L T P C
3 0 0 3

19CS503   **CRYPTOGRAPHY AND NETWORK SECURITY**

OBJECTIVES
- To understand Cryptography Theories, Algorithms and Systems.
- To understand necessary Approaches and Techniques to build protection mechanisms in order to secure computer networks.

UNIT I   INTRODUCTION   9
Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.

UNIT II   SYMMETRIC KEY CRYPTOGRAPHY   9
MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures - Modular arithmetic-Euclid"s algorithm- Congruence and matrices - Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES – Differential and linear cryptanalysis - Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard - RC4 – Key distribution.

UNIT III   PUBLIC KEY CRYPTOGRAPHY   9
MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem - Chinese Remainder Theorem – Exponentiation and logarithm - ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange - ElGamal cryptosystem – Elliptic curve arithmetic-Elliptic curve cryptography.

UNIT IV   MESSAGE AUTHENTICATION AND INTEGRITY   9
Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications - Kerberos, X.509

UNIT V   SECURITY PRACTICE AND SYSTEM SECURITY   9
Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.

TEXTBOOK
William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

UNIT I – INTRODUCTION

PART-A

1. What is cryptography?(Remember)

An original message in a communication is known as the plaintext, while the coded message is called the cipher text. The process of converting from plaintext to cipher text is known as enciphering or encryption. The process of restoring the plaintext from the cipher text is deciphering or decryption. The many schemes used for encryption constitute the area of study known as cryptography.

2. Define security attack and mechanism?(Remember)

A security attack is defined as an action that compromises the security of information owned by an organization. A Security mechanism is a process that is designed to detect, prevent, and recover from a security attack.

3. What is meant by passive and active attack?(Nov/Dec 2017)(Remember)

Passive attacks are in the nature of eavesdropping, or monitoring of transmissions. The types of passive attack include the release of message content and traffic analysis. Active attacks involve some modification of data stream or creation of a false stream. The types of active attack includes masquerade, Replay, Modification, Denial of service.

4. What are the various security services?(Remember)

- ➢ Access control
- ➢ Data confidentiality
- ➢ Data Integrity
- ➢ Non Repudiation
- ➢ Authentication

5. How does simple columnar transposition work?(Remember)

This works by writing the message in a rectangle, row by row and read the message off, column by column, but permutes the order of the columns. The order of the columns then becomes the key to the algorithm.

6. What is meant by Steganography?(Remember)

A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

7. What are the types of attacks?(Remember)

Ciphertext Only

Known Plaintext

Chosen Plaintext

Chosen Ciphertext

Chosen Text

8. What is meant by Brute force attack?(Remember)

A **brute-force attack** involves trying every possible key until an intelligible translation of the cipher text into plaintext is obtained. On average, half of all possible keys must be tried to achieve success. That is, if there are X different keys, on average an attacker would discover the actual key after $X>2$ tries.

9. What is meant by substitution techniques?(Remember)
A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

10. What are the various substitution techniques used for encryption?(Remember)

> Caesar cipher
> Monoalphabetic cipher
> Playfair cipher
> Hill cipher
> Polyalphabetic cipher
> One time pad

11. What is meant by transposition technique?(Remember)
Transposition is achieved by performing some sort of permutation on the plaintext letters. The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

12. List out the problem of one time pad?(Analyze)
There is a practical problem in making large quantities of random keys. Daunting is a problem of key distribution and protection.For every message to be sent a key of equal length is needed by bith sender and receiver. Thus a mammoth key distribution problem exists.

13. Define LFSR sequence? (Understand)
A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is XOR. Thus, an LFSR is most often a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value.

14. What is the difference between monoalphabetic and polyalphabetic cipher? (Remember)
In monoalphabetic cipher single cipher alphabet is used per message. But in polyalphabetic cipher there are multiple ciphertext letters for each plaintext letter, one for each unique letter of keyword.

15. What is avalanche effect? (Remember)
A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect

16. Convert the given text "Anna University"into cipher text using rail fence technique? (Analyze)

> Ans: Anuiest nanvriy

17. Define integrity and Non - repudiation? (Remember)
Integrity - Service that ensures that only authorized person able to modify the message
Non repudiation - This service helps to prove that the person who denies the message transaction is true or false.

18. Define the following terms. (Remember)
Plaintext: the original message to be transmitted.
Cipher text: the coded (encrypted) message or the scrambled message.
Encryption / Enciphering: process of converting plain text to cipher text.
Decryption/ Deciphering: process of converting cipher text to plain text.

19. Define the two basic building blocks of encryption techniques (Remember).
i) Substitution technique – it is one in which the letters of the plaintext are replaced by other letters or by numbers or symbols. * Eg: Caeser cipher

ii) Transposition technique – it is one which performs some sort of permutation on the plaintext letters. * Eg: DES, AES

20. Define Diffusion and confusion. (Remember)

Diffusion - It means each plaintext digits affect the value of many cipher text digits which is equivalent to each cipher text digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and cipher text.

Confusion - It can be achieved by substitution algorithm. It is the relationship between cipher text and key.

21. Compare passive and active attack.(NOV/DEC 2016) (APR/MAY 2019) (Remember)

Passive attack	Active attacks
A passive attack involves someone listening in on telecommunications exchanges or passively recording computer activity	Active attacks on computers involve using information gathered during a passive attack, such as user IDs and passwords.

22. Why is asymmetric cryptography bad for huge data? Specify the reason. (Remember)
(APRIL/MAY 18)

1. Size of cryptogram: Symmetric encryption does not increase the size of the cryptogram (asymptotically), but asymmetric encryption does.
2. Performance: On a modern CPU with hardware AES support, encryption or decryption speed is over 2000 megabyte/second (per core).

23. Distinguish between attack and threat. (Understand) (NOV/DEC 18)

Threat: object, person, or other entity representing a constant danger to an asset

Attack: a deliberate act that exploits vulnerability

24. Calculate the cipher text for the following using one time pad cipher.
Plain text: ROCK & Keyword: BOTS. (Apply)   (NOV/DEC 18)

Plain text:	R(17)	O(14)	C(2)	K(10)
Keyword:	B(1)	O(14)	T(19)	S(18)
Plaintext + Keyword:	18	28	21	28
Plaintext + Keyword mod 26:	18	2	21	2
Cipher text:	**S**	**C**	**V**	**C**

25. What is Modern cryptography? (Remember)

Modern Cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.

26. What are the characteristics of Modern Cryptography? (Understand)

Classic Cryptography	Modern Cryptography
It manipulates traditional characters, i.e., letters and digits directly.	It operates on binary bit sequences.
It is mainly based on 'security through obscurity'. The techniques employed for coding were kept secret and only the parties involved in communication knew about them.	It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.

Classic Cryptography	Modern Cryptography
It requires the entire cryptosystem for communicating confidentially.	Modern cryptography requires parties interested in