Cryptography and Network Security

UNIT-I
PART-A

1. Differentiate passive attack from active attack with example. [April/May 2011]

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.

2. What is the use of Fermat's theorem? [April/May 2011]

Two theorems that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem. This is sometimes referred to as Fermat's little theorem. Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p , then $A^{p-1}=1(\text{mod } p)$

3. What are the two problems with one-time pad? [Nov/Dec 2011]

- It makes the problem of making large quantities of random keys.
- It also makes the problem of key distribution and protection.

4. Define threat and attack.(April/May 2010) (Nov/Dec 2009)

Threat: A Potential violation of security which exists when there is circumstance, capacity, action or event that could breach security and cause harm .i.e. A threat is a possible danger that might exploit a vulnerability.

Attack: An assault on system security that derives from an intelligent threat: i.e. an intelligent act or deliberate attempt to evade security services and violate the security policy of the system.

5. State Euler's theorem. (April/May 2010)

Euler's theorem states that for every a and n that are relatively prime $a^{\varphi(n)} \equiv 1 \text{ mod } n$
Eg: a=3 n=10 $\varphi(n) \equiv 1$ $3^4 \equiv 1 \text{ mod } 10$

6. Calculate the value using Fast modular exponentiation algorithm. (April/May 2010)

$11^{23} \text{ mod } 187=88$

7. What is cryptanalysis and cryptography? (Nov/Dec 2009)

Cryptanalysis is the study of taking encrypted data, and trying to unencrypted it without use of the key. The other side of cryptography, cryptanalysis is used to break codes by finding weaknesses within it. In addition to being used by hackers with bad intentions, cryptanalysis is also often used by the military. Cryptanalysis is also appropriately used by designers of encryption systems to find, and subsequently correct, any weaknesses that may exist in the system under design. Cryptography the primary goal of cryptography is to conceal data to protect it against unauthorized third-party access by applying encryption. The more theoretical or mathematical effort is required for an unauthorized third party to recover data, the stronger is the encryption.

8. What are the key principles of security? (May/June 2009)

- Confidentiality
- Integrity
- Availability

9. How does simple columnar transposition work?(May/June 2009)

Write the message in a rectangle row by row and read message off column by column but permute the order of the columns. The order of the column becomes the key to the algorithm.

10. What are the essential ingredients of a symmetric cipher?

A symmetric cipher encryption has five ingredients. They are:

- Plaintext
- Encryption algorithm
- Secret key
- Cipher text
- Decryption algorithm

11. What are the two basic functions used in encryption algorithms?

The two basic functions used in encryption algorithms are

- Substitution
- Transposition

12. How many keys are required for two people to communicate via a cipher?

If both sender and receiver use the same key, the system is referred to as symmetric, single key, secret key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.

13. What is the difference between a block cipher and a stream cipher?

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

14. What are the two approaches to attacking a cipher?

The two approaches to attack a cipher are:

- Cryptanalysis
- Brute-force attack

15. What is the difference between an unconditionally secure cipher and a Computationally secure cipher?

An unconditionally secure cipher is a scheme such that if the cipher text generated by the scheme does not contain enough information to determine uniquely the corresponding plain text, no matter how much cipher text is available.

A computationally secure scheme is such that the cost of breaking the cipher exceeds the value of the encrypted information and the time required to break the cipher exceeds the useful lifetime of the information.

16. Briefly define the Caesar cipher.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example:

Plain: meet me after the toga party
Cipher: PHHW PH DIWHU WKH WRJD SDUWB

17. Briefly define the monoalphabetic cipher?

A monoalphabetic cipher maps from a plain alphabet to cipher alphabet. Here a single cipher alphabet is used per message.

18. Briefly define the playfair cipher.

The best-known multiple-letter encryption cipher is the playfair, which treats diagrams in the plain text as single units and translates these units into cipher text diagrams.

19. What is a transposition cipher?

Transposition cipher is a cipher, which is achieved by performing some sort of permutation on the plaintext letters.

20. What is Steganography?

Hiding the message into some cover media. It conceals the existence of a message. The process of hiding a message in image.

22. Why is it not practical to use an arbitrary reversible substitution cipher?

An arbitrary reversible cipher for a large block size is not practical, however, from an implementation and performance point of view. Here the mapping itself is the key.

23. What is the difference between diffusion and confusion?

In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation.

In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution.

24. What is the difference between a mono alphabetic cipher and a poly alphabetic cipher? (NOV/DEC 2012)

- Mono alphabetic cipher: Here a single cipher alphabet is used.
- Poly alphabetic cipher: Here a set of related mono alphabetic substitution rules is used.

25. List the types of cryptanalytic attacks.

- Cipher text only
- Known plaintext
- Chosen plaintext
- Chosen cipher text
- Chosen text

26. Explain active and passive attack with example?(APR/MAY 2011)

Passive attack:
Monitoring the message during transmission Eg: Interception
Active attack:
It involves the modification of data stream or creation of false data stream. E.g.: Fabrication, Modification, and Interruption

27. Define integrity and nonrepudiation?

Integrity:

Service that ensures that only authorized person able to modify the message.

Nonrepudiation:

This service helps to prove that the person who denies the transaction is true or false.

28. Compare Substitution and Transposition techniques.

SUBSTITUTION	TRANSPOSITION
***A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols.** ***Eg: Caeser cipher.**	*** It means,different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.** ***Eg: DES, AES.**

29. what are the different types of attack?(NOV/DEC 2011)
30. Define LFSR sequence(MAY/JUNE 2012)
31. Define finite field (MAY/JUNE 2012)

32. Define steganography. [May/June- 2013]

Hiding the message into some cover media. It conceals the existence of a message. The process of hiding a message in image.

33. What are active and passive attacks that compromise information security? [May/June-2014]

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

34. Why random numbers are used in network security? [May/June- 2014]

Good random numbers are fundamental to almost all secure computer systems. Without them everything from Second World War ciphers like Lorenz to the SSL your browser uses to secure web traffic are in serious trouble.

