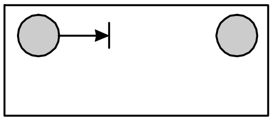
Model Question Paper
Cryptography, Computer Security plus Disaster Recovery (MB3H2IT)

Section A: Basic Concepts (30 Marks)

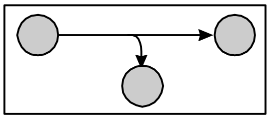
- This section consists of questions with serial number 1 - 30.
- Answer all questions.
- Each question carries one mark.
- Maximum time for answering Section A is 30 Minutes.

1. Which of the following figures of security threat represent ‘modification’?

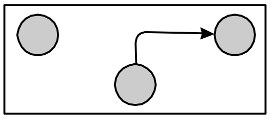
(a)



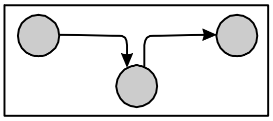
(b)



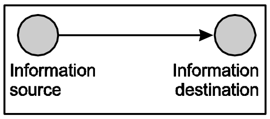
(c)



(d)



(e)



.

2. Which of the following statements is/are **true** about different types of security attacks?

I. Denial of service is a type of active attack which prevents or inhibits the normal use or management of communications facilities.
II. Masquerade is a type of active attack which takes place when one entity pretends to be a different entity.
III. Replay is a type of passive attack which involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

(a) Only (I) above
(b) Only (II) above
(c) Both (I) and (II) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

3. Keplar networks, a trusted third party, wanted to establish a network access security model which may be responsible for distributing the secret information to the two principals while keeping it from any opponent. In this context, which of the following are the basic tasks that Keplar networks should consider in designing security service?

I. Design an algorithm for performing the security-related transformation.
II. Generate secret information to be used with the algorithm.
III. Develop methods for the distribution and sharing of the secret information.
IV. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

(a) Both (I) and (II) above
(b) Both (III) and (IV) above
(c) (I), (II) and (III) above

(d) (II), (III) and (IV) above
(e) All (I), (II), (III) and (IV) above.

4. Which of the following aspects of information security enhance the security of the data processing systems and the information transfers of an organization?

(a) Security recovery
(b) Security attack
(c) Security service
(d) Security prevention
(e) Security identification.

5. Fragmentation is one of the steps in Secure Socket Layer (SSL) record protocol operation. In fragmentation, each upper layer message is fragmented into blocks of

(a) 2^{16} bytes
(b) 2^{14} bytes
(c) 2^{15} bytes
(d) 2^{18} bytes
(e) 2^{20} bytes.

6. Which of the following algorithms is used in Secure Electronic Transaction (SET)?

(a) DES
(b) IDEA
(c) Triple DES
(d) CAST-128
(e) RC5.

7. Which of the following algorithms is used by Pretty Good Privacy (PGP) to provide transparency for e-mail applications?

(a) ZIP
(b) Radix-64 conversion
(c) CAST
(d) DSS
(e) SHA.

8. Which of the following type of firewall is also called as proxy server?

(a) Packet filtering router
(b) Application-level gateway
(c) Circuit-level gateway
(d) Direction-level gateway
(e) Service filtering router.

9. In RSA public-key encryption, if we select two prime numbers, p and q as 7, 13, then find the values of n and $\varphi(n)$.

(a) $n = 91,\ \varphi(n) = 72$
(b) $n = 72,\ \varphi(n) = 91$
(c) $n = 91,\ \varphi(n) = 112$
(d) $n = 112,\ \varphi(n) = 91$
(e) $n = 72,\ \varphi(n) = 112$.

10. What is the output of SHA-1 algorithm?

(a) 32-bit message digest
(b) 64-bit message digest
(c) 84-bit message digest
(d) 128-bit message digest
(e) 160-bit message digest.

11. The default automated key management protocol for IPSec is referred to as Internet Security Association and

Key Management Protocol (ISAKMP). In ISAKMP header format, what is the size of Message ID field?

(a) 8 bits
(b) 32 bits
(c) 64 bits
(d) 128 bits
(e) 256 bits.

