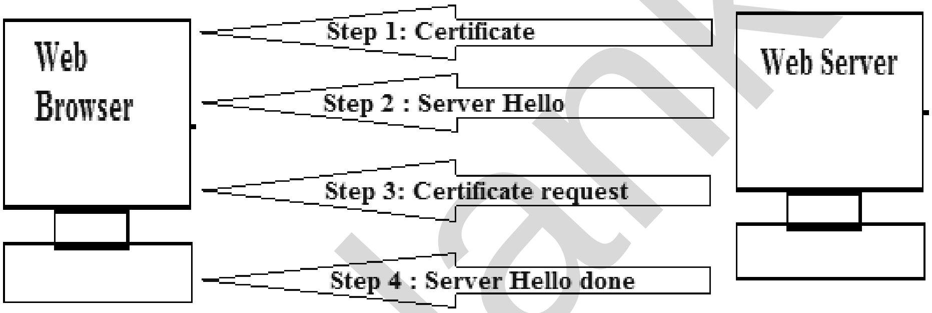
Handshake protocol is actually made up of four phases. These are :
1) Establish security capabilities
2) Server authentication and key exchange
3) Client authentication and key exchange
4) Finish

1) **Establish security capabilities :**
   - This first phase is used to initiate a logical connection and establish the security capabilities associated with that connection.

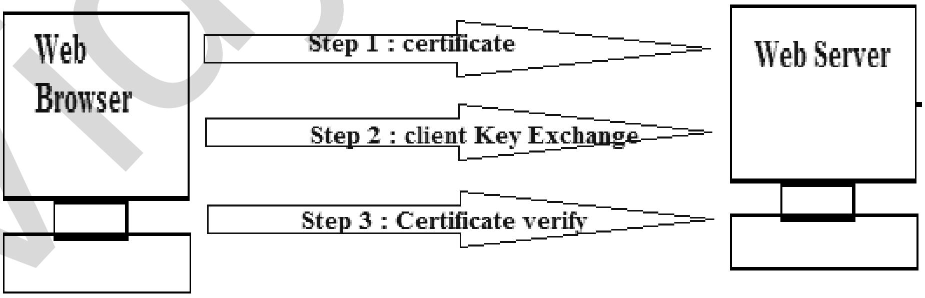


This consists of two messages, the Client hello and the Server hello.

2) **Server Authentication and Key exchange :**
   - Initiated by the server which is the sole sender of all the messages in this phase.
   - The client is the sole recipient.
   - Contains 4 steps :
     1) Certificate
     2) Server Key Exchange
     3) Certificate Request
     4) Server Hello done



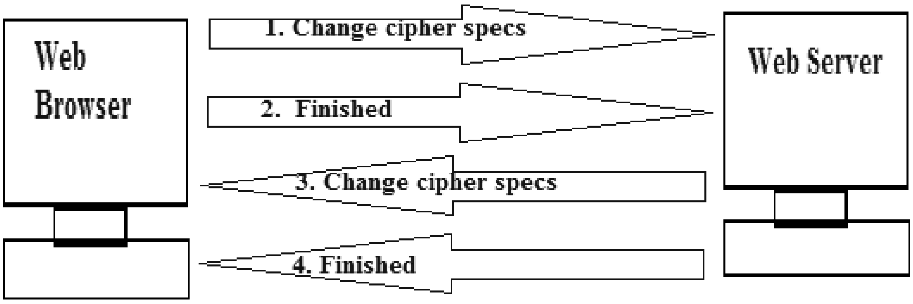
3) **Client Authentication and Key Exchange :**
   - The client initiates this third phase and is the sole sender of all the messages in this phase and the server is the sole recipient.
   - This phase contains three steps
     1) Certificate
     2) Client Key exchange
     3) Certificate Verify



4) **Finish**

   Based on the pre-master secret that was created and sent by the client in the Client key exchange message, both the client and the server create a master secret. Before secure encryption or integrity verification can be performed on records, the client and server need to generate shared secret information known only to them. This is master secret which is used to generate keys and secrets for encryption and MAC calculations.
   - Finally, the symmetric keys to be used by the client and the server are generated.

After this, the first step, Change cipher specs, is a confirmation from the client that all well from its end, which it strengthens with the Finished Message.



The Record Protocol :

- The Record Protocol in SSL comes into picture after a successful handshake between the client and the server.
- This protocol provides two services to an SSL connection
  - › **Confidentiality :** This is achieved by using the secret key that is defined by the handshake protocol.
  - › **Integrity :** The handshake protocol also defines a shared secret key (MAC) that is used for assuring the message integrity.
- Record protocol takes an application message as input. First, it fragments it into smaller blocks, optionally compresses each block, adds MAC, encrypts it, adds a header and gives it to the transport layer, where the TCP protocol processes it like any other TCP block. At the receiver's end, the header of each block is removed; the block is then decrypted, verified, decompressed into application message.

The Alert Protocol :

- When either the client or the server detects an error, the detecting party sends an alert message to the other party. If the error is fatal, the parties immediately close the SSL connection. Both parties also destroy the session identifiers, secrets and keys associated with this connection before it is terminated.
- Each alert message consists of two bytes. The first byte signifies the type of error. If it is a warning, the byte contains 1. If the error is fatal, this byte contains 2. The second byte specifies the actual error.