To understand why, and the threat that bad random numbers pose, it's necessary to understand a little about random numbers themselves (such as "what is a good random number anyway?") and how they are used in secure systems.

35. State Euler's theorem. [May/June- 2014]

In number theory, **Euler's theorem** (also known as the **Fermat–Euler theorem** or **Euler's totient theorem**) states that if *n* is a positive integer and *a* is a positive integer coprime to *n*, then

Where φ(*n*) is Euler's totient function and "... ≡ ... (mod *n*)" denotes ... congruence ... modulo n. The converse of Euler's theorem is also true; if the above congruence holds, then a and n are coprime.

The theorem is a generalization of Fermat's little theorem, and is further generalized by Carmichael's theorem.

The theorem may be used to easily reduce large powers modulo *n*. For example, consider finding the last decimal digit of 7^{222}, i.e. 7^{222} (mod 10). Note that 7 and 10 are coprime, and φ(10) = 4. So Euler's theorem yields $7^4 \equiv 1 \pmod{10}$, and we get $7^{222} \equiv 7^{4x55 + 2} \equiv (7^4)^{55}x7^2 \equiv 1^{55}x7^2 \equiv 49 \equiv 9 \pmod{10}$.

In general, when reducing a power of *a* modulo *n* (where *a* and *n* are coprime), one needs to work modulo φ(*n*) in the exponent of *a*:

Euler's theorem also forms the basis of the RSA encryption system: encryption and decryption in this system together amount to exponentiating the original text by φ(*n*), so Euler's theorem shows that the decrypted result is the same as the origina.

Part B

1. Discuss the classical cryptosystems and its types. [April/May 2011]

- Explain about the single round of DES algorithm. (10)
- Describe key discarding process of DES. (6)

2. Explain RSA method in detail. (16) [April/May 2011]

3. Using play fair cipher algorithm encrypt the message using the key "MONARCHY" and explain. [Nov/Dec 2011]

4. Explain the ceaser cipher and monoalphabetic cipher. [Nov/Dec 2011]

5. Explain Classical crypto systems.

- Shift cipher
- Affine cipher
- The vigenere cipher
- Substitution cipher
- Playfair cipher
- One time pad cipher

6. Explain LFSR sequences.

Refer Text Book 1: Page No: 43-50

7. Explain Chinese Remainder theorem.

Refer Text Book 1: Page No: 76-78

8. Explain Fermat and Euler's theorem

Refer Text Book 1 : Page No:79-83

9. Explain Legendre and Jacobi symbols

Refer Text Book 1 : Page No:88-93

10. Explain Modular exponentiation

Refer Text Book 1 : Page No:78-79

11. Explain Congruences.

Refer Text Book 1 : Page No:70-76

12. Write about any two classical crypto systems (substitution and transposition) with suitable examples. [May/June- 2013]

13. Write about Fermat and Euler's theorem in detail. [May/June- 2013]

14. Explain any two classical ciphers and also describe their security Limitations. [May/June-2014]

15. Describe Linear Feedback Shift Registers Sequences and Finite Fields with their application in Cryptography. [May/June- 2014]

UNIT II

1. Why is it important to study feistel cipher?

This cipher can be used to approximate the simple substitution cipher by utilizing the concept of a product cipher, which is the performing of two or more basic ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

2. Which parameters and design choices determine the actual algorithm of a feistel cipher?

- Block size
- Key size
- Number of rounds
- Sub key generation algorithm
- Round functions
- Fast software encryption or decryption
- Ease of analysis

3. What is the purpose of the S-boxes in DES? [Nov/Dec 2011]

Each row of a S-box defines a general reversible substitution. It consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

4. Explain the avalanche effect. (NOV/DEC 2012)

It is that a small change in either the plaintext or the key should produce a significant change in the cipher text.

A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text.

5. What is the difference between differential and linear cryptanalysis? (MAY/JUNE 2012)

- In differential cryptanalysis, it breaks the DES in less 255 complexities.
- In cryptanalysis, it finds the DES key given 247 plaintexts.

6. Compare stream cipher with block cipher with example.

Stream cipher:

Processes the input stream continuously and producing one element at a time. Example: caeser cipher.

Block cipher:

Processes the input one block of elements at a time producing an output block for each input block. Example: DES.

7. Specify the components of encryption algorithm.

1. Plaintext
2. Encryption algorithm
3. secret key
4. ciphertext
5. Decryption algorithm

8. Define confidentiality and authentication

Confidentiality:

It means how to maintain the secrecy of message. It ensures that the information in a computer system and transmitted information are accessible only for reading by authorized person.

Authentication:

It helps to prove that the source entity only has involved the transaction.

9. Compare Substitution and Transposition techniques.

SUBSTITUTION	TRANSPOSITION
*A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols. *Eg: Caeser cipher.	* It means,different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. *Eg: DES, AES.

10. Give the five modes of operation of Block cipher.

Electronic Codebook(ECB)

Cipher Block Chaining(CBC)

Cipher Feedback(CFB)

Output Feedback(OFB)

Counter(CTR)

11. State advantages of counter mode.

- Hardware Efficiency
- Software Efficiency
- Preprocessing
- Random Access
- Provable Security
- Simplicity.

12. What is traffic padding? What is its purpose?

Traffic padding produces cipher text output continuously, even in the absence of the plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible to for an attacker to distinguish between true dataflow and padding and therefore impossible to deduce the amount of traffic.

13. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

Some block cipher modes of operation only use encryption because the input is set to some initialization vector and the leftmost bits of the output of the encryption function are XORed with the first segment of plain text p1 to produce the first unit of cipher text C1 and it is transmitted. While in decryption, the cipher text is XORed with the output of the encryption function to produce the plain text.

