USN | | | | | | | | | | |

Internal Assesment Test III(scheme and solution) –April. 2018

Sub:	INFORMATION AND NETWORK SECURITY					Sub Code:	10CS835	Branch :	CSE
Date:	/ 05 / 2018	Duration :	90 mins	Max Marks:	50	Sem / Sec:	8 (A,B,C)		OBE

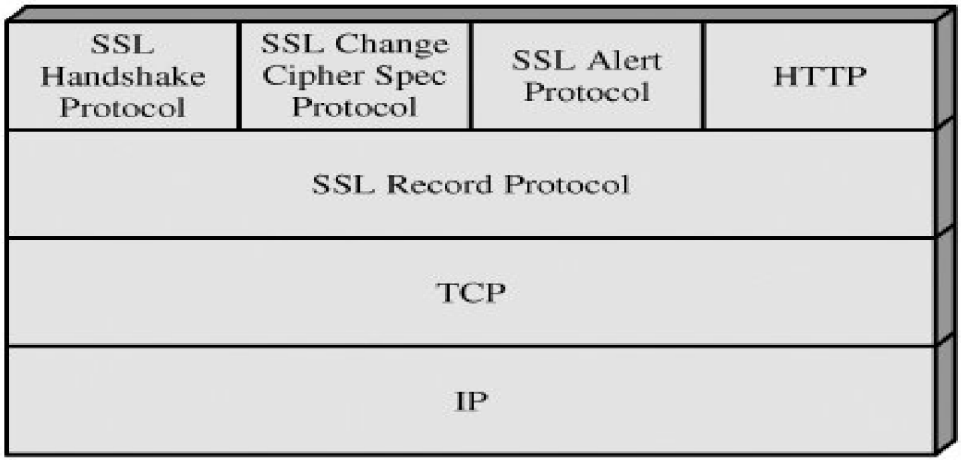
Answer Any FIVE FULL Questions

		MARKS	CO	RBT
1 (a)	Describe SSL architecture? And With a neat diagram explain SSL handshake protocol?	[10]	CO6	L1.L3

SSL Architecture

SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but rather two layers of protocols,

The SSL Record Protocol provides basic security services to various higher-layer protocols. In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL. Three higher-layer protocols are defined as part of SSL: the Handshake Protocol, The Change Cipher Spec Protocol, and Alert Protocol. These SSL-specific protocols are used in the management of SSL exchanges and are examined later in this section.



Two important SSL concepts are the SSL session and the SSL connection, which are define in the specification as follows:

Connection: A connection is a transport (in the OSI layering model definition) that
provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one
session.

Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security

parameters, which can be shared among multiple connections. Sessions are used to
SSL
Handshake Protocol. Thereafter the final ciphertext block from each record is preserved for use as the IV with the following record.