Q.3 Attempt any FOUR of the following : [16]

Q.3(a) Compare MD5 and SHA algorithm. [4]

(A)

	Points	**MD5**	**SHA-1**
1)	Message digest length in bits	128	160
2)	Attack to try and find the original message given a message digest	Requires 2^128 operations to break in	Requires 2^160 operations to break in, therefore more secure.
3)	Attack to try and find two messages producing the same message digest	Requires 2^64operations to break in	Requires 2^80 operations to break in
4)	Successful attacks so far	Reported attempts to some extent	No such claims so far
5)	Speed	Fast	Slower
6)	Software implementation	Simple	Simple

Q.3(b) Explain how Pretty Good Privacy e-mail security works? [4]

(A)
- It is Pretty Good Privacy.
- It offers email cryptographic support.
- PGP supports the basic requirement of cryptography, is quite simple to use and is completely free, including its source code and documentation.
- PGP operation has 5 steps –
  1) Digital signature
  2) Compression
  3) Encryption
  4) Enveloping
  5) Base-64 Encoding

Digital signature : This process starts by creating a message digest of the email message using MD@ or MD5 algorithm.

Email message		
To : anand@abc.com		
From: abhay@xyz.net →	Message Digest algorithm →	10101
Subject: Our meeting	(MD2 or MD5)	01010
		10…
		Message digest

Diagram : Message Digest creation of the original message

The message digest thus created is then encrypted with the sender's private key to form the sender's digital signature.

Compression – the input message as well as the digital signature together to reduce the size of the final message that will be transmitted. For this the ZIP program is used which uses Lempel-Ziv algorithm.

It looks for repeated strings or words and stores them in variables. It then replaces the actual occurrence of the repeated strings or word with a pointer to the corresponding variable. Since a pointer requires only a few bits of memory as compared to the original string, this method results in the data being compressed.

Example :

What is your name? My name is Atul	→ Original String
1) A = 2 2) B= name	→ Variable creation and Assignment
What 1 your 2? My 2 1 Atul	→ compressed string

- **Encryption :** In this step, the compressed output of Step 2 are encrypted with a symmetric key.
- **Digital Enveloping :** In this case, the symmetric key used for encryption in step 3 is now encrypted with the receiver's public key. the output of Step 3 and step 4 together form a digital envelop.
- **Base-64 encoding :** The output of step 4 is Base-64 encoded.(this step is mentioned in PEM answer.

Q.3(c) Explain IDS with its types. [4]

(A) **Intrusion Detection System :**
- Intrusion Detection System is a system for detecting Network Attacks.
- IDS consists of a set of sensors gathering data, either located on host or on the network. There, data is analyzed, intrusions reported and reactions triggered,

  There are two types of IDSs
  1) Network based IDS
  2) Host based IDS

1) **Network based IDS :** Network based IDS resides on a computer connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks. When a situation occurs that the NIDs is programmed to recognize as an attack, it responds by sending notifications to administrators. When examining the packets transmitted through an organization's network, a NID looks for attack patterns within network traffic such as a denial-of-service-attacks, port scan attack etc.
2) **Host based IDS :** Host based IDS resides on a particular computer or server, known as the host, and monitors activity only on that system. HIDS are also known as system integrity verifiers as they monitor the status of the key system files and detect when an intruder creates, modifies or deletes modified files. The HIDs is also capable of monitoring system configuration databases, such as windows registries, in addition to stored configuration files like .ni, .cfg and .dat files. Most HIDs work on the principle of configuration or change management which means they can record the sizes, locations and other attributes of the system files. The HIDs then triggers an alert when one of the following changes occurs: file attributes change, new files are created, or existing files are deleted.

Q.3(d) Explain Honey Pots with respect to Intrusion Detection. [4]

(A)
- **Honey pots** – are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves.
- These systems are created for the sole purpose of deceiving potential attackers.
- A honey pots system contains pseudo-services that emulate well known services but is configured in ways that it looks vulnerable.
- The combination of attractive features such as presence of both well-known services and vulnerabilities is meant to lure potential attackers into committing an attack, and thereby revealing their existence- the idea is that once organizations have detected these attackers, they can better defend their networks against future attacks against real assets.
- In sum, honey pots are designed to
  - › Divert an attacker from accessing critical systems
  - › Collect information about the attacker's activity.
  - › Encourage the attacker to stay on the system long enough for administrators to document the event and respond.