14. What is triple encryption?

Tuchman proposed a triple encryption method that uses only two keys [TUCH79]. The function follows an encrypt – decrypt – encrypt (EDE) sequence. C=Ek1 [Dk2 [Ek1 [P]]] There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES:
C=Ek1[Dk2[Ek1[P]]] = Ek1[P]

15. What is a meet-in-the-middle attack?

Meet-in-the-middle attack, was first described in [DIFF77]. It is based on the observation that, if we have C=Ek2[Ek1[P]] Then X=Ek1[P]=Dk2[C] Given a known pair, (P,C), the attack proceeds as follows. First, encrypt P for all 256 possible values of K1. Store these results in a table and then sort the table by the values of X. Next, decrypt C using all 256 possible values of K2. As each decryption is produced, check the result against the table for a match. If a match occurs, then test the two resulting keys against a new known plaintext-ciphertext pair. If the two keys produce the correct ciphertext, accept them as the correct keys.

16. What primitive operation is used in RC4?

The primitive operation used in RC4 is bit wise Exclusive-OR (XOR) operation.

17. Differentiate symmetric and asymmetric encryption?

Symmetric	Asymmetric
It is a form of cryptosystem in which encryption and decryption performed using the same key.	It is a form of cryptosystem in which encryption and decryption Performed using two keys.
Eg: DES, AES	Eg: RSA, ECC

18. List important design considerations for a stream cipher.

The encyption sequence should have a large period. The keystream should approximate the properties of a true random number stream as close as possible. The output of the pseudorandom number generator is conditioned on the value of the input key.

19. Why is it not desirable to reuse a stream cipher key?

If two plaintexts are encrypted with the same key using a stream cipher then cryptanalysis is often quite simple. If the two cipher text streams are XORed together the result is the XOR of the original plaintexts. So it is not desirable to reuse a stream cipher key.

20. For a user workstations in a typical business environment, list potential locations for confidentiality attacks.

- LANs in the same building that are interconnected with bridges and routers.
- The wiring closet itself is vulnerable.
- Twisted pair and coaxial cable can be attacked using either invasive taps or
- Inductive devices that monitor electromagnetic emanation.
- In addition to the potential vulnerability of the various communications links, the
- Various processors along the path are themselves subject to attack.

21. What is the difference between link and end-to-end encryption?

S. No	link encryption	end-to-end encryption
1	With link encryption, each vulnerable Communications link is equipped on Both ends with an encryption device	With end to end encryption, the encryption process is carried out at the two end systems
2	Message exposed in sending host and in intermediate nodes	Message encrypted in sending and intermediate nodes
3	Transparent to user	User applies encryption
4	Host maintains encryption facility	Users must determine algorithm
5	One facility for all users	Users selects encryption scheme
6	Can be done in hardware	Software implementations
7	Provides host authentication	Provides user authentication
8	Requires one key per(host-intermediate) Pair and (intermediate-intermediate)pair	Requires one key per user pair

22. What types of information might be derived from a traffic analysis attack?

The following types of information can be derived from traffic analysis attack:

- Identities of partners
- How frequently the partners are communicating
- Message pattern, message length, or quantity of messages that suggest important

- information is being exchanged
- The events that correlate with special conversations between particular partners.

23. What is traffic padding and what is its purpose?

Traffic padding produces ciphertext output continuously, even in the absence of plaintext. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted.

24. List ways in which secret keys can be distributed to two communicating parties.

• A can select a key and physically deliver it to B.
• A third party can select the key and physically deliver it o A and B
• If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key
• If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B

25. What is the difference between Rijndael and AES?

AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES.NIST selected rijndael as the proposed AES algorithm. The two researchers who developed and submitted Rijndael for the AES are the both cryptographers from Belgium.

26. Why is the middle portion of 3DES a decryption rather than an encryption?

Decryption requires that the keys be applied in reverse order:
P=Dk1[Ek1[P]]
This results in a dramatic increase in cryptographic strength.The use of DES results in a mapping that is not equivalent to a single DES encryption.

27. What is the difference between the AES decryption algorithm and the equivalent inverse cipher?

In AES decryption, we use inverse shift rows inverse sub bytes, add round key, inverse mix columns. But in equivalent inverse cipher, we interchange inverse shift rows and inverse sub bytes

28. What is Triple DES?(April/May 2010)

Two keys:C=EK1(DK2(EK1(P)))
Three keys:C=EK1(EK2(EK3(P)))
Where C=cipher text ,P=plain text ,E=encryption,D=decryption,K1,K2,K3=keys

29. 5.Perform encryption and decryption using RSA alg. For the following.

P=7; q=11; e=17; M=8.
Soln: n=pq
n=7*11=77
ö(n)=(p-1) (q-1)
=6*10 = 60
e=17
d =27
C= Me mod n
C = 817 mod 77
= 57
M = Cd mod n
= 5727 mod 77
= 8

30.List the evaluation criteria defined by NIST for AES?

The evaluation criteria for AES is as follows:

1.Security
2. Cost
3.Algorithm and implementation characteristics

31. Differentiate public key and conventional encryption? (NOV/DEC 2011)

S.No	Conventional Encryption	Public key Encryption
1	The same algorithm with the same Key is used for encryption and decryption	One algorithm is used for encryption and decryption with a pair of keys, one for encryption and another for decryption
2	The sender and receiver must share The algorithm and the key	The sender and receiver must each have one of the Matched pair of keys
3	The key must be secret	One of two keys must be kept Secret
4	It must be impossible or atleast impractial decipher a message if no other information is available	It must be impossible or to at least impractical to decipher a message if no other information is available
5	Knowledge of the algorithm plus samples of cipher text must insufficient to determine the key	Knowledge of the algorithm plus one of key plus samples of ciphertext must be insufficient to determine the other key.

32. Specify the applications of the public key cryptosystem?

The applications of the public-key cryptosystem can classified as follows

1. Encryption/Decryption: The sender encrypts a message with the recipient's public key.

2.Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to a message or to a small block of data that is a function of the message.