12. Which of the following Internet Security Association and Key Management Protocol (ISAKMP) payload types contain random data used to guarantee liveness during an exchange and protect against replay attacks?

(a) SA payload
(b) Hash payload
(c) Transform payload
(d) Nonce payload
(e) Notification payload.

13. In RSA public-key encryption, which of the following formulae is used to calculate plaintext (M)?

(a) $M=C^d \pmod{n}$

(b) $M=C \times d \pmod{n}$

(c) $M=(C+d) \pmod{n}$

(d) $M=(C/d) \pmod{n}$

(e) $M=(C-d) \pmod{n}$.

14. There are many metrics which are useful for profile-based intrusion detection. For all these metrics some models are used to determine whether current activity fits within acceptable limits. Which of the following statements are **true** about these models?

I. Operational model is used to establish transition probabilities among various states.
II. Markov process model is based on a judgment of what is considered abnormal, rather than an automated analysis of past audit records.
III. Multivariate model is based on correlations between two or more variables.
IV. Time series model focuses on time intervals, looking for sequence of events that happen too rapidly or too slowly.

(a) Both (I) and (II) above
(b) Both (II) and (III) above
(c) Both (III) and (IV) above
(d) (I), (II) and (III) above
(e) (II), (III) and (IV) above.

15. There are several techniques that firewalls use to control access and enforce the site's security policy. Which of the following statements are **true** about the control techniques?

I. Service control controls how particular services are used.
II. Direction control determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
III. User control controls access to a service according to which user is attempting to access it.
IV. Behavior control determines the types of internet services that can be accessed, inbound or outbound.

(a) Both (I) and (II) above
(b) Both (II) and (III) above
(c) Both (III) and (IV) above
(d) (I), (II) and (III) above
(e) (II), (III) and (IV) above.

16. Markov model is represented as a quadruple [*m, A, T, k*]. In this model, *A* represents

(a) State space
(b) Matrix of transition probabilities
(c) Number of states in the model
(d) Number of relations for each state
(e) Order of the model.

17. Which of the following default policies of packet-filtering router increase ease of use for end users, but provides reduced security?

(a) Default = discard
(b) Default = forward
(c) Default = backward
(d) Packet = discard
(e) Packet = forward.

18. A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Which of the following is/are **false** about the characteristics of a bastion host?

I. The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
II. Each proxy runs as a privileged user in a private and secured directory on the bastion host.
III. Each proxy is dependent on other proxies on the bastion host.

(a) Only (I) above
(b) Only (II) above
(c) Both (I) and (II) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

19. There are many metrics which are useful for profile-based intrusion detection. Counter, Gauge, Resource utilization, Interval timer are some of the examples of metrics that are useful for profile-based intrusion detection. Which of the following statements are **true** about these metrics?

I. Counter is a nonnegative integer that may be incremented or decremented until it is reset by management action.
II. Gauge is a nonnegative integer that may be incremented but not decremented until it is reset by management action.
III. Resource utilization is the quantity of resources consumed during a specified period.
IV. Interval timer is the length of time between two related events.

(a) Both (I) and (II) above
(b) Both (II) and (III) above
(c) Both (III) and (IV) above
(d) (I), (II) and (III) above
(e) (II), (III) and (IV) above.

20. Which of the following statements is/are **false** about SMTP/822 scheme?

I. SMTP cannot transmit executable files or other binary objects.
II. SMTP servers may reject mail message over a certain size.
III. SMTP transmits text data that includes national language characters.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (II) and (III) above.

21. Which of the following statements is/are **false** about the classes of intruders?

I. Masquerader is likely to be an insider.
II. Misfeasor is generally an outsider.
III. Clandestine user can be either an outsider or an insider.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (II) and (III) above.

22. Which of the following statements is/are **true** about X.509 authentication service?

I. X.509 defines a framework for the provision of authentication services by the X.500 directory to its users.
II. X.509 standard does not dictate the use of a specific algorithm but recommends RSA.

III. X.509 is based on the use of private-key cryptography and digital signatures.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (II) and (III) above.

23. Pretty Good Privacy (PGP) provides various functions. Which of the following algorithms is used for the function "Compression"?

