CMR INSTITUTE OF TECHNOLOGY

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

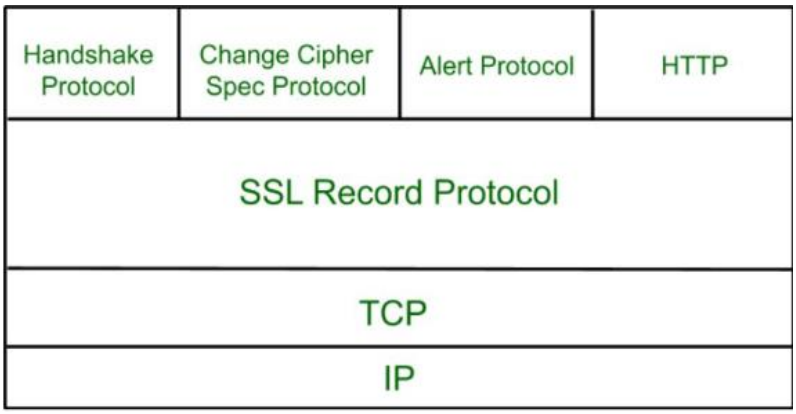
Internal Assesment Test-I								
Sub:	Network Security						Code:	21EC732
Date :	16/10/2024	Duration:	90 mins	Max Marks:	50	Sem: 7th	Branch:	ECE(A,B,C,D)
Answer any **FIVE FULL** Questions								

		Marks	OBE CO	OBE RBT
1.a)	How can a client giving instructions to a stockbroker and later denying those instructions lead to disputes, and what measures can be put in place to prevent misunderstandings or false claims in such situations?" Answer: **Non-repudiation** refers to the ability to ensure that a party cannot deny the authenticity of their actions or instructions. In the case of a client giving trade instructions to a broker, non-repudiation measures are crucial to prevent disputes by creating undeniable proof that specific instructions were indeed authorized by the client. **Digital Signatures**: Implementing digital signatures on trade instructions ensures that each instruction is uniquely signed by the client. This cryptographic signature is impossible to forge without the client's private key, ensuring that the client cannot later deny having authorized the instruction.	[06]	CO1	L3
b)	Draw a table illustrating the relation between security services and security mechanisms. Answer:	[04]	CO2	L1

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic Padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

2.a)	What is SSL, and how does it provide secure communication over the internet? Draw the SSL Protocol stack. Answer: **SSL (Secure Sockets Layer)** is a standard security protocol for establishing encrypted links between a web server and a web browser. This encryption ensures that all data passed between the server and browser remains private and secure. SSL uses digital certificates to verify the identity of the server. This certificate is issued by a trusted Certificate Authority (CA) and serves as proof that the website is legitimate. SSL includes mechanisms to ensure data integrity, which means that any data sent or received cannot be tampered with during transit. This is achieved through	[04]	CO1	L1

cryptographic hashes, which act as fingerprints for the data.



b) List and briefly define the parameters that define an SSL session state. [06] CO1 L3

Answer: A session state is defined by the following parameters.

Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.

Peer certificate: An X509.v3 certificate of the peer. This element of the state may be null.

Compression method: The algorithm used to compress data prior to encryption.

Cipher spec: Specifies the bulk data encryption algorithm (such as null, AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the `hash_size`.

Master secret: 48-byte secret shared between the client and the server.

Is resumable: A flag indicating whether the session can be used to initiate new connections.

3. What are the key web security considerations? Discuss common web threats, their possible consequences, and the most effective countermeasures to safeguard against these threats. [10] CO1 L2

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

4. Discuss the four principles of security in detail, each with an example. [10] CO L

Answer: The four fundamental principles of security are **Confidentiality**, **Integrity**, **Availability**, and **Non-repudiation**.

Confidentiality protects sensitive data from unauthorized access and disclosure.
Example: Online banking services use encryption to protect customer information, such as account balances and transaction details, so that only the account holder and authorized bank personnel can view it. Unauthorized parties attempting to access this information will see only encrypted data, which they cannot interpret without the proper decryption key.
I**ntegrity** ensures that data remains accurate, consistent, and unaltered from its original form. It prevents unauthorized changes to information, whether intentional or accidental.
Example: During an online transaction, integrity is maintained by using a hashing algorithm. The transaction details are hashed before sending, and the hash is verified by the recipient. If an attacker modifies the data in transit, the hash wills no longer match, alerting the system to a potential data tampering attempt.
Availability ensures that information and resources are accessible to authorized users when they are needed.
Example: Companies use redundant servers and backup systems to ensure website availability. For instance, if a primary server goes down, a backup server automatically takes over to keep the website online.
Non-repudiation ensures that a party cannot deny the authenticity of their actions, such as sending a message or approving a transaction.
Example: In e-commerce, digital signatures provide non-repudiation. When a customer approves a transaction with a digital signature, they are legally bound by that signature.
Authentication is the process of verifying that an individual, device, or system is who or what it claims to be.