3.Key Exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

33. What are the different modes of operations in DES?(APR/MAY 2011)
34. Name any two methods for finding prime numbers?(APR/MAY 2011)
35. Show that 3 is a primitive root of 7.(MAY/JUNE 2009)
36. Find the GCD of 2740 and 1760 using Euclidian algorithm.(MAY/JUNE 2009)
37. What are the disadvantages of double DES?(NOV/DEC 2012)
38.Define primitive roots.(NOV/DEC 2012)
39.Define: diffusion.(NOV/DEC 2011)
40.Define factoring (NOV/DEC 2012)
41. What do you mean by differential cryptanalysis?(NOV/DEC 2012)
42. What is the disadvantage with ECB mode of operation? [May/June- 2013]

ECB is the simplest mode of operation for a block cipher. The input data is padded out to a multiple of the block size, broken into a integer number of blocks, each of which is encrypted independently using the key. In addition to simplicity, ECB has the advantage of allowing any block to be decrypted independently of the others. Thus, lost data blocks do not affect the decryption of other blocks. The disadvantage of ECB is that it aids known-plaintext attacks. If the same block of plaintext is encrypted twice with ECB, the two resulting blocks of ciphertext will be the same.

43. What is Optimal Asymmetric Encryption Padding? [May/June- 2014]

To counter attacks such as RSA Security Inc., a leading RSA vendor and former holder of the RSA patent, recommends modifying the plaintext using a procedure known as optimal asymmetric encryption padding (OAEP)

44. What is discrete logarithm problem? [May/June- 2014]

The discrete logarithm problem is defined as: given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups. For example, a popular choice of groups for discrete logarithm based crypto-systems is Zp* where p is a prime number. However, if p−1 is a product of small primes, then the Pohlig–Hellman algorithm can solve the discrete logarithm problem in this group very efficiently. That's why we always want p to be a safe prime when using Zp* as the basis of discrete logarithm based crypto-systems. A safe prime is a prime number which equals 2q+1 where q is a large prime number. This guarantees that p-1 = 2q has a large prime factor so that the Pohlig–Hellman algorithm cannot solve the discrete logarithm problem easily. Even p is a safe prime, there is a sub-exponential algorithm which is called the index calculus. That means p must be very large (usually at least 1024-bit) to make the crypto-systems safe.

The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of modular exponentiation. To form a cryptographic system using elliptic curves, we need to find a "hard problem" corresponding to factoring the product of two primes or taking the discrete logarithm.

Consider the equation $Q = kP$ where Q, P $Ep(a, b)$ and $k < p$. It is relatively easy to calculate Q given k and P, but it is relatively hard to determine k given Q and P. This is called the discrete logarithm problem for elliptic curves.

45. State whether symmetric and asymmetric cryptographic algorithms need Key Exchange. [May/June- 2014]

PART B

1.a)Explain about the single round DES[April/May 2011]
2. b)Describe key descrading in DES [April/May 2011]
3. a)Write the RSA method in detail [April/May 2011]
4. (a) Explain the Key Generation, Encryption and Decryption of SDES algorithm in detail. [Nov/Dec 2011]
5.(b) Write the algorithm of RSA and explain with an example. [Nov/Dec 2011]
6. Explain the OSI security architecture alon with the services available.(Nov/Dec 2009)

- Notes
- Diagram
- llustration

7.Explain Classical Encryption Techniques.

- Symmetric Ciphers
- Caesar Cipher
- Mono alphabetic
- Poly alphabetic

3.Explain DES Algorithm.

- Notes
- Diagram
- Illustration
- Algorithm

4.Explain AES.

- Notes
- Diagram
- Illustration
- Algorithm

5.Describe about Traffic Confidentiality.

Cryptanalytic methods in traffic analysis and ciphers achieving confidentiality.

6. Given 10bit key k=1010000010. determine K1,K2 where P10=3 5 2 7 4 10 1 9 8 6 p8 = 6 3 7 4 8 5 10 9

by using SDES key generation method.(Nov/Dec 2009)

7. Perform encryption/decryption using RSA algorithm for the following: p=3, q=11, e=7, m=5 (12) (Nov/Dec 2009)

8. What attacks are possible on RSA algorithm? (Nov/Dec 2009)

9. Given the key "MONARCHY" apply play fair to pain text "FACTIONALISM" to ensure confidentially at the destination, decrypt the ciphertext and establish authenticity. (Nov/Dec 2009)

10.Explain about the various Key management techniques.

- public announcement
- Publicly available directory
- public-key authority
- public-key certificates 2.Describe Diffie-Hellman Key Exchange.
- Algorithm
- Illustration
- Notes

11.List the steps in RSA algorithm using an example. (April/May 2010)
Explain how encryption and decryption are done using RSA cryptosystems. (May/June 2009)

- Algorithm
- Illustration
- Diagram
- Notes

12.Describe Public Key Cryptography.

Two Keys

- Private key
- public key
- distribution

13.Apply public key encryption to establish confidentiality in the message from A to B. you are given m=67. KU={7,187}, KR={23,187}.(Nov/Dec 2009)

14. Explain the block cipher modes of operation. (April/May 2010,May/June 2009)

- Diagram
- Notes

15.Explain the operation of hill cipher with an example. (April/May 2010)

- Diagram
- Notes

16. Draw the general structure of DES and explain the encryption decryption process.(May/June 2009)

17. Mention the strength and weaknesses of DES algorithm.(May/June 2009)

18. How do Elliptic curves take part in encryption and decryption process. (May/June 2009)

19. Explain briefly about DES in detail. [May/June- 2013]

20.Explain about RSA with one suitable example. [May/June- 2013]

21. Describe the working principle of Simple DES with an example. [May/June- 2014]

22. Explain RSA algorithm. [May/June- 2014]

23. Demonstrate encryption and decryption for the RSA algorithm Parameters p=3, q=11, s=7, d=1, M=5. [May/June- 2014]

UNIT III

1. Define Message Digest. (April/May 2010)

A Message Digest is a fingerprint or the summary of a message similar to the concepts of longitudinal redundancy check and cyclic redundancy check used to verify the integrity of data.