(a) DSS
(b) CAST
(c) Radix-64 conversion
(d) ZIP
(e) SHA.

24. Content-Transfer-Encoding field can actually take on six values. Which of the following value encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans?

(a) 7 bit
(b) 8 bit
(c) quoted-printable
(d) binary
(e) x-token.

25. The following are the steps done by the Secure Socket Layer (SSL) record protocol in SSL record protocol operation. Arrange the following steps in **correct** order.

I. Collecting application data.
II. Adding Message Authentication Code (MAC).
III. Compression.
IV. Encryption.
V. Fragmentation.
VI. Appending SSL record header.

(a) I-II-III-IV-V-VI
(b) I-V-III-II-IV-VI
(c) I-III-V-II-IV-VI
(d) I-IV-V-III-II-VI
(e) I-III-IV-II-V-VI.

26. In which of the following phases, virus performs the function, which may be harmless such as a message on the screen or harmful such as destructive of programs and data files?

(a) Dormant phase
(b) Propagation phase
(c) Triggering phase
(d) Execution phase
(e) Active phase.

27. Which of the following Kerberos version5 flags tell Ticket-Granting-Server (TGS) that a new ticket-granting ticket with a different network address may be issued based on this ticket-granting ticket?

(a) FORWARDABLE
(b) PROXIABLE
(c) PRE-AUTHENT
(d) HW-AUTHENT
(e) POSTDATED.

28. Encapsulating Security Payload (ESP) provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. In ESP packet format, what is the size of sequence number field?

(a) 8 bits
(b) 16 bits
(c) 32 bits

(d) 64 bits
(e) 128 bits.

29. The default automated key management protocol for IPSec is referred to as Internet Security Association and Key Management Protocol (ISAKMP). Which of the following is/are **true** about ISAKMP exchanges?

I. Informational exchange is used for one-way transmittal of information for Security Association (SA) management.
II. Identity protection exchange expands the base exchange to protect the user's identities.
III. Authentication only exchange is used to perform mutual authentication, without a key exchange.

(a) Only (I) above
(b) Both (I) and (II) above
(c) Both (I) and (III) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

30. Verisign provides three levels or classes of security for public-key certificates. Verisign uses class–II digital IDs for

I. E-banking.
II. Online subscriptions.
III. Software validations.

(a) Only (III) above
(b) Both (I) and (II) above
(c) Both (I) and (III) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

END OF SECTION A

Cryptography, Computer Security plus Disaster Recovery (MB3H2IT)

Section B : Caselets/Problems (50 Marks)

- This section consists of questions with serial number 1 – 5.
- Answer all questions.
- Marks are indicated against each question.
- Detailed explanations/workings should form part of your answer.
- Do not spend more than 110 - 120 minutes on Section B.

Caselet 1

Read the caselet carefully and answer the following questions:

1. Critically analyze the reasons behind choosing PGP by National Security Agency. **(12marks)**

2. If you are the manager of National Security Agency, how do you classify security service? Explain. **(12marks)**

Enforcing Network Security Policy

The National Security Agency with more than 1,000 employees is charged with protecting the nation's public health, safety and environment as well as promoting and securing the common defense. In its daily work, the agency handles and protects various types of sensitive information, which is exchanged both internally and externally. In fact, its security must meet the standards of the National Information Security Management Act (NISMA). The Act requires all federal agencies to put in place an agency-wide program to secure sensitive information as well as the information systems that support agency operations and assets. In addition, many federal agencies whose documents are “sensitive but unclassified” are limited to their security services. The government mandates that national agencies may purchase only security technology that complies with National Information Processing Standard published by the National Institute of Standards and Technology (NIST).

In 2004, the agency was tasked with finding an encryption solution that would meet FIPS 140-2 requirements. The agency had been using WinZip technology, but WinZip could not provide the strength or type of encryption required. Also in keeping with the FIPS 140-2 mandate, the agency was in the process of implementing a Public Key Infrastructure (PKI) to secure its data using X.509 standard digital certificates.