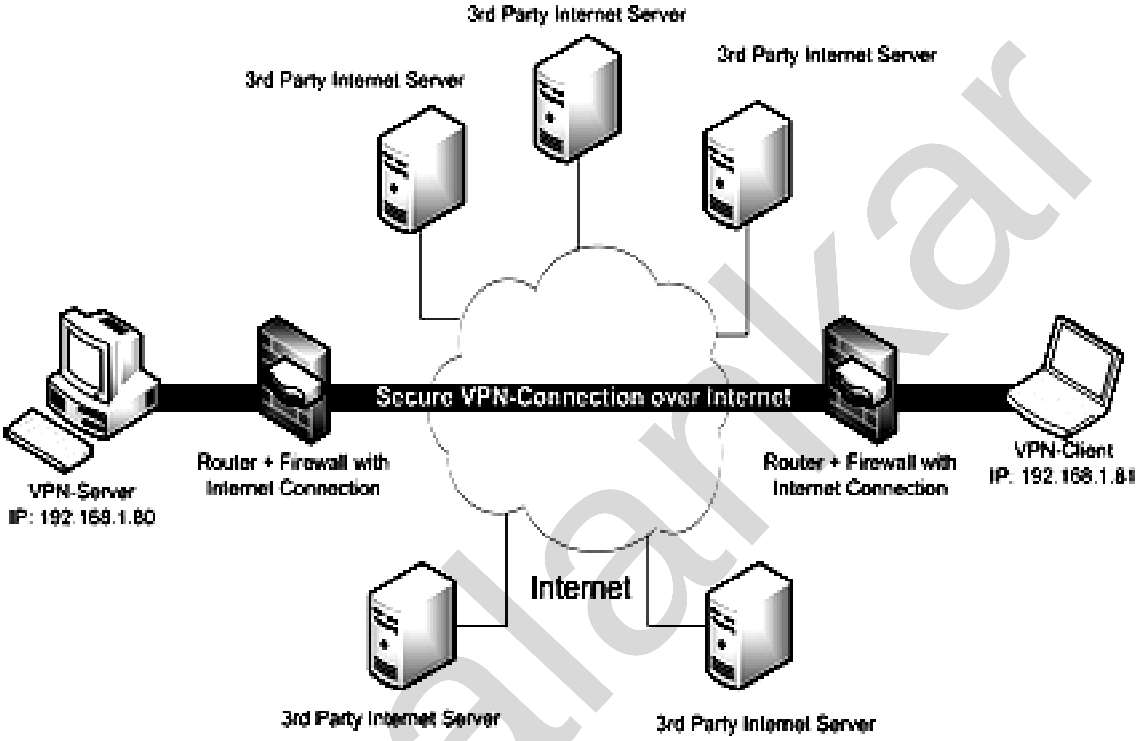
Q.3(e) Explain VPN with a Diagram. [4]

(A)
- A VPN is a mechanism of employing encryption, authentication and integrity protection so that one we use a public network (internet) as if it is a private network aerated and controlled by us.
- VPN offers high amount of security and yet does not require any special cabling on behalf of the organization that wants to use it.
- Thus a VPN combines the advantages of a public network(cheap and easily available) with those of a private network (secure and reliable).
- A VPN can connect distant networks of an organization or it can be used to allow travelling users to remotely access a private network securely over the internet.

VPN Architecture

- Suppose an organization has two networks, Network 1 and Network 2, which are physically apart from each other, two firewalls can be set up, Firewall1 and firewall 2. The encryption and decryption are performed by firewalls.
- Network 1 connects to Internet via firewall1 and Network connects to Internet via firewall 2. Two firewalls are virtually connected to each other via the Internet.
- Let's assume Host X on Network 1 to send data packet to Host Y on Network 2.

- Host X creates the packet, inserts its own IP address as the address and the IP address of host Y as the destination address.
- The packet reaches firewall 1. Firewall 1 now adds new headers to the packet. It changes the source IP address of the packet from that of Host X to its own address. It also changes the destination IP address of the packet from that if host Y to the IP address of firewall 2. It also performs encryption and authentication.
- The packet reaches Firewall 2 over the Internet via one or more routers. Firewall 2 discards the outer header and performs the decryption and other cryptographic functions. This yields the original packet. Then the packet is delivered to Y.


3rd Party Internet Server
3rd Party Internet Server
3rd Party Internet Server
Secure VPN-Connection over Internet
VPN-Server
IP: 192.168.1.80
Router + Firewall with Internet Connection
Router + Firewall with Internet Connection
VPN-Client
IP: 192.168.1.81
Internet
3rd Party Internet Server
3rd Party Internet Server

Q.4(a) Attempt any THREE of the following : [12]

Q.4(a) (i) Define intruder and state it's any three types. [4]

(A) **Intruder** – an intruder is a person who is not belonging to the organization(an outsider) who tries to intrude and launch security threats and attacks from outside.

3 types of intruders :

1) Masqurader – A user who does not have the authority to use a computer, but penetrates into a system to access a legitimate user's account is called a masquerader. It is generally an external user.
2) Misfeasor – There are two possible cases for an internal user to be called as misfeasor
   (a) A legitimate user, who does not have access to some applications, data or resources, accesses them.
   (b) A legitimate user, who has access to some applications, data or resources misuses these privileges.
3) Clandestine user – an internal or external user who tries to work using the privileges of a supervisor user to avoid auditing information being captured and recorded is called as a clandestine user.

Q.4(a) (ii) What is role based authentication? [4]

(A) **Role Based Access Control (RBAC)**

- Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the enterprise.

- When properly implemented, RBAC enables users to carry out a wide range of authorized tasks by dynamically regulating their actions according to flexible functions, relationships, and constraints. This is in contrast to conventional methods of access control, which grant or revoke user access on a rigid, object-by-object basis.
- In RBAC, roles can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.
- RBAC can be viewed as a set of permissions granted to subject for its current role.
  - > Role assignment – the role should be assigned to the subject and that limits the working domain of the subject.
  - > Role authorization – the role is authorized to the given subject ensuring that the subject is working within the role authorized to it.
  - > Transaction authorization – the subject is granted permission to carry out transaction specified within the assigned and authorized role.