2. Write the use of MAC when authentication is tied to cipher text. (April/May 2010)

A— >B :EK2[M]||CK1(EK2[M])

3. What is the role of session key in public key schemes?(Nov/Dec 2009)

Session key

Session keys are transmitted in encrypted form, using master key that is shared by the keys distribution center and an end system. The session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded.

4. What are the functions used to produce an authendicator? (Nov/Dec 2009)

These are grouped into 3 classes

i. Hash function:A function that maps a message of any length into a fixed length hash value,which serves as an authenticator.
ii. Message encryption:The cipher text of a entire messages acts as an its authenticator.
iii. MAC:A function of the message and a secret key that produces a fixed length value that serves as an authenticator

5. L ist the properties a digital signature should possess? (Nov/Dec 2009)

i. It must verify the author and the date and time of the signature.
ii. It must to authenticate the contents at the timt of the signature.
iii.It must be verifiable by third parties to resolve disputes.

6. What is the difference between a session key and a master key?

Session key

Session keys are transmitted in encrypted form, using master key that is shared by the keys distribution center and an end system. The session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded.

Master key

Communication between end systems is encrypted using temporary key, often referred to as a session key. For each end system or user, there is a unique master key that it shares with the key distribution center. These master keys must be distributed in some fashion.

7. What is nonce?

Consider A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier, N1, for this transaction, which we refer to as nonce. The nonce may be a timestamp, a counter, or a random number.

8. Differentiate public key encryption and conventional encryption.(NOV/DEC 2011)

Conventional Encryption Public key Encryption

1. Same algorithm with 1.Same algorithm is used for same key used for encryption & decryption with encryption and decryption. a pair of keys.

2. Sender & receiver must 2.Sender & receiver have one of share the algorithm and key. the matched pair keys.

3. Key must be kept secret. 3. Any one of the key must be kept secret.

9. Specify the application of public key cryptography.

Encryption/Decryption.
Digital signature.
Key exchange.

10.What is message authentication?

It is a procedure that verifies whether the received message comes from assigned source has not been altered.

11. Define the classes of message authentication function.

• Message encryption: The entire cipher text would be used for authentication.
• Message Authentication Code: It is a function of message and secret keyproduce a fixed length value.
• Hash function: Some function that map a message of any length to fixed length which serves as authentication.

12. What you meant by MAC?

MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC.

13. Specify the techniques for distribution of public key.

- Public announcement.
- Publicly available directory.
- Public key authority.
- Public key certificate.

14. Specify the requirements for message authentication.
i. Disclosure.
ii. Traffic analysis.
iii. Masquerade.
iv. Content Modification.
v. Sequence Modification.
vi. Timing modification.
vii. Repudiation.

15. Differentiate internal and external error control.

- Internal error control: In internal error control, an error detecting code also known as frame check sequence or checksum.
- External error control: In external error control, error detecting codes are appended after encryption.

16. What you meant by hash function?

Hash function accept a variable size message M as input and produces a fixed size hash code H(M) called as message digest as output. It is the variation on the message authentication code.

17. Differentiate MAC and Hash function?

- MAC:
  In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.
- Hash Function:
  The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

18. What is key distribution center?

A key distribution center is responsible for distributing keys to pairs of users such as hosts, processes, applications. Each user must share a unique key with the key distribution center for purposes of key distribution.

19. Differentiate symmetric and Asymmetric Encryption
Symmetric Encryption
Sender and receiver use the same key.
Asymmetric
Sender and receiver uses different key.

20. User A & B exchange the key using Diffie Hellman alg. Assume á=5 q=11 XA=2 XB=3. Find YA, YB, K.
Soln:
YA = áXA mod q
=52 mod 11
= 3
YB = áXB mod q
= 53 mod 11
= 4
KA = YBXA mod q
= 42 mod 11
= 5
KB = YAXB mod q
= 33 mod 11
= 5

21. What are roles of public and private key?

The two keys used for public-key encryption are referred to as the public key and the private key. Invariably, the private key is kept secret and the public key is known publicly. Usually the public key is used for encryption purpose and the private key is used in the decryption side.

22. What is discrete logarithm?(APR/MAY 2011)
23. What do you mean by one way property in Hash function?(APR/MAY 2011)
24. Why is SHA more secure than MD5?(MAY/JUNE 2011)
25. Mention the fundamental idea of HMAC.(MAY/JUNE 2011)
26. What is one –way property(NOV/DEC 2012)
27.What are the two approaches of Digital signatures?(NOV/DEC 2012)
28.Define:Replay attack(NOV/DEC 2011)
29. List the parameters of AES.(NOV/DEC 2011)
30. Difference between public key and private key cryptosystems?(MAY/JUNE 2012)
31.Find GCD(21,300) using Euclid's algorithm. [May/June- 2013]

32. Define discrete logarithm. [May/June- 2013]

Discrete logarithms are fundamental to a number of public-key algorithms. Discrete logarithms are analogous to ordinary logarithms, but operate over modular arithmetic

33. What is List the authentication requirements. [May/June- 2014]

Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.

Traffic analysis: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.

Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by anopponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient.

Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.**Sequence modification:** Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.

Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

Source repudiation: Denial of transmission of message by source.

Destination repudiation: Denial of receipt of message by destination.

34.What are birthday attacks? [May/June- 2014]

Birthday attack is a name used to refer to a class of brute-force attacks. It gets its name from the surprising result that the probability that two or more people in a group of 23 share the same birthday is greater than 1/2; such a result is called a birthday paradox.

If some function, when supplied with a random input, returns one of k equally-likely values, then by repeatedly evaluating the function for different inputs, we expect to obtain the same output after about 1.2k1/2. For the above birthday paradox, replace k with 365.