Moreover, WinZip does not enable administrators to control how the product is being used. The agency could neither prevent users from encrypting files nor control how files were encrypted. To make sure that the security was truly bulletproof, security algorithms like DES (Data Encryption Standard) and Triple DES were used. The careful blending of these cutting edge cryptography technologies reduced the chances of a security leak to a minimum.

National agencies are required to evaluate at least three solutions before purchasing an application. Therefore the agency contacted a consultant to help assess possible solutions. The consultant investigated PGP (Pretty Good Privacy), Sigaba, File Assurity and Tumbleweed and he recommended that PGP for providing a solution.

END OF CASELET 1

Caselet 2

Read the caselet carefully and answer the following questions:

3. Explain the types of threats, OFS is likely to face. **(8 marks)**

4. What are the methods available to counteract such types of threats in network security? Explain. **(4 marks)**

Oriental Financial Services (OFS) is a premier financial services provider. OFS employs around 2700 people for its operations. Most of them are busy working for client’s transactions, making payments, dealing with brokerage firms, granting loans and credits, the foreign exchange dealings etc. All these transactions are done online.

Recently the company has seen a report published by the Gartner IT research group, which stated that US financial institutions lost around USD2.4 billion in one year due to fraud, much of which is associated with on-line transactions. The Gartner study was based on a survey of 5,000 Internet users in the US.

In most cases it was not an insider’s job. Thieves stole account numbers and passwords to get into accounts on-line or through telephone banking services. It did not involve face-to-face transactions. Much of the crime was the result of so-called phishing attacks, or e-mail scams that lure users to fake Web sites or that upload key logging applications on users’ PCs.

Frightened with the reports the bank has assessed its online security and to its surprise it has found that the company did not employ any security systems as such.

END OF CASELET 2

5. a. Write Diffie-Hellman key exchange algorithm. **(6 marks)**

b. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root $\alpha = 2$.

i. If user A has public key $Y_A = 9$, what is A's private key X_A ?

ii. If user B has public key $Y_B = 3$, what is the shared secret key K? **(8 marks)**

END OF SECTION B

Section C : Applied Theory (20 Marks)

- This section consists of questions with serial number 6 - 7.
- Answer all questions.
- Marks are indicated against each question.
- Do not spend more than 25-30 minutes on Section C.

6. SET (Secure Electronic Transaction) is an open encryption and security specification designed to protect credit card transactions on the Internet. List the transaction types supported by SET. **(10 marks)**

7. S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security and defined in RFCs. Explain the functions provided by S/MIME and also explain cryptographic algorithms used in S/MIME. **(10 marks)**

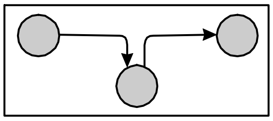
END OF SECTION C

END OF QUESTION PAPER

Suggested Answers
Cryptography, Computer Security plus Disaster Recovery (MB3H2IT)

Section A : Basic Concepts

Answer **Reason**

1. D  represents modification.

2. C Denial of service is a type of active attack which prevents or inhibits the normal use or management of communications facilities. Masquerade is a type of active attack which takes place when one entity pretends to be a different entity. Replay is a type of active attack which involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

3. E The basic tasks in designing security service: Design an algorithm for performing the security-related transformation. Generate secret information to be used with the algorithm. Develop methods for the distribution and sharing of the secret information. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

4. C Security service: Enhances the security of the data processing systems and the information transfers of an organization.

5. B The first step in SSL Record protocol is fragmentation. Each upper layer message is fragmented into blocks of 2^{14} bytes.

6. A DES is used in Secure Electronic Transaction (SET) (or) SET is an application of DES.

7. B Radix-64 conversion algorithm is used by Pretty Good Privacy (PGP) to provide transparency for e-mail applications.

8. B An Application-level gateway is also called as proxy server.

9. A Given p = 7, q = 13,

$n = p * q$,

Therefore, $n = (7 * 13) = 91$.

$\varphi(n) =(p - 1) (q - 1) = (7 - 1) (13 - 1) = (6 * 12) = 72$.

10. E The output of SHA-1 algorithm is 160-bit message digest.

11. B In ISAKMP header format, the size of Message ID field is 32 bits.

12. D Nonce payload contains random data used to guarantee liveness during an exchange and protect against replay attacks.