Q.4(a) (iii) Describe the term virus and its working with example. [4]

(A) **Virus** is defined as a piece of malicious code that attaches itself to legitimate program code and runs when the legitimate program runs. It can then infect other programs in that computer or programs that are in other computers but on the same network.

Working of Boot Sector Viruses :

- Infest the boot sector of a computer system.
- Relocates the original OS boot sector.
- Gains early control on the system (while it is booting)

Boot sector viruses copy their code in the first sector of the boot disk device. The original boot sector contents of OS are copied to some other sectors on the disk. On such infected system, the booting is done through virus. Virus first loads and activates itself and subsequently gives the control to the actual boot sector of OS. Then the OS booting takes place.

- The virus gains access before OS and so has a free hand on system resources.
- The virus can report falsely to the OS about memory and other system parameters and therefore successfully hiding itself.
- The virus gains control at the highest privilege level and therefore surpasses OS protection.

Working of Program viruses

Program viruses attach to their host code in different ways. The simplest way is to append the program at one of its ends either in the beginning or at the end. Such viruses are easy to attach, however they are in single piece making them easy to detect and easy to remove. Another way is to embed the host code into multiple pieces. In this case, virus splits into small pieces and infects the host code at various locations.

Working of E-mail viruses: An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software.

Q.4(a) (iv) Explain the difference between Active and Passive Computer Security Attack. [4]

(A)

	Active Computer security attack	Passive Computer Security attack
1)	The active attacks are those, wherein the attacker indulges in the modification of the original message in some manner or creation of false message.	Passive attacks are those, wherein the attacker indulges in eavesdropping or monitoring of data transmission.
2)	The term active indicates that the attacker does perform modifications to the data.	The term passive indicates that the attacker does not attempt to perform any modifications to the data.
3)	Active attacks are comparatively easier to detect.	Passive attacks are harder to detect.
4)	Example, Fabrication (Denial of service attack), Modification attacks (Replay attacks, alteration of message)	Example, Release of message content, traffic analysis

Q.4(b) Attempt any ONE of the following : [6]

Q.4(b) (i) Explain different methods of authentication. [6]

(A) Authentication

Authentication is any process by which a system verifies the identity of a user wishes to access it.

Different methods of authentication –

1) **Knowledge or password based Authentication (Security)**
   - Authentication on the basis of something that is in the knowledge of user password is the most common method.
   - Password : it is defined as unique sequence of symbols that positively identifies the user to the system and known only to the user and the system and no one else.
   - Password based security is most commonly used authentication method.
   - Passwords are maintained by system in a system password list which is hidden from the user and is in encrypted form.
   - Passwords must be maintained absolutely secretly by the users in order to uphold the system security.

2) **Gadget or instrument based authentication (Security)**
   - Authentication on the basis of something that is possessed by the user.
   - **Tokens :**
     - tokens are the cards like code card, smart cards , RFID cards, magnetic strip cards etc. . Different types of cards that are unique and that cannot be forged are used as tokens.
   - **Certificates :**
     - It is the digital form.
     - It is required to be possessed for the verification. The certificates are the proof of authentication. It iks often meant for transaction and has a time velocity(it expires after some time). Certificates are usually in encrypted form.

3) **Biometric Authentication (Security)**
   - Biometric identification is used on the basis of some unique physical attribute of the user that positively identifies the user.
   - Examples – Fingerprint, handprint recognition, retina scan techniques, palm capillary mapping, voice patterns, signature and writing patterns, keystrokes.

- **Fingerprint recognition** – in this, the fingerprints of the user are matched with algorithms. The user is authenticated if match of satisfactory level is obtained. Hand print recognition -
- **Retina scan technique** – in this method, the image of user's eye showing unique patterns on the retina is taken and match is found using IP algorithms.
- **Voice patterns** – in this method, the voice of user is recorded and its digital signal analysis is carried out. The analysis is matched and depending on satisfactory match, authentication is carried out.

4) **Signatures and writing patterns** – signature is the process used to recognize an individual's hand written signature. This technology uses the behavioral biometrics of a hand written signature to confirm the identity of a computer. This is done by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing.
5) **Keystrokes :**

Keystroke dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type.

Similar neuro-physiological factors that make written signatures unique, are also exhibited in a user's typing pattern. When a person types, the latencies between successive keystrokes, keystroke durations, finger placement and applied pressure on the keys can be used to construct a unique signature (i.e., profile) for that individual. For well-known, regularly typed strings, such signatures can be quite consistent. Furthermore, recognition based on typing rhythm is not intrusive, making it quite applicable to computer access security as users will be typing at the keyboard anyway.