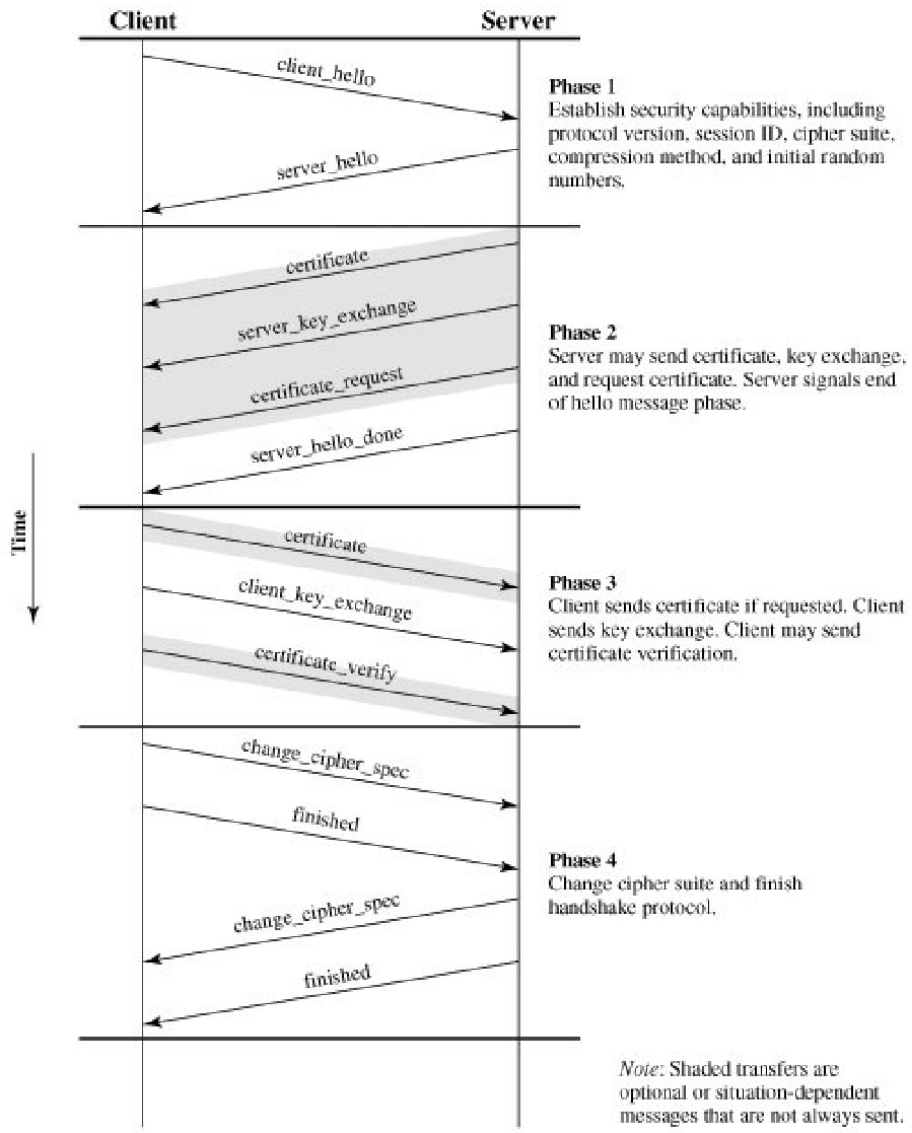
Sequence numbers: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change
cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed 2^{64}- 1.

Handshake Protocol:

The most complex part of SSL is the Handshake Protocol. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The Handshake Protocol is used before any application data is transmitted.

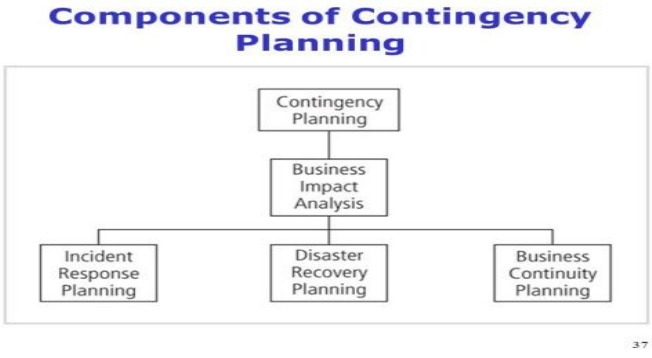
The Handshake Protocol consists of a series of messages exchanged by client and server. All of these have the format shown in Figure 1.5c. Each message has three fields:

Type (1 byte): Indicates one of 10 messages.
Length (3 bytes): The length of the message in bytes.
Content (_ 0 bytes): The parameters associated with this message



Handshake Protocol Action

2 (a) What are the components of contingency planning? Describe briefly the important steps involved in the recovery process after the extent of damage caused by an incident has been assessed? [10] CO1 L1,L2



An incident is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability. An incident response (IR) plan addresses the identification, classification, response, and recovery from an incident. A disaster recovery (DR) plan addresses the preparation for and recovery from a disaster, whether natural or man-made. A

business continuity (BC) plan ensures that critical business functions continue if a catastrophic incident or disaster occurs. The primary functions of these three types of planning are as follows:
The IR plan focuses on immediate response, but if the attack escalates or is disastrous
(e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery
and the BC plan.

The DR plan typically focuses on restoring systems at the original site after disasters
occur, and as such is closely associated with the BC plan.