13. A In RSA public-key encryption, The formula used to calculate plaintext (M) is

$M=C^{d} \text{ (mod n)}$.

14. C Operational model is based on a judgment of what is considered abnormal, rather than an automated analysis of past audit records. Markov process model is used to establish transition probabilities among various states. Multivariate model is based on correlations between two or more variables. Time series model focuses on time intervals, looking for sequence of events that happen too rapidly or too slowly.

15. B Service control determines the types of internet services that can be accessed, inbound or outbound. Direction control determines the direction in which particular service requests may be initiated and allowed to flow through the firewall. User control controls access to a service according to which user is attempting to access it. Behavior control controls how particular services are used.

16. A Markov model is represented as a quadruple [*m, A, T, k*]. In this model, *A* represents state space.

17. B The default forward policy increases ease of use for end users but provides reduced security.

18. D The bastion host hardware platform executes a secure version of its operating system, making it a trusted system. Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host. Each proxy is independent on other proxies on the bastion host.

19. C Counter is a nonnegative integer that may be incremented but not decremented until it is reset by management action. Gauge is a nonnegative integer that may be incremented or decremented. Resource utilization is the quantity of resources consumed during a specified period. Interval timer is the length of time between two related events.

20. C The following are true about SMTP/822 scheme: SMTP cannot transmit executable files or other binary objects, SMTP servers may reject mail message over a certain size, SMTP cannot transmits text data that includes national language characters.

21. D Masquerader is likely to be an outsider, Misfeasor is generally an insider and Clandestine user can be either an outsider or an insider.

22. D X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. X.509 standard does not dictate the use of a specific algorithm but recommends RSA. X.509 is based on the use of public-key cryptography and digital signatures.

23. D ZIP is used for compression.

24. C quoted-printable: encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.

25. B The Record Protocol takes an application message to be transmitted , fragments the data into manageable blocks, optionally compress the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.

26. D In Execution phase the virus performs the function, which may be harmless such as a message on the screen or harmful such as destructive of programs and data files.

27. A FORWARDABLE flag tells Ticket-Granting-Server (TGS) that new ticket-granting tickets with a different network address may be issued based on this ticket-granting ticket.

28. C The size of sequence number field is 32 bits.

29. E Identity protection exchange expands the base exchange to protect the user’s identities. Authentication only exchange is used to perform mutual authentication, without a key exchange. Informational exchange is used for one-way transmittal of information for Security Association (SA) management.

30. D Verisign uses class–II digital IDs for Online subscription, software validation etc. Verisign uses class–III digital IDs for E-banking, Personal banking, Content integrity services and e-commerce server.

Cryptography, Computer Security plus Disaster Recovery (MB3H2IT)

Section B : Problems/Caselets

1. The following are the possible reasons behind choosing PGP by National Security Agency.

   - FIPS 140-2 compliance: Most importantly for the agency, PGP was the only product that included FIPS 140-2-compliant encryption technology by leveraging the RSA BSAFE library.
   - Supports Public Key Infrastructures: PGP supports this infrastructure; WinZip does not and the agency was intent on using PKI.
   - PGP was the only solution that could work effortlessly with these certificates.
   - Centralized encryption policies: Security only works if it can be easily enforced. The great advantage of PGP is that an enterprise can set security protocols so they automatically become part of the workflow. Therefore, the agency viewed these policy manager capabilities within PGP as a decided advantage. Using Policy Manager, administrators could centrally control encryption standards, configuring and securing protocols. Every time an Agency employee or affiliate created a PGP file, the user was locked into encrypting the file according to the agency's settings. This is the control that was lacking with WinZip.
   - PGP serves the dual purpose of encryption and compression: The agency had become accustomed to the efficiency of compressed files using WinZip. Accepting a solution without compression would be an operational step backward.
   - PGP is available free worldwide in versions that run on a variety of platforms, including DOS/Windows, UNIX, Macintosh, and many more. In addition, the commercial version satisfies users who want a product that comes with vendor support.
   - PGP is based on algorithms that have survived extensive public review and are considered extremely secure. Specifically, the package includes RSA, DSS, and Diffie-Hellman for public-key encryption; CAST-128, IDEA, and TDEA for conventional encryption and SHA-1 for hash coding.
   - PGP has wide range of applicability, from corporations that wish to select and enforce a standardized scheme for encrypting files and messages to individuals who wish to communicate securely with others worldwide over the Internet and other networks.
   - PGP was not developed by, nor is it controlled by, any governmental or standards organization.