Q.4(b) (ii) Differentiate between Centralized and decentralized infrastructure. **[6]**

(A)

	Centralized infrastructure	Decentralized infrastructure
1)	In a centralized structure all the decision making and authority are focused on the top tier of management.	A decentralized system, on the other hand, delegates authority throughout the organization and to all levels of management.
2)	Advantages of centralization include an organization's ability to be able to keep a tight grip on all aspects of the business. In a smaller business where centralization is possible, there is less chance that employees will be unaware of what is expected and what the common goals are because there is such a tight grip on all aspects of the organization from management.	An advantage o Advantages of decentralization is that there tends to be faster decision making and an ability to adapt to the demographic area of production. It also means that lower level managers have the opportunity to gain valuable experience and develop more fully because there is more room to grow.

Q.5 Attempt any TWO of the following : **[16]**

Q.5(a) Write a note on Intellectual Property (IP). **[8]**

(A)

- It is a kind of protection given for creations of the inventions like literacy and artistic works, symbols, names and images used ion commerce. IP has two kinds of values – moral and commercial.
- IP provides exclusive rights to the creator to use his/her creation for a certain period of time.
- It is divided into two main categories :

1) Copyright

- Copyright protects the rights of authors for their work of literary-novels, poems, plays, films, music and artistic work (drawings, paintings, photographs and sculptures and architectural designs) etc.

- The important and social purpose of giving protection of copyright encourages and rewards the creative work.

2) Industrial property

- **Patent** –
  - It is a special right given to an individual for his invention. Patent is a new process or product which shows a new way of doing something or it may offer a new technical solution to the previous problem.
  - Patent also provides the protection to the patent owners for their inventions and it is granted for at least next 20 years.
  - It provides incentives to patent owner by identifying his creativity and by offering the material reward for his remarkable inventions.
  - Special rights are given to the patent owners to decide who may or may not use his inventions for the period of patent's protection.
  - Patent owners can sell his invention rights to anyone, then that person becomes the new owner of the patent. When patent expires, the protection given to patent also ends and the invention enters into the public domain hence anyone can use it.

- **Trademark** –
  - The trademark sign is used to identify certain goods or services produced or provided by an individual or by a company.
  - Trademarks helps the consumers to identify and purchase a product or service of the system based on whether it has specific characteristics and /or quality that are mentioned in a trademark.
  - Its protection ensures that the owners of trademark have the special rights to use them for identifying goods or services. Protection of trademark is legally enforced by courts hence the systems with trademark have the authority to stop its infringement.
  - In general, the term of protection is five years with the possibility of further renewal, in most cases for a period of 15 years.

- **Industrial Design** –
  - It is related to the ornamental or artistic part of an article. A design can be made up of three-dimensional (3D) features like shape or surface of an article, or it may have two-dimensional (2D) features like – patterns, lines or color etc.
  - Industrial designs are used by a wide variety of industrial products like technical, medical instruments, Integrated circuits used in computers etc.
  - It makes an article attractive to add commercial value to it to increase its marketability.
  - The owner who has registered the design will be assured with an exclusive right and the protection against unauthorized use or imitation by anyone else.
  - The protection to the industrial design also provides benefit to the consumers and the public about the fair competition and honest trade practices that encourages the creativity for more pleasing products.
  - Such type of protection helps the economic development by encouraging creativity in the industrial, manufacturing, arts and craft services.

- **Geographical Indication** –
  - Geographical indication is a sign used on goods which specifies the geographical origin of those goods.
  - A geographical indication for a particular good has the name of the place of good's origin.

> Many Agricultural products have qualities which are derived from the place of origin and they are influenced by particular geographical factors like climate and soil.
>
> A geographical indication highlights the specific qualities of a product because of the human factors found in the place of origin of the product like manufacturing skills or traditions.
>
> For example, in many countries, the word "Switzerland" or "Swiss" perceived as a geographical indication for products made in Switzerland like watches

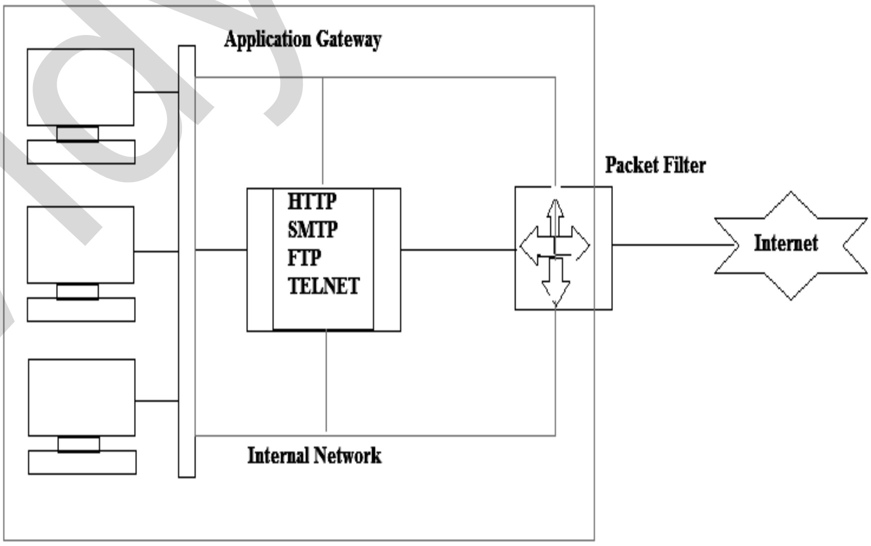
Q.5(b) Write a note on implementing firewall. [8]