The BC plan occurs concurrently with the DR plan when the damage is major or ongoing, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

RECOVERY
Full recovery from an incident requires that you perform the following:

1. Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
2. Address the safeguards that failed to stop or limit the incident, or were missing from the system in the first place. Install, replace, or upgrade them.
3. Evaluate monitoring capabilities (if present). Improve their detection and reporting
methods, or simply install new monitoring capabilities.
4. Restore the data from backups. See the Technical Details boxes on the following topics for more information:
(1) data storage and management,
(2) system backups and recovery,
(3) redundant array of independent disks (RAID).
Restoration requires the IR team
to understand the backup strategy used by the organization, restore the data contained in
backups, and then recreate the data that were created or modified since the last backup.

5. Restore the services and processes in use. Compromised services and processes must be examined, cleaned, and then restored. If services or processes were interrupted during
the process of regaining control of the systems, they need to be brought back online.

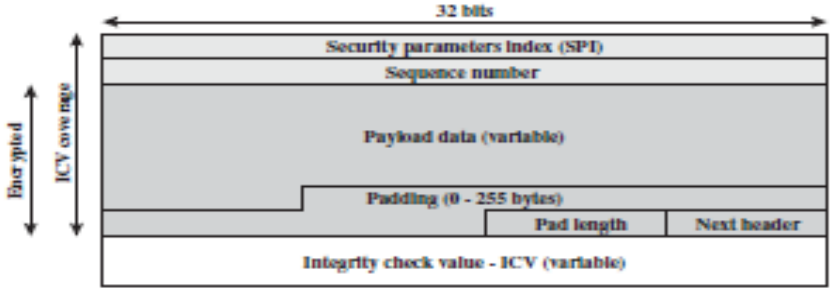
6. Continuously monitor the system. If an incident happened once, it can easily happen
again. Just because the incident is over doesn't mean the organization is in the clear.
Hackers frequently boast of their abilities in chat rooms and dare their peers to match
their efforts. If word gets out, others may be tempted to try their hands at the same or

different attacks. It is therefore important to maintain vigilance during the entire IR
process.
7. Restore the confidence of the organization's communities of interest. It may be advisable to issue a short memorandum that outlines the incident and assures everyone that it was handled and the damage controlled. If the incident was minor, say so. If the incident was major or severely damaged the systems or data, reassure the users that they can expect operations to return to normal shortly. The objective is not to placate or lie, but to prevent panic or confusion from causing additional disruptions to the operations of
the organization.

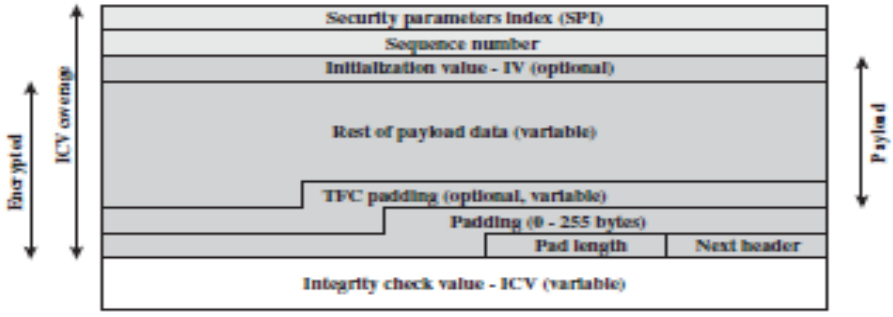
3 (a) Explain the format of an ESP packet in IP security. [8] CO6 L2

Security Parameters Index (32 bits): Identifies a security association.

- **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0–255 bytes):** The purpose of this field is discussed later.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).



(a) Top-level format of an ESP Packet



(b) Substructure of payload data

Figure 8.5 ESP Packet Format

(b) List out the benefits of IPSEC. [2] CO6 L1

Benefits of IPsec

Some of the benefits of IPsec:

• When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.Traffic within a company or workgroup does not incur the overhead of security-related processing.
• IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
• IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.There is no need to change software on a user or server system\ when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.
• IPsec can be transparent to end users.There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
• IPsec can provide security for individual users if needed.This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

4 (a)	Explain the overall operation of secure socket layer record protocol, in detail? List the differences between SSL and TLS protocols?	[10]	CO6	L2