2. If I am the manager of National Security Agency, I will classify security services as follows:

   - Confidentiality
   - Authentication
   - Integrity
   - Nonrepudiation
   - Access control
   - Availability.

   Confidentiality:

   Confidentiality is the protection of transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement.

   The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Authentication:

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic (that is, that each is entity it claims to be). Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Integrity:

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages only without regard to any larger context, generally provides protection against message modification only.

We can make a distinction between the service with and without recovery. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data, as we will review subsequently. The incorporation of automated recovery mechanisms is, in general, the more attractive alternative.

Nonrepudiation:

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver.

Access Control:

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this control, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Availability:

A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

3. The types of threats that are prone to attack the systems of OFS are:

The threats come in the form of viruses or take different other forms such as malicious programs, trap doors, logic bomb, Trojan horses.

- **Malicious programs:** These can be classified into two categories – those that need a host program, and those that are independent. The former are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program. The latter are self-contained programs that can be scheduled and run by the operating system.
- **Trap doors:** A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. They become threats when they are used by unscrupulous programmers to gain unauthorized access.
- **Logic bombs:** The logic bomb is a code embedded in some legitimate program that is set to ‘explode’ when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a

particular day of the week or date, or a particular user running the application.

- **Trojan horses:** A Trojan horse is a useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function. Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
- **Worms:** Network worm programs use network connections to spread from system to system. Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.
- **Bacteria:** Bacteria are programs that do not explicitly damage any files. Their sole purpose is to replicate themselves. Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory or disk space, denying users access to those resources.
- **Viruses:** A virus is a program that can 'infect' other programs by modifying them; the modification includes a copy of the virus program, which can then go to infect other programs. A virus can do everything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs.

4. Two most commonly used methods in network security are encryption and firewalls.

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as computers, networks(e.g. the Internet e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Encryption is also used in digital rights management to restrict the use of copyrighted material and in software copy protection to protect against reverse engineering and software piracy.

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to verify the integrity and authenticity of a message; for example, a message authentication code (MAC) or digital signatures. Standards and cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security is a challenging problem.

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text ;* encrypted data is referred to as *cipher text*.

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the internet.A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system. A firewall is a convenient platform for several Internet functions that are security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function audits or logs Internet usage. A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

5. a. **Diffie-Hellman Key Exchange:**

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography is generally referred to as Diffie-Hellman key exchange. A number of commercial products employ this key exchange technique.

The purpose of the algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of the keys.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. Briefly, we can define the discrete logarithm in the following way. First, we define a primitive root of a prime number *p* as one whose powers generate all the integers from 1 to $p - 1$. That is, if *a* is a primitive root of the prime number *p,* then the numbers

a *modp,* a^2 *modp,...,* $a^{P}\text{-}^{1}$ *modp*

are distinct and consist of the integers from 1 through $p - 1$ in some permutation.

For any integer *b* and a primitive root *a* of prime number *p,* one can find a unique exponent *i* such that

$b = a^{i}$ *modp.* where $0 \leq i \leq (p - 1)$

The exponent *i* is referred to as the discrete logarithm, or index, of *b* for the base *a,* mod *p.* This value is denoted as $\text{ind}_{a,p}(b)$

There are two publicly known numbers: a prime number *q* and an integer α that is a primitive root of *q.* Suppose the users A and B wish to exchange a key. User A selects a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A}$ mod *q.* Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B}$ *mod q.* Each side keeps the *X* value private and makes the *Y* value available publicly to the other side. User A computes the key as K = $(Y_B)^{X_A}$ mod *q* and user B computes the key as K = $(Y_A)^{X_B}$ mod *q.* These two calculations produce identical results.