(A)

- A firewall is a combination of packet filter and application level gateway. Based on these, there are three types of configurations –
  1) Screened host firewall, Single-Homed Bastion
  2) Screened host firewall, Dual-Homed Bastion
  3) Screened subnet firewall

1) Screened host Firewall, Single-Homed Bastion –

- Here, the firewall configuration consists of two parts – a packet filter router and an application level gateway.
- A packet filter router ensures that the incoming traffic is allowed only if it is intended for the application gateway, by examining the destination address field of each incoming IP packet.
- It also ensures that the outgoing traffic is allowed only it is originated from application level gateway, by examining the source address field of every outgoing IP packet.
- Advantages –
  > It improves security of the network by performing checks at both levels-packet and application level.
- Disadvantages –
  > Internal users are connected to the application gateway as well as packet filter router. Therefore, if the packet filter is somehow successfully attacked and its security compromised, then the whole internal network is exposed to the attacker.

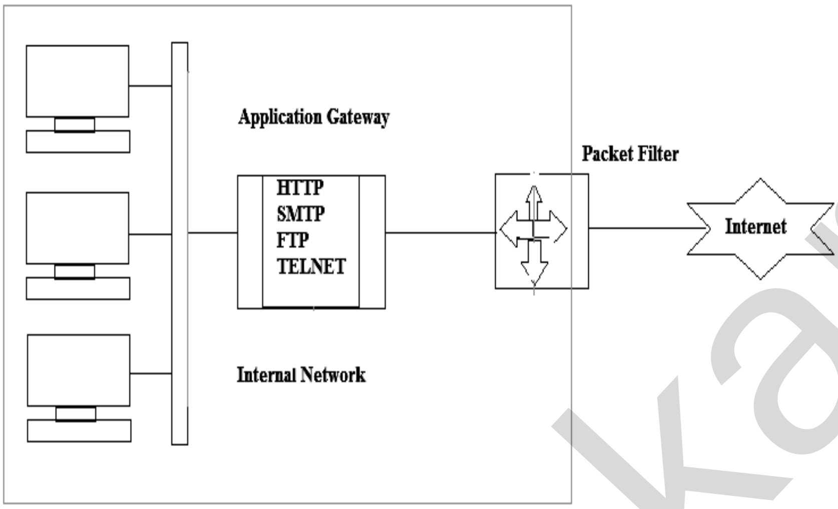


Single Home Bastion

2) Screened host Firewall, Dual-Homed Bastion –

- To overcome the drawback of Screened host Firewall, Single-Homed Bastion, this configuration exists.

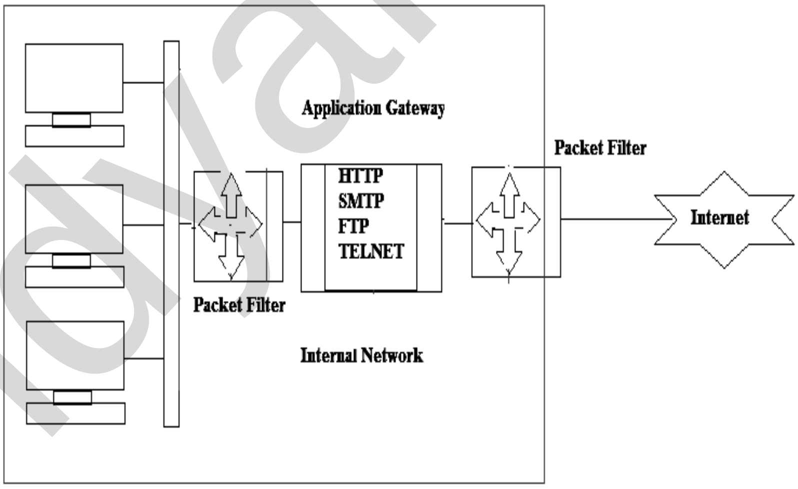
- It is an improvement over the earlier scheme. Here, direct connection between the internal hosts and the packet filter are avoided. Instead, the packet filter connects only to the application gateway, which in turn, has a separate connection with the internal hosts.
- Therefore even though if the packet filter is successfully attacked, only the application gateway is visible to the attacker. The internal hosts are protected.



Dual-Homed Bastion

3) Screened Subnet Firewall –

- This type of configuration offers highest security among the possible configurations.
- In this type, two packet filters are used, one between the Internet and application gateway and other between application gateway and the internal network.
- This configuration achieves 3 levels of security for an attacker to break into.



Screened subnet firewall

Q.5(c) Describe IP security and authentication header mode of IP security with suitable sketch(s). **[8]**

(A)
- The protocol for providing security at the IP level, is called as IP Security (IPSec).
- IPSec encrypts and seals the transport and application layer data during transmission. It also offers integrity protection for the Internet layer. However, the Internet header itself is not encrypted, because of which the intermediate routers can deliver encrypted IPSec messages to the intended recipient.

Authentication Header (AH)

- The authentication Header (AH) protocol provides support for data integrity and authentication of IP Packets. The data integrity ensures that data inside IP packets is not altered during transit. The authentication service enables an end user to authenticate the user or the application at the other end and decide to accept or reject packets, accordingly. This also prevents the IP spoofing attacks.