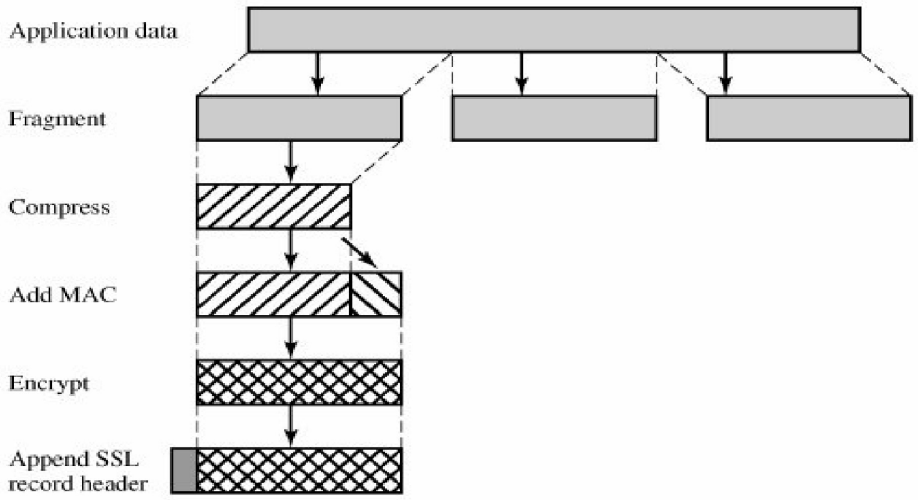
SSL Record Protocol

The SSL Record Protocol provides two services for SSL connections:

Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

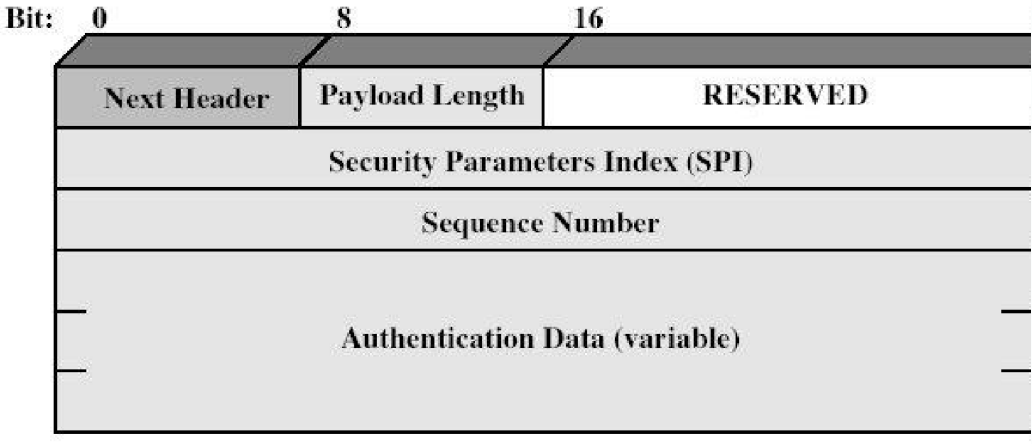
the overall operation of the SSL Record Protocol. The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data are decrypted, verified, decompressed, and reassembled and then delivered to higher-level users.



The first step is **fragmentation**. Each upper-layer message is fragmented into blocks of 2^{14} bytes (16384 bytes) or less. Next, **compression** is optionally applied. Compression must be lossless and may not increase the content length by more than 1024 bytes.
In SSLv3 (as well as the current version of TLS), no compression algorithm is specified, so the default compression algorithm is null. The next step in processing is to compute a **message authentication code** over the compressed data. For this purpose, a shared secret key is used.

The final step of SSL Record Protocol processing is to prepend a header, consisting of the following fields:
Content Type (8 bits): The higher layer protocol used to process the enclosed fragment.
Major Version (8 bits): Indicates major version of SSL in use. For SSLv3, the value is 3.
Minor Version (8 bits): Indicates minor version in use. For SSLv3, the value is 0.
Compressed Length (16 bits): The length in bytes of the plaintext fragment (or compressed fragment if compression is used). The maximum value is $2^{14} + 2048$.