Birthday attacks are often used to find collisions of hash functions

35.What is collision resistance? What is the use of it? [May/June- 2013]

Collision resistance is a property of cryptographic hash functions: a hash function is **collision resistant** if it is hard to find two inputs that hash to the same output; that is, two inputs a and b such that H(a) = H(b), and a ≠ b.

PART B

1. Discuss the discrete logarithm and explain Diffie-Hellman key Exchange algorithm with its merits and demerits. (16) [April/May 2011]
2. (b) Explain about MD5 in detail. (16) [April/May 2011]
3.(a) Illustrate about the SHA algorithm and explain. [Nov/Dec 2011]
4. (b) Write a detailed note on Digital signatures. [Nov/Dec 2011]

1.Explain Authentication Functions.

- Message Encryption
- MAC
- Hash function

2.Describe HMAC algorithm.

- Algorithm
- Diagram
- Notes

3.Describe RIPEMD-160.

- Algorithm
- Diagram
- Notes

4.Explain Hash Functions.

- Security features
- Algorithms used
- Illustration

5.Explain Digital Signature Standard.

- Algorithm

- Analysis
- Diagram

6. Apply the MAC on the cryptographic checksum method to authenticate build confidentiality of the message where the authentication is tied to message M=8376, K1=4892, K2=53624071 (Nov/Dec 2009)

7. What are the properties a hash function must satisfy? (Nov/Dec 2009)

- Explanation

6. Explain MD5 message digest algorithm, with its logic and compression function. (Nov/Dec 2009)

- Algorithm
- Explanation
- Diagram

7. Explain the secure hash algorithm. (April/May 2010)

- Algorithm
- Explanation
- Diagram

8. Describe the steps in MD5 algorithm. (April/May 2010)

- Algorithm
- Explanation
- Diagram

11. Explain the Diffie –Hellman key exchange using an example. (April/May 2010)

- Algorithm
- Illustration
- Diagram

12. .Explain Elliptic Curve Architecture.
- Architecture
- Algebraic description
- Geometric description

13. How does SHA-1 logic produce message digest? (May/June 2009)
14.What is message authentication ?Explain. (May/June 2009)

15. Write and explain the Digital Signature Algorithm.

- Signature = (r,s)
- Verify v = r'

- Algorithm
- Block diagram

16.Explain about hash algorithm (SHA) in detail. [May/June- 2013]

17.Explain about Diffie Hellman Key exchange algorithm with one suitable example.

[May/June- 2013] Explain Digital Signature Standard. [May/June- 2014]

18.Briefly explain Diffie-Hellman Key Exchange. [May/June- 2014]

19.Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root a=7. If user A has private key Xa=5, what is A's public key Ya? [May/June-2014]

Unit IV

PART – A

1.Define Kerberos.

Kerberos is an authentication service developed as part of project Athena at MIT.The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

2.In the content of Kerberos, what is realm?

A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:

- The Kerberos server must have user ID and hashed password of all participating users in its database.
- The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".

3.Assume the client C wants to communicate server S using Kerberos procedure.
How can it be achieved?
a) C → AS: [IDC|| PC || IDV]
b) AS → C: Ticket
c) C → V: [IDC || ADC || IDV]
Ticket = EKV [IDC ||ADC || IDV]

4. Any three hash algorithm.
• MD5 (Message Digest version 5) algorithm.
• SHA_1 (Secure Hash Algorithm).
• RIPEMD_160 algorithm.

5. Specify the four categories of security threats
• Interruption

• Interception
• Modification
• Fabrication

5. What are the services provided by PGP services
• Digital signature
• Message encryption
• Compression
• E-mail compatibility
• Segmentation

6. Explain the reasons for using PGP?
a) It is available free worldwide in versions that run on a variety of platforms, including DOS/windows, UNIX, Macintosh and many more.
b) It is based on algorithms that have survived extensive public review and are considered extremely secure.
E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128, IDEA, 3DES for conventional encryption, SHA-1for hash coding.
c) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.
d) It was not developed by nor is it controlled by any governmental or standards organization. 3. Why E-mail compatibility function in PGP needed?
Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.

7. Name any cryptographic keys used in PGP?
a) One-time session conventional keys.
b) Public keys.
c) Private keys.
d) Pass phrase based conventional keys.

8. Define key Identifier?
PGP assigns a key ID to each public key that is very high probability unique with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.

9. List the limitations of SMTP?
a) SMTP cannot transmit executable files or binary objects.
b) It cannot transmit text data containing national language characters.
c) SMTP servers may reject mail message over certain size.
d) SMTP gateways cause problems while transmitting ASCII and EBCDIC.
e) SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.

10. Define S/MIME? (MAY/JUNE 2012)
Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME Internet E-mail format standard, based on technology from RSA Data Security.

11. What are the elements of MIME?

- Five new message header fields are defined which may be included in an
- RFC 822 header.
- A number of content formats are defined.
- Transfer encodings are defined that enable the conversion of any content
- format into a form that is protected from alteration by the mail system.

12. What are the headers fields define in MME?

• MIME version.
• Content type.
• Content transfer encoding.
• Content id.
• Content description.

13. What is MIME content type ?

It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes. They are,

1. Text type
    - Plain text.
    - Enriched.
2. Multipart type
    - Multipart/mixed.
    - Multipart/parallel.
    - Multipart/alternative.
    - Multipart/digest.
3. Message type
    - Message/RFC822.
    - Message/partial.
    - Message/external.
4. Image type
    - JPEG.
    - CIF.
5. Video type.
6. Audio type.
7. Application type
    - Post script.
    - Octet stream.

14. What are the key algorithms used in S/MIME?

- Digital signature standards.
- Diffi Hellman.
- RSA algorithm.

15. Give the steps for preparing envelope data MIME?

- Generate Ks.
- Encrypt Ks using recipient's public key.
- RSA algorithm used for encryption.
- Prepare the 'recipient info block'.
- Encrypt the message using Ks.

16. What you mean by versioned certificate?

Mostly used issue X.509 certificate with the product name" versioned digital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.