Bit 0	8	16	31
Next header	Payload length	Reserved	
Security Parameter Index (SPI)			
Sequence number			
Authentication data (Variable size)			

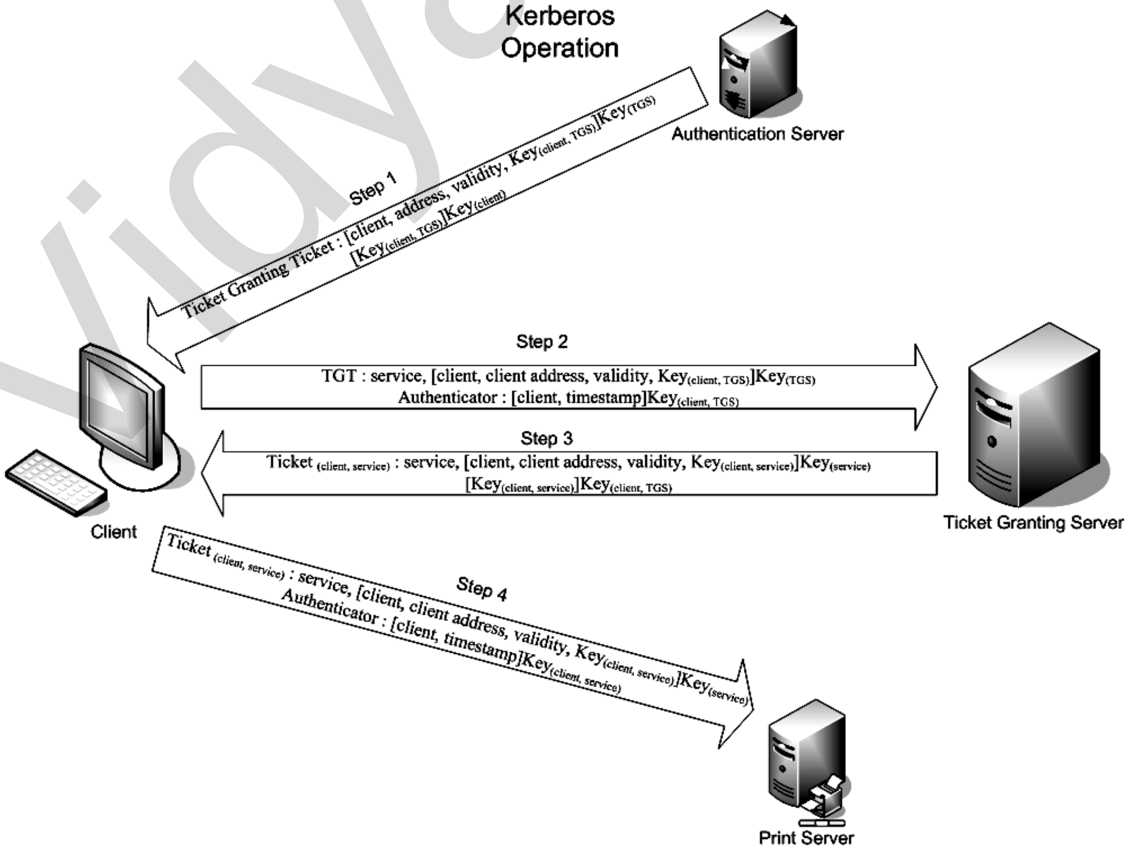
Authentication Header Format

Next Header :	this 8 bit field identifies the type of header that immediately follows the AH.
Payload Length :	this 8 bit field contains the length of the AH in 32-bit words minus 2.
Reserved :	this 16-bit field is reserved for future use.
Security parameter index :	this 32-bit field is used in combination with the source and destination addresses as well as the IPSec protocol used to uniquely identify the Security Association (SA) for the traffic to which a datagram belongs.
Sequence number :	this 32-bit field is used to prevent replay attacks.
Authentication data :	this variable-length field contains the authentication data, called as the Integrity Check Value (ICV), for the datagram.

Q.6 Attempt any FOUR of the following : [16]

Q.6(a) What is Kerberos? Explain with diagram different servers involved in Kerberos. [4]

(A)
- Many real life systems use an authentication protocol called as Kerberos.
- It is designed to allow workstations to use network resources in a secure manner.


Kerberos Operation
Authentication Server
Step 1
Ticket Granting Ticket : [client, address, validity, Key(client, TGS)]Key(TGS)
[Key(client, TGS)]Key(client)
Step 2
TGT : service, [client, client address, validity, Key(client, TGS)]Key(TGS)
Authenticator : [client, timestamp]Key(client, TGS)
Step 3
Ticket (client, service) : service, [client, client address, validity, Key(client, service)]Key(service)
[Key(client, service)]Key(client, TGS)
Client
Ticket Granting Server
Ticket (client, service) : service, [client, client address, validity, Key(client, service)]Key(service)
Authenticator : [client, timestamp]Key(client, service)
Step 4
Print Server

- The servers used in Kerberos are -
  - Authentication Server (AS) : Authenticates the user during Login
  - Ticket Granting Server (TGS) : Issues tickets to certify proof of Identity.
  - Authenticate Server (AS) : the job of AS is to authenticate every user at the login time. AS shares a unique secret password with every user.
  - Ticket Granting Server (TGS) – the job of TGS is to certify to the servers in the network that user is really what she claims to be.