5 (a) Explain the general structure of IPSEC authentication header. Describe how anti reply service is supported. [10] | CO4 | L1,L3



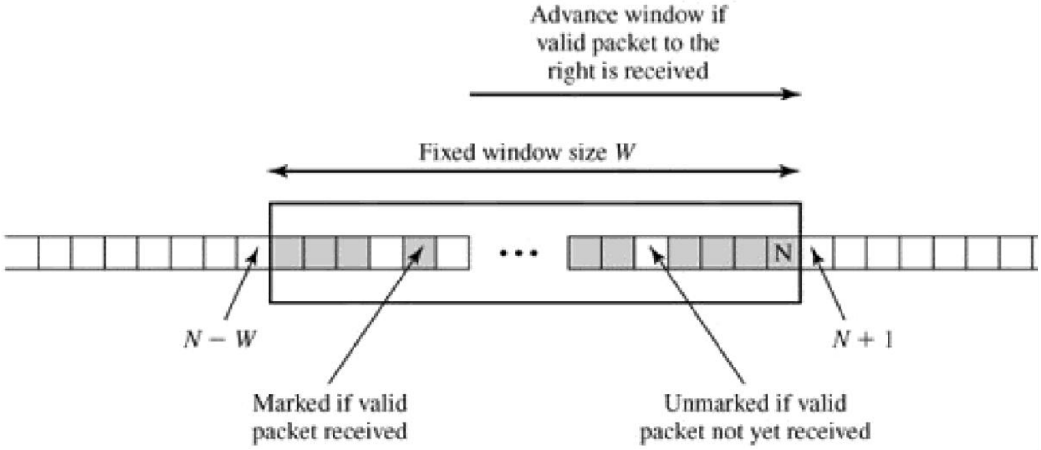
The Authentication Header consists of the following field:

- **Next Header (8 bits):** Identifies the type of header immediately following this header.
- **Payload Length (8 bits):** Length of Authentication Header in 32-bit words, minus 2.

For example, the default length of the authentication data field is 96 bits, or three 32- bit words. With a three-word fixed header, there are a total of six words in the header, and the Payload Length field has a value of 4

- **Reserved (16 bits):** For future use.
- **Security Parameters Index (32 bits):** Identifies a security association
- **Sequence Number (32 bits):** A monotonically increasing counter value, discussed later.
- **Authentication Data (variable):** A variable-length field (must be an integral number. of 32-bit words) that contains the Integrity Check Value (ICV), or MAC, for this packet, discussed later.

Anti-Replay Service: A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The Sequence Number field is designed to thwart such attacks.



Anti Replay Mechanism

When a new SA is established, the **sender** initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field. Thus, the

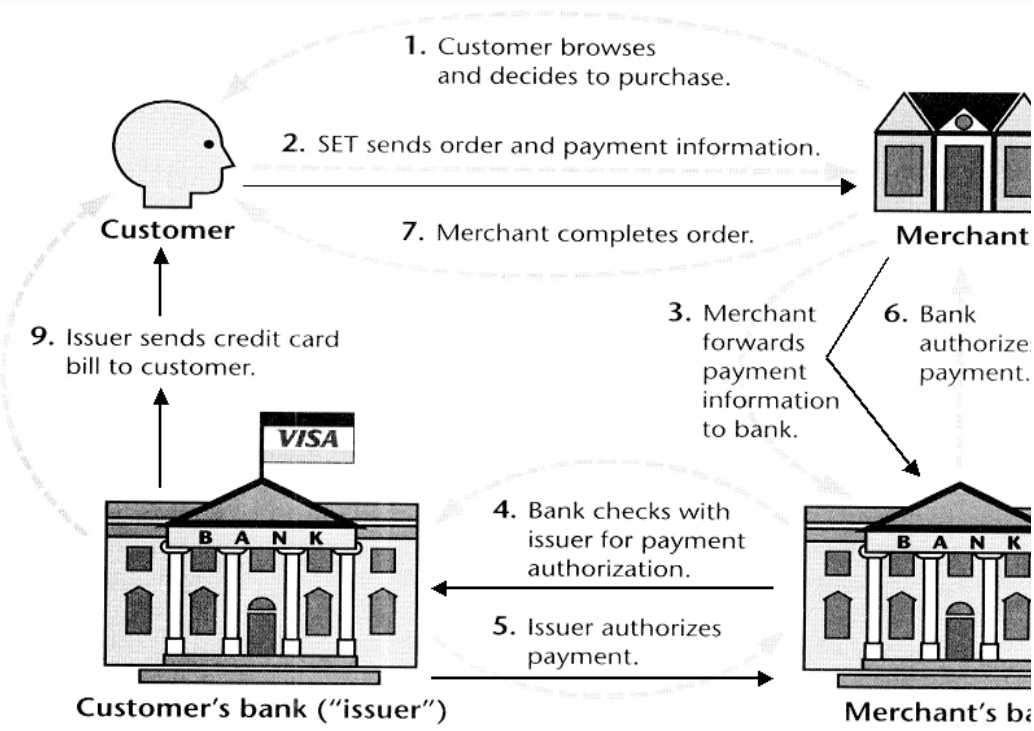
first value to be used is 1. If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past 2 32 - 1 back to zero. Otherwise, there would be multiple valid packets with the same sequence number. If the limit of 2 32 -1 is reached, the sender should terminate this SA and negotiate a new SA with a new key.