17. What are the function areas of IP security?

- Authentication
- Confidentiality
- Key management.

18. Give the application of IP security? • Provide secure communication across private & public LAN.

- Secure remote access over the Internet.
- Secure communication to other organization.

19. Give the benefits of IP security?

- Provide security when IP security implement in router or firewall.
- IP security is below the transport layer is transparent to the application.
- IP security transparent to end-user.
- IP security can provide security for individual user.

20. What are the protocols used to provide IP security?

- Authentication header (AH) protocol.
- Encapsulating Security Payload(ESP).

21. Specify the IP security services?

- Access control.
- Connectionless interpretty.
- Data origin authentication
- Rejection of replayed packet.
- Confidentiality.
- Limited traffic for Confidentiality.

22. What do you mean by Security Association? Specify the parameters that identifies the Security Association?

- An association is a one-way relationship between a sender and receiver that affords security services to the traffic carried on.
- A key concept that appears in both the authentication and confidentiality mechanism for ip is the security association (SA). A security Association is uniquely identified by 3 parameters:
- Security Parameter Index (SPI).
- IP Destination Address.
- Security Protocol Identifier.

23. What does you mean by Reply Attack?

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
- Each time a packet is send the sequence number is incremented .

24. Explain man in the middle attack?

If A and B exchange message, means E intercept the message and receive the B's public key and b's userId,E sends its own message with its own public key and b's userID based on the private key and Y.B compute the secret key and A compute k2 based on private key of A and Y

25. Steps involved in SS L required protocol?

1. SSL record protocol takes application data as input and fragments it.
2. Apply lossless Compression algorithm.
3. Compute MAC for compressed data.

4. MAC and compression message is encrypted using conventional alg.

26. What is mean by SET? What are the features of SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet.

Features are:

1. Confidentiality of information
2. Integrity of data
3. Cardholder account authentication
4. Merchant authentication

27. What are the steps involved in SET Transaction?

1. The customer opens an account
2. The customer receives a certificate
3. Merchants have their own certificate
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant requests payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or services.
10. The merchant requests payment.

28. What are the requirements of Kerberos? (April/May 2010,2011)

Secure, reliable, transparent,scalable.

29. Mention the fields of IPSec authentication header(April/May 2010)

Next header(8 bits),Payload length(8 bits),Reserved(16 bits),Security parameter index(32 bits),Sequence number(32 bits),Authentication data(variable length-integral of 32 bit words).

30. Mention the scenario where kerberos scheme is preferred. (April/May 2010)

Kerberos is a authentication service designed for use in a distributed environment .

The kerberos that is preferred to address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

31. What are the technical deficiencies in the kerberos version 4 protocol?(Nov/Dec 2009)

i. Double encryption:
ii. PCBC encryption:It uses non standard modes of DES
iii. Session key:Each ticket includes a session key that is used by the client to encrypt the authenticator
iv. Password attacks: Vulnerable to Password attacks

32. How does IPSec offers the authentication and confidentiality services?

33. Mention any four SSL protocols.(APR/MAY 2011)

34. What are the security options PGP allows when sending an email message?(MAY/JUNE 2009)

35. How IPSec does offers the authentication and confidentiality services?(MAY/JUNE 2009)

36.What are the different types of MIME?(NOV/DEC 2012)

37. What protocols comprise SSL?(NOV/DEC 2012)

38. Define primality test.(NOV/DEC 2011)

39. Define TLS (may/june 2012)

40. List out the services provided by PGP. [May/June- 2013]

Function	Algorithms	Used Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.
Segmentation		To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

41. Expand and define SPI. [May/June- 2013]

Security Parameters Index (SPI): A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed

42. Differentiate spyware and virus. [May/June- 2014]

Spyware and adware collect information about you without appropriate notice and consent.

A computer virus spreads software, usually malicious in nature, from computer to computer.

- Spyware collects information about you without appropriate notice and consent.
- A computer virus spreads software, usually malicious in nature, from computer to computer.

Spyware can get installed on your computer in a number of ways. One way is through a virus.

Another way is for it to be secretly downloaded and installed with other software you've chosen to install. Spyware is a general term used to describe software that performs certain behaviors, generally without appropriately obtaining your consent first, such as:

- Advertising
- Collecting personal information
- Changing the configuration of your computer

A **Virus** is a specific way software can be secretly distributed, often by e-mail or instant messaging. Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk. Computer viruses are often spread by attachments in e-mail messages or instant

messaging messages. That is why it is essential that you never open e-mail attachments unless you know who it's from and you are expecting it.

Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Computer viruses also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs you might download.

43. What are zombies? [May/June- 2014]

A zombie is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator. Zombies are used in denial-of-service attacks, typically against targeted Web sites. The zombie is planted on hundreds of computers belonging to unsuspecting third parties, and then used to overwhelm the target Web site by launching an overwhelming onslaught of Internet traffic.

PART B

1. Write on the following : [April/May 2011]

(i) Differentiate SSL from SET. (8)

(ii) Overview of IP security documents.(8)

2.Explain PGP message generation and reception. (16) [April/May 2011]

3. Describe the SSL Architecture in detail. [Nov/Dec 2011]

4. List out the participants of SET system, and explain in detail. Nov/Dec 2011]

5.Explain Kerberos.

- **Algorithm**
- **Explanation**
- **Diagram**

6. Explain X.509 authentication servise and its certificates. (Nov/Dec 2009)

- Algorithm
- Explanation
- Diagram

7.Describe Electronic Mail Security.

- Algorithm
- Explanation
- Diagram

8. Explain the services of PGP. (Nov/Dec 2009)

how does PGP provide confidentiality and authentication service for e-mail and file storage applications? draw the block diagram and explain its components. (May/June 2009)

- Algorithm
- Explanation
- Diagram
-

9.Write down the functions provided by S/MIME. (Nov/Dec 2009)

- Algorithm
- Explanation
- Diagram
-

10.Discuss the Handshake protocol in detail. (April/May 2010)

- Explanation
- Diagram

11. Discuss the IP SEC architecture in detail. (April/May 2010)

- Explanation

- Diagram
    a. Bring out the importance of security association in IP. **(May/June 2009)**
    b. **Describe the SSL specific protocol handshake action in detail(May/June 2009)**

12. Discuss about X.509 authentication service in detail. [May/June- 2013]

13. Explain about S/MIME in detail. [May/June- 2013]

14. Elaborately explain Kerberos authentication mechanism with suitable diagrams. [May/June-2014]

15. Explain Pretty Good Privacy in detail. [May/June- 2014]

Unit V

1. List the 3 classes of intruder? Define intruder (April/May 2010,2011) (Nov/Dec 2009,2012)

Classes of Intruders

1) Masquerader
2) Misfeasor
3) Clandestine user

Intruder:

someone who intrudes on the privacy or property of another without permission.

2. Define virus. Specify the types of viruses? (Nov/Dec 2009)

A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program.

Types:

1) Parasitic virus
2) Memory-resident virus
3) Boot sector virus
4) Stealth virus
5) Polymorphic virus

3. What is application level gateway?

An application level gateway also called a proxy server; act as a relay of application-level traffic. The user contacts the gateway using a TCP\IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

4. List the design goals of firewalls?

1. All traffic from inside to outside, and vise versa, must pass through the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
   The firewall itself is immune to penetration.

5. What are Honey Pots? (April/May 2010)

Honey Pots are decoy systems that are designed to lure a potential attacker away from critical systems.

*Divert an attacker from accessing critical system
* collect information about attacker's activity
* encourage an attacker to stay tolong enough for administrators to respond.

6. What are the common techniques used to protect a password file?(May/June 2009)

One-way encryption: The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.

Access control: Access to the password file is limited to one or a very few accounts.

7. What is IP Address spoofing? (May/June 2009)

IP address spoofing denotes the action of generating IP packets with fake source IP addresses in order to impersonate other systems or to protect the identity of the sender. Spoofing can also refer to forging or using fake headers on emails or netnews to - again - protect the identity of the sender and to mislead the receiver or the network as to the origin and validity of sent data.

8. Define malicious software.(NOV/DEC 2011)

Malicious software is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

9.Define viruses and worms.(nov/dec 2012)

viruses and worms, are known for the manner in which they spread, rather than any other particular behavior. The term computer virus is used for a program that has infected some executable software and that causes that when run, spread the virus to other executables. Viruses may also contain a payload that performs other actions, often malicious. A worm, on the other hand, is a program that actively transmits itself over a network to infect other computers. It too may carry a payload.

10. Define Trojan horse.(APR/MAY 2011)

A **Trojan horse**, or **Trojan**, is malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system. "It is a harmful piece of software that looks legitimate.

11.Name any two security standards(NOV/DEC 2011), (may/june 2012)

12. Define Intrusion (MAY/JUNE 2012)

Intrusion detection systems focused on single-system stand-alone facilities. The typical organization, however, needs to defend a distributed collection of hosts supported by a LAN or internetwork. Although it is possible to mount a defense by using stand-alone intrusion detection systems on each host, a more effective defense can be achieved by coordination and cooperation amongintrusion detection systems across the network.

13. Mention the two levels of hackers. [May/June- 2013]

An analysis of this attack revealed that there were actually two levels of hackers. The high level were sophisticated users with a thorough knowledge of the technology; the low level were the "foot soldiers" who merely used the supplied cracking programs with little understanding of how they worked. This teamwork combined the two most serious weapons in the intruder armory: sophisticated knowledge of how to intrude and a willingness to spend countless hours "turning doorknobs" to probe for weaknesses.

14. What is logic bomb? [May/June- 2013]

A set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.

One of the oldest types of program threat, predating viruses and worms, is the logic bomb. The logic bomb is 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. Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage. A striking example of how logic bombs can be employed was the case of Tim Lloyd, who was convicted of setting a logic bomb that cost his employer, Omega Engineering, more than $10 million, derailed its corporate growth strategy, and eventually led to the layoff of 80 workers .Ultimately, Lloyd was sentenced to 41 months in prison and ordered to pay $2 million in restitution.

PART B

1. Explain definition, phases, types of virus structures and types of viruses. (16)
2. Write in detail about definition, characteristics, types and limitations of firewalls. (16)[April/May 2011]

3.Explain the types of Intrustion Detection Systems. [Nov/Dec 2011]
4. Explain the different types of firewall and its configurations in detail.[Nov/Dec 2011]
5. List the approaches for the intrusion detection. (Nov/Dec 2009)

- Audit records
- Statistical Anomaly Detection
- Rule Based Intrusion Detection
- Base-Rate Valley
- Distributed
- Honey pot
- Exchange format

6. Give the basic techniques which are in use for the password selection strategies. (Nov/Dec 2009)

- Password Protection
- Password Selection Strategies

7. Explain firewall design principles, characteristics, and types of firewalls. (Nov/Dec 2009,April/May 2010)

- Firewall characteristics

- Types of Firewall Configuration

8. Describe about Trusted Systems.

- Data Access Control
- Concept
- Trojan Horse Defense
-

9. Write down the four generations of antivirus software. (Nov/Dec 2009)

- Malicious Programs
- Nature
- Types
- Macro viruses
- E-mail Viruses
- Worms

10. Write detailed notes on intrusion detection systems.(April/May 2010)

- Explanation
- Diagram

11. Explain the types of host based intusion detection .List any 2 IDS software available. (May/June 2009)

12. What are the positive and negative effects of firewall? (May/June 2009)

13. Describe packet filtering router in detail. (May/June 2009)

14. Write about virus and related threats in detail. [May/June- 2013]

15. Explain briefly about trusted system. [May/June- 2013]

16. Explain statistical anomaly detection and rule based intrusion detection. [May/June- 2014]

17. Describe any two advanced anti-virus techniques in detail. [May/June- 2014]