Here's how the logon process works with Kerberos as the authentication method :

To log on to the network, the user provides an account name and password.

1) The Authentication Server (AS) component of the KDC accesses Active Directory user account information to verify the credentials.
2) The KDC grants a Ticket Getting Ticket (TGT) that allows the user to get session tickets to access servers in the domain, without having to enter the credentials again (the TGT is good for 10 hours by default; this expiration period can be configured by the administrator).(Step 1 in the diagram)
3) When the user attempts to access resources on a server in the domain, the TGT is used to make the request. The client presents the TGT to the KDC to obtain a service ticket. (Step 2)
4) The Ticket Granting Service (TGS) component of the KDC authenticates the TGT and then grants a service ticket. The service ticket consists of a ticket and a session key. A service ticket is created for the client and the server that the client wants to access. (Step 3)
5) The client presents the service ticket to create a session with the service on the server. The server uses its key to decrypt the information from the TGS, and the client is authenticated to the server. (Step 4)
6) If mutual authentication is enabled, the server also authenticates to the client.

Q.6(b) Write a note on active directory. **[4]**

(A)
- Active Directory is a special-purpose database.
- The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates.
- Active directory data is hierarchical, replicated and extensible.
- Because it is replicated, one does not need to store dynamic data such as corporate stock prices or CPU performance.
- If your data is machine-specific, store the data in the registry.
- Examples of data stored in the directory include printer queue data, user contact data and network/computer configuration data.
- The Active Directory database consists of objects and attributes.
- Objects and attribute definitions are stored in the Active Directory schema.

Q.6(c) Enlist threats to web security. Describe any three of them in detail. **[4]**

(A) Possible web security threats and their effects -

- **Phishing :** Phishing refers to attacks where the victim is led to believe that he or she is on a legitimate website, when in fact it is just a copy of the real one.
  This attack relies on the fact that anyone can create their own website and any website can look like any other.
- **Web browser exploits :** Cybercriminals have also set up websites that exploit security holes in the web browser. This technique allows them to gain access without the victim's knowledge. This means that a successful attacker who exploits the web browser gets access to private emails, sensitive documents and anything else that that the user running the web browser has access to.

- **Third party add-ons :** The majority of websites require the use of third party add-ons such as Adobe Flash player and Acrobat Reader. Both of these widely used products have become a favorite target for cybercriminals. As more administrators and home users update their machines with the latest security updates and patches for their browsers, as well as the ability to automate the process, it becomes harder to use web browsers as an attack vector. However, although they may be updating their browser software, it is also true that many people forget to update third party add-ons. These third party add-ons are used to push users to other websites that have been compromised.

  The bad guys love to play on two characteristics of human nature: fear and curiosity. In 2009, the rise of 'scareware' has been considerable. Playing on people's fears that their machine has been infected with malware, users are encouraged to download antivirus software. This is nothing but malware that infects the machine and demands payment if the user wants to uninstall the software.
- **Poisoned search engine results :** Another threat is the use of poisoned search engine results. The bad guys create numerous websites for well-known keywords and use these sites to feature high upon on web searches. When a user searches for a particular name or subject and clicks on a poisoned link, he or she is taken to a fake website where they are told to either download software to continue or else malware is downloaded while they are looking at the content.

Q.6(d) Why is there a need for Cyber Law? [4]

(A)

- Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence hsave been grossly misusing this aspect of the internet to perpetuate criminal activities in cyberspace. Hence there is a need for Cyber Law.
- There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are mentioned below.
  - Cyberspace is an intangible dimensions that is to govern and regulate using conventional law.
  - Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minute. Cyberspace handles gigantic traffic every second. Billons of emails are crisscrossing the globes every second, billions of dollars are electronically transferred around the world by banks every day.
  - Image and sound files ensure the confidentiality of information exchanged between cyber-citizens. Softwares worth of Billions of dollars can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any custom duty.
  - Electronic information has become the main object of cyber-crime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.
  - A software course code worth crores of rupees or a movie can be pirated across the globe within hours of their release.
  - Theft of corporal information (e.g. books, papers, CD ROMs) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, and often via telecommunication facilities. Here, the "original" information remains in the "possession" of the "owner" and yet information gets stolen.

Q.6(e) Write a note on Bug Exploits. [4]

(A)
- An exploit is a piece of software, a chunk of data or a sequence of commands that take the advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware or some electronic devices. Such behavior frequently includes things like gaining control of a computer system.
- Criminals can use these bugs to gain unauthorized access to computers or networks or to crash the system to deny services to others.
- Common bugs can be classified as –
  1) **Buffer Overflows :** It occurs when number of bytes or characters input exceeds the maximum number allowed by the programmer.
  2) **Unexpected Input :** It occurs when programmer is not defining what happens if invalid input is entered. This may cause the program to crash or open a way into the system.
  3) **Configuration bugs :** These are the ways of configuring the software that leaves it vulnerable to the penetration.
  4) Major software vendor's regularly release security patches to fix exploitable bugs.

❑ ❑ ❑ ❑ ❑