Because IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered. Therefore, the IPSec authentication document dictates that the **receiver** should implement a window of size W, with a default of $W = 64$. The right edge of the window represents the highest sequence number, N, so far received for a valid packet. For any packet with a sequence number in the range from $N - W + 1$ to N that has been correctly received (i.e., properly authenticated), the corresponding slot in the window is marked (Figure). Inbound processing proceeds as follows when a packet is received:

- ➢ If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
- ➢ If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
- ➢ If the received packet is to the left of the window, or if authentication fails, the packet is discarded; this is an auditable event.

6 (a) With a block diagram explain secure electronic transaction (SET)? Explain what is dual signature and what is its purpose in SET? [10] CO6 L2

A good way to begin our discussion of SET is to look at the business requirements for SET, its key features, and the participants in SET transactions.



SET TRANSACTIONS

Requirements:
The SET specification lists the following business requirements for secure payment
processing with credit cards over the Internet and other networks:

Provide confidentiality of payment and ordering information:
It is necessary toassure cardholders that this information is safe and accessible only to the intendedrecipient. Confidentiality also reduces the risk of fraud by either party to the transaction or by malicious third parties. SET uses encryption to provide confidentiality.

Ensure the integrity of all transmitted data: That is, ensure that no changes in content occur during transmission of SET messages. Digital signatures are used to
provide integrity.

Provide authentication that a cardholder is a legitimate user of a credit card account: A mechanism that links a cardholder to a specific account number reduces
the incidence of fraud and the overall cost of payment processing. Digital signatures
and certificates are used to verify that a cardholder is a legitimate user of a valid account.

Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution: This is the complement to the
preceding requirement. Cardholders need to be able to identify merchants with whom
they can conduct secure transactions. Again, digital signatures and certificates are

used.

Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction: SET is a well-tested specification based on highly secure cryptographic algorithms and protocols.

Create a protocol that neither depends on transport security mechanisms nor
prevents their use: SET can securely operate over a "raw" TCP/IP stack. However,
SET does not interfere with the use of other security mechanisms, such as IPSec and
SSL/TLS.

Facilitate and encourage interoperability among software and network providers: The SET protocols and formats are independent of hardware platform,
operating system, and Web software.

Key Features of SET

To meet the requirements just outlined, SET incorporates the following features:

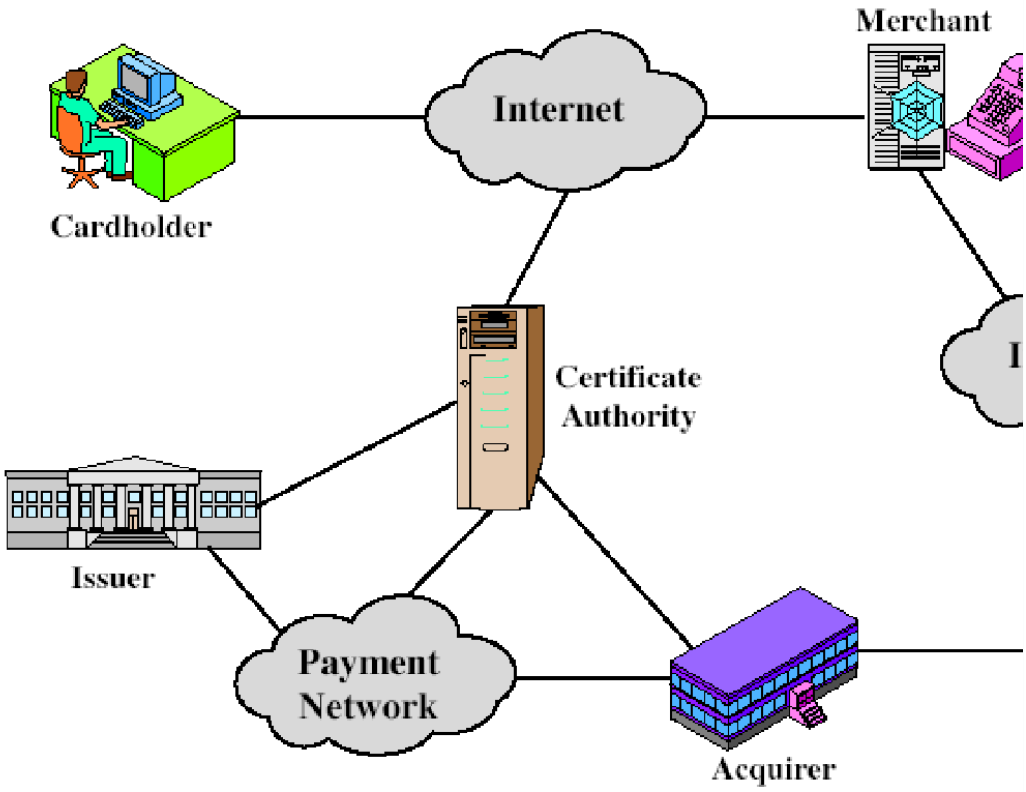
Confidentiality of information:
Cardholder account and payment information is secured as it travels across the network. An interesting and important feature of SET is that it prevents the merchant from learning the cardholder's credit card number; this is only provided to the issuing bank. Conventional encryption by DES is used to provide confidentiality.

Integrity of data:
Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. SET guarantees that these message contents are not altered in transit. RSA digital signatures, using SHA-1 hash codes, provide message integrity. Certain messages are also protected by HMAC using SHA-1.

Cardholder account authentication: SET enables merchants to verify that a cardholder is a legitimate user of a valid card account number. SET uses X.509v3
digital certificates with RSA signatures for this purpose.

Merchant authentication: SET enables cardholders to verify that a merchant has a
relationship with a financial institution allowing it to accept payment cards. SET uses X.509v3 digital certificates with RSA signatures for this purpose. Note that unlike IPSec and SSL/TLS, SET provides only one choice for each cryptographic algorithm. This makes sense, because SET is a single application with a single set of requirements, whereas IPSec and SSL/TLS are intended to support a range of applications.

SET Participants:



Cardholder: In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.

Merchant: A merchant is a person or organization that has goods or services to sell to the cardholder. Typically, these goods and services are offered via a Web site or by electronic mmail. A merchant that accepts payment cards must have a relationship with an acquirer.

Issuer: This is a financial institution, such as a bank, that provides the cardholder with the payment card. Typically, accounts are applied for and opened by mail or in person.

Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.

Acquirer: This is a financial institution that establishes an account with a merchant and

processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that a given card account is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account.

Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer.

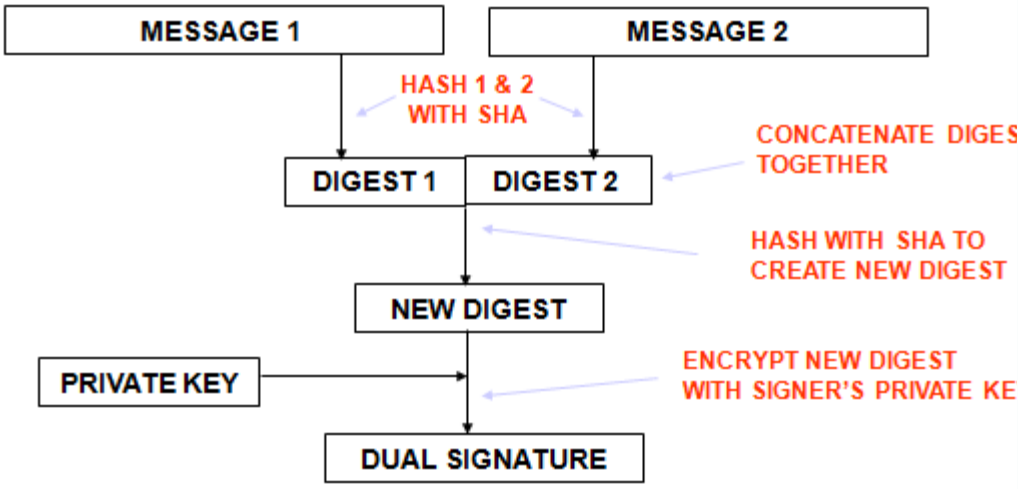
Payment gateway: This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

Certification authority (CA): This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose.