Suppose that user A wishes to set up a connection with user B and u secret key to encrypt messages on that connection. User A can generate a one-time private key X_A, calculate Y_A and send that to user B. User B responds by generating a private value X_B, calculating Y_B, and sending Y_B to user A. Both users can now calculate the key. The necessary public values *q* and α would need to be known ahead of time. Alternatively, user A could pick values for *q* and α and include in the first message.

The algorithm can be summarized as below:

Global Public Elements

q	prime number
α	α<q and α a primitive root of q

User A key generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B key generation

Select private X_B	$X_B < q$
Calculate Y_B	$Y_B = \alpha^{X_B} \bmod q$

Generation of secret key by User A

K= $(Y_B)^{X_A} \bmod q$

Generation of secret key by User B

K= $(Y_A)^{X_B} \bmod q$

b. From given data q = 11, $\alpha = 2$

i. Given $Y_A = 9$

To find X_A , we have

$Y_A = \alpha^{X_A} \bmod q$

$9 = 2^{X_A} \bmod 11$ ($X_A < 11$)

$\therefore X_A = 6$

ii. Given $Y_B = 3$

To find the shared key, we should know X_B

$Y_B = \alpha^{X_B} \bmod q$

$3 = 2^{X_B} \bmod 11$ ($X_B < 11$)

$X_B = 8$.

$\therefore$ Shared secret key K= $(Y_B)^{X_A} \bmod q$ (or) K= $(Y_A)^{X_B} \bmod q$

K = $3^6 \bmod 11$

= 729 mod 11 = 3

(or)

K = $9^8 \bmod 11$

= 43046721mod11 = 3

Section C: Applied Theory

6.SET Transaction Types

Cardholder registration	Cardholders must register with a CA before they can send SET messages to merchants.
Merchant registration	Merchants must register with a CA before they can exchange SET messages with customers and payment gateways.
Purchase request	Message from customer to merchant containing OI for merchant and PI for bank.
Payment authorization	Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given credit card account.
Payment capture	Allows the merchant to request payment from the payment gateway.
Certificate inquiry and status	If the CA is unable to complete the processing of a certificate request quickly, it will send a reply to the cardholder or merchant indicating that the requester should check back later. The cardholder or merchant sends the Certificate Inquiry message to determine the status of the certificate request and to receive the certificate if the request has been approved.
Purchase inquiry	Allows the cardholder to check the status of the processing of an order after the purchase response has been received. Note that this message does not include information such as the status of back-ordered goods, but does indicate the status of authorization, capture, and credit processing.
Authorization reversal	Allows a merchant to correct previous authorization requests. If the order will not be completed, the merchant reverses the entire authorization. If part of the order will not be completed (such as when goods are back

	ordered), the merchant reverses part of the amount of the authorization.
Capture reversal	Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.
Credit	Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping. Note that the SET Credit message is always initiated by the merchant, not the cardholder. All communications between the cardholder and merchant that result in a credit being processed happen outside of SET.
Credit reversal	Allows a merchant to correct a previously request credit.
Payment gateway certificate request	Allows a merchant to query the payment gateway and receive a copy of the gateway's current key exchange and signature certificates.
Batch administration	Allows a merchant to communicate information to the payment gateway regarding merchant batches.
Error message	Indicates that a responder rejects a message because it fails format or content verification tests.

7.S/MIME provides the following functions:

- **Enveloped data:** This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.
- **Signed data:** A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
- **Clear-signed data:** As with signed data, a digital signature of the content is formed, however in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.

Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed data or clear-signed data may be encrypted.

Cryptographic Algorithms Used in S/MIME

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1 and MD5. SHOULD use SHA-1.
Encrypt message digest to form digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with message.	Sending and receiving agents MUST support Diffie-Hellman. Sending agent SHOULD support RSA encryption with key sizes 512 bits to 1024 bits. Receiving agent SHOULD support RSA decryption.
Encrypt message for transmission with one-time session key.	Sending agents SHOULD support encryption with tripleDES and RC2/40. Receiving agents SHOULD support decryption using tripleDES and MUST support decryption with RC2/40.