Question no 1

Discussion Board

a) Please give an example of a hardware opponent which can access any message sent from a sender and a receiver.

➔ The modem is one of the examples of a hardware opponent which can access any message sent from a sender and a receiver.

b) What is the organization NSA? How does it affect the security industry?

➔ The organization NSA stands for National Security Agency which leads the US government as an intelligence agency that is responsible for cryptographic and communication intelligence. It provides the critical information needed to defend the country, save lives, and advance U.S. goals and alliances globally.

c) NSA prefers exportable security algorithms easier to break or harder to break.

➔ NSA prefers harder to break.

Question no.2

Briefly describe the 6 security building blocks. Which block is required for eCommerce?

The 6 security building blocks are:

i) Identification and Authentication: It presents the identity of an individual in a transaction means identification. Authentication verifies the identity of various participants (users/systems) exchanging the information.

ii) Authorization: Rather than intercepting other messages or files, the hacker sends the message or file as the manager to the user. The user accepts the message with the knowledge that the message or file has been sent by the manager and updates its authorization file accordingly. It deals with the question of whether you are communicating with a specific process. It helps in the verification of the user's ability of performance and what information the user can access.

iii) Integrity: One user(A) transmits the file to another user(B) when the unauthorized third person(C) can add or delete the file sent by the user. It shows as the A user sends the file to the B user without the notification that the file has been changed by user C. It ensures the correctness of the content and source of a piece of information.

iv) Confidentially: When user A transfers a file containing sensitive information that is to be protected from disclosure other than user B, read by user C is unauthorized and manages to monitor the transmission and capture a copy of the file during transmission. It can be referred to as privacy. It helps to keep information secret from everyone but those who are authorized to see it. Ear drooping causes a lack of confidence.

v) Auditing: It helps to track the day-to-day operation of the corporate network which allows an organization to reconstruct what happened if a transaction is compromised. It also relies on the previous 4 blocks.

vi) Non-Repudiation: A message or file is sent to the customer to a stockbroker with the information of various transactions. The customer then denies sending the message, and the investments lose value. It helps to prove that the sender did indeed send the transaction and that the recipient received the same transaction. This block cannot occur until the previous five security building blocks are in place. It prevents the denial of previous commitments or actions.

Every block is required for eCommerce but the one building block which provides security to eCommerce is non-Repudiation.

Question no 3

Virus

a) What is the difference between a worm and a virus

Worm	Virus
It must be triggered by the activation of their host.	It stand-alone malicious programs that can self-replicate and propagate independently.
It can infect files	It can't infect the files.

It spread slowly.	It has lower latency.

b) Where is the boot virus stored?
➔ It is stored in the boot sector of floppy disks or the primary boot record of hard disks.

c) Can a virus attach to data?
➔ Yes, the virus can attach to data.

Question no.4

The 1997 IEEE paper "Encryption", which was submitted by Fred Piper at European Conference on Security and Detection, has this statement

Thus, anyone sending a message over a public network or storing it on a database should ask themselves:

* Am I happy for everyone else to know its contents?

If their answer is YES then there may be no problem, but if it

is not then they may need to ask:

* How much am I prepared to pay to stop them?

➔ The answer is no. I can stop them by having security and we can create groups to send the message to the specific person.

 * Am I allowed to stop them?
➔ Yes, we are allowed to stop them.

For transmitted messages the sender may also ask:

 * Do I need acknowledgment of delivery?
➔ yes, I need it.
Similarly, anyone receiving a message over a network will need to ask themselves the following:

 * Am I confident to know the identity of the sender?
➔ I need to have an idea who sends the message without identification it's better not to open it.

 * Am I happy that the message I have received is identical to the one which the originator sent?
➔ Yes, I am happy to see the message from the identical person.

 * Am I concerned that the sender may later deny sending this message and/or claim to have sent a different one?

➔ I need to have proof of the message is sent by the person.

These are the statement and my thoughts regarding the answer.

Question no .5

Please answer these questions related to security Service Links

a) Which security service can assure a sender that people other than the receiver cannot see the content of a message sent from the sender?
   ➔ message encryption.
b) Which security service can provide the identity of the sender?
   ➔ Public key cryptography and hashing.
c) Which security service can assure the receiver that the message the receiver has received is identical to the one which the originator sent?
   ➔ Non-repudiation.
d) Which security service can assure the receiver that the sender cannot deny sending a message and/or claim to have sent a different one?
   ➔ Non-repudiation.

Question no. 6

What is the difference between encryption and encoding

➔

Encryption	Encoding
It is the practice of concealing data or information in such a way that it appears random and can be accessed by authorized parties only.	It is the practice of secu information transforming it into secured format transmission ac insecure networks.
Key is used which can be secret or public.	The key is not used.
Changing of old data to new data is called ciphertext.	Old data changes to a format.