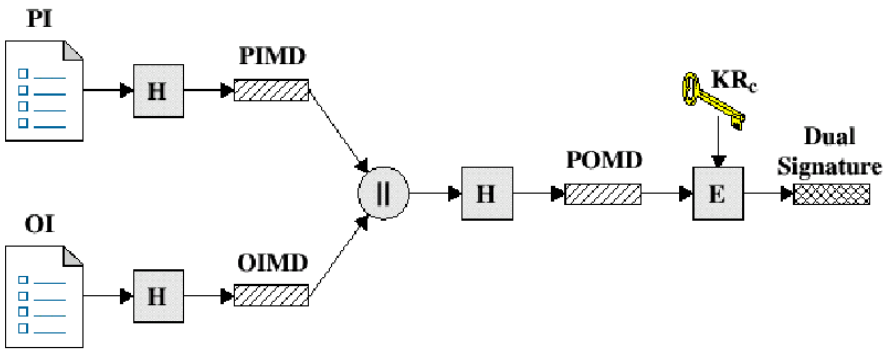
DUAL SIGNATURE FOR SET

- Concept: Link Two Messages Intended for Two Different Receivers:
  - Order Information (OI): Customer to Merchant
  - Payment Information (PI): Customer to Bank
- Goal: Limit Information to A "Need-to-Know" Basis:
  - Merchant does not need credit card number.
  - Bank does not need details of customer order.
  - Afford the customer extra protection in terms of privacy by keeping these items separate.

- Links two messages securely but allows only one party to read each.



DUAL SIGNATURE



- The operation for dual signature is as follows:
  - Take the hash (SHA-1) of the payment and order information.
  - These two hash values are concatenated [H(PI) || H(OI)] and then the result is hashed.
  - **Customer encrypts the final hash with a private key creating the dual signature**
  - DS = E_{KRC} [H(H(PI) || H(OI))]

7 (a) With a block schematic diagram explain how policies, standards, practices, procedures and guidelines are related? Mention the applications of IPSec? [6+4] CO1, CO4 L2

Policies are put in place to support the mission, vision, and strategic planning of an organization.
The **mission** of an organization is a written statement of an organization's purpose. The
vision of an organization is a written statement about the organization's goals—where will The organization be in five years? In ten? Strategic planning is the process of moving the organization toward its vision.The meaning of the term **security policy** depends on the context in which it is used. Governmental agencies view security policy in terms of national security and national policies to deal with foreign states. A security policy can also communicate a credit card

agency's method for processing credit card numbers. In general, a security policy is a set of rules that protect an organization's assets. An **information security policy** provides rules for the protection of the information assets of the organization.

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

For a policy to be effective and thus legally enforceable, it must meet the following criteria:

Dissemination (distribution)—The organization must be able to demonstrate that the
policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution

Review (reading)—The organization must be able to demonstrate that it disseminated
the document in an intelligible form, including versions for illiterate, non-English reading,
and reading-impaired employees. Common techniques include recording the policy
in English and other languages.

Comprehension (understanding)—The organization must be able to demonstrate the employee understood the requirements and content of the policy. Common techniques
include quizzes and other assessments.

Compliance (agreement)—The organization must be able to demonstrate that the employee agrees to comply with the policy, through act or affirmation. Common techniques include logon banners which require a specific action (mouse click or keystroke)to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

Uniform enforcement—The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

APPLICATIONS OF IPSEC

Applications of IPsec

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

• **Secure branch office connectivity over the Internet:** A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

• **Secure remote access over the Internet:** An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network.This reduces the cost of toll charges for traveling employees and telecommuters.

• **Establishing extranet and intranet connectivity with partners:** IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

• **Enhancing electronic commerce security:** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.