5. Define security attack, security service, and security mechanism. Classify the different types of security attacks and explain them in detail with the help of clear diagrams. [10] CO L

Security attack: Any action that compromises the security of information owned by an organization.
Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
A useful means of classifying security attacks is in terms of passive attacks and active attacks.
A passive attack attempts to learn or make use of information from the system but does not affect system resources.
An active attack attempts to alter system resources or affect their operation.
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.
Two types of passive attacks are **release of message contents** and **traffic analysis.**

- The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- A second type of passive attack, traffic analysis, is subtler. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place

.Active attacks involve some modification of the data stream or the creation of a

false stream and can be subdivided into four categories:
1. Masquerade, 2. replay, 3. modification of messages, and 4. denial of service.
A masquerade takes place when one entity pretends to be a different entity.
Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
Denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).

6.a) What is the difference between an SSL connection and an SSL session? [03] CO L

An **SSL connection** is a temporary, peer-to-peer communication link established using the SSL/TLS protocol. It is created when a client (e.g., a web browser) connects to a server (e.g., a website), and they go through a handshake process to establish encryption and other security parameters.
An **SSL session** is a set of security parameters that can be reused across multiple SSL connections. It is established during the SSL handshake and can be maintained for a certain period to avoid repeating the full handshake for each new connection.

b) Explain briefly about various parameters involved in an SSL connection. [07] CO L

Answer:
Server and client random: Byte sequences that are chosen by the server and client for each connection.
•**Server write MAC secret:** The secret key used in MAC operations on data sent by the server.
• **Client write MAC secret:** The secret key used in MAC operations on data sent by the client.
•**Server write key:** The secret encryption key for data encrypted by the server and decrypted by the client.
•**Client write key:** The symmetric encryption key for data encrypted by the client and decrypted by the server.
•**Initialization vectors:** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key.
•**Sequence numbers:** Each party maintains separate sequence numbers for transmitted and Received.

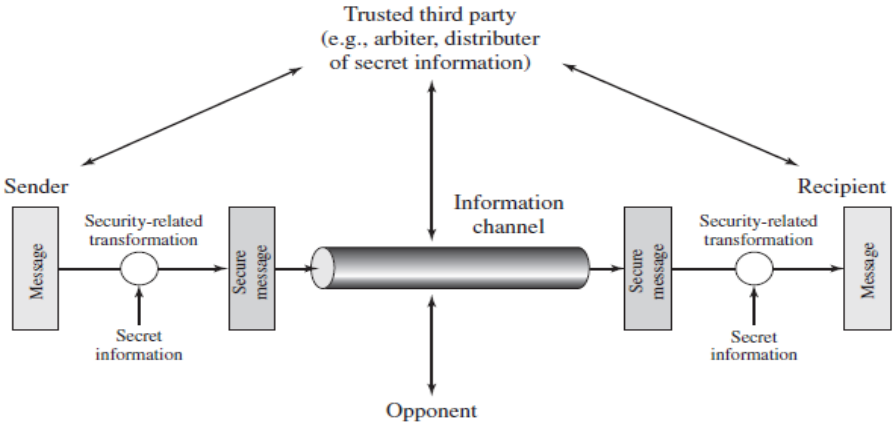
7.a) How can unauthorized modification of messages during a bank transaction lead to financial loss, and what essential security mechanisms are required to prevent such tampering? Discuss the role of integrity protection and the specific cryptographic techniques that ensure secure and unaltered communication in financial systems [05] CO L

Ans: Unauthorized modification of messages during a bank transaction often referred to as message tampering or data integrity attacks, can lead to severe financial losses. In a typical bank transaction, any modification to the transaction amount, recipient details, or account information can result in unauthorized funds transfer or incorrect financial records.
Message Authentication Codes (MAC): A MAC is a cryptographic technique that appends a short piece of information to the message. It is generated by combining the message data with a shared secret key. Both sender and receiver can verify the integrity of the message by recalculating and comparing the MAC.
Digital Signatures: Digital signatures use public-key cryptography to authenticate messages. The sender generates a signature using their private key, which can be verified by the recipient using the sender's public key. This not only authenticates the sender but also guarantees message integrity, as any

tampering would invalidate the signature.

Encryption: Symmetric and asymmetric encryption ensures that transaction messages remain confidential and unreadable to unauthorized parties.

b) Discuss Network security model with neat illustration and explain the components of the model. [05] CO L



The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. Security aspects come into play when it is necessary to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.
2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
3. A trusted third party may be may be responsible for distributing the secret information.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The Algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.