Question no. 7

Please draw a diagram to show the tree structure relationship among the following security technologies

Obfuscation

Information security

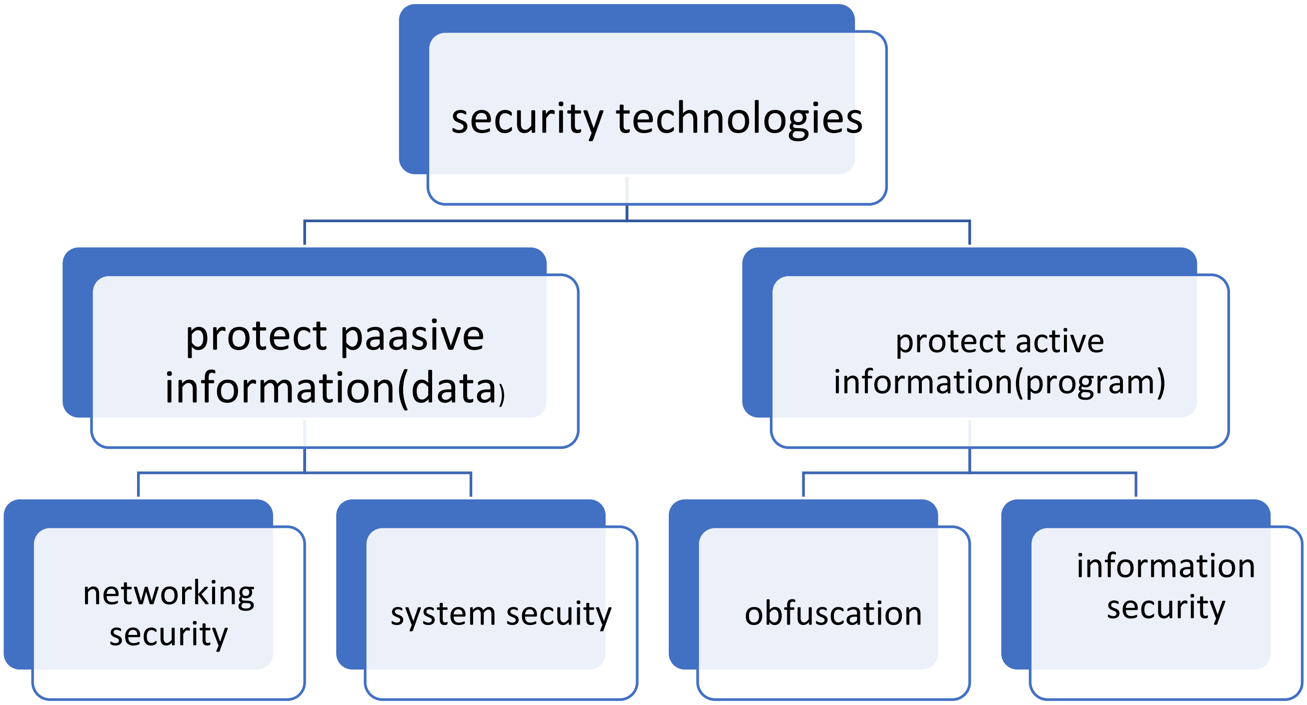
Network security

Protect passive information (data)

Protect active information (program)

System security (i.e., Network Access Security)

➔



Question no. 8

Please map the security services and key concepts

Authentication 1. assessment
Authorization 2. modify
Data integrity 3. authorize
Data confidentiality 4. read by sender/receiver
Non-repudiation 5. read by hacker
Privacy 6. deny
Auditing 7. Proof

➔ Authentication ➔ read by sender/receiver
Authorization ➔ authorize
Data integrity➔ modify
Data confidentiality ➔ read by hacker
Non- repudiation ➔ deny
Privacy ➔ proof
Auditing ➔ assessment

Question no.9

Multiple choices

a) Which US government agency is the Big Brother which controls whether a security algorithm can be exported?

1. FBI
2. CIA
3. NSA

➔ 3. NSA

b) What are the three aspects of information security?

1. Network Attack, System Attack, and Virus Attack
2. Security mechanism, security service, and security attack
3. Asymmetric Key Cryptography, Symmetric Key Cryptography, and Data Mining
4. Authentication, Confidentiality, and Integrity
5. ➔ 4 Authentication, Confidentiality, and Integrity

c) What are the two major types of security attacks?

1. Network Security Attack, and Virus Attack
2. System Security Attack, and Virus Attack
3. Network Security Attack and System Security Attack
4. None of above
5. ➔ 3 Network Security Attacks and System Security Attacks

d) Which of the following data does not need to be sent via an out-of-band channel?

1. public key
2. secret key
3. key for creating MAC

➔1

e) Who invented public key cryptography?

1. Ray Ozzie
2. Diff Whit
3. Phil Zimmermann
4. Ron Rivest
5. Len Adleman

➔ 2 Diff Whit

f) Postcards put inside a see-through windows envelope achieves what service?

1. Authentication
2. Confidentiality
3. Integrity
4. Authorization
5. Auditing
6. Non-repudiation

➔ 6

g) Human DNA corresponds to which of the following electronic security mechanism?

1. Public key
2. Private key
3. Message Digest
4. Symmetric key
5. Digital certificate

➔ 1

h) Passport corresponds to which of the following electronic security mechanism?

1. Public key
2. Digital certificate
3. Private key
4. Message Digest
5. Symmetric key

➔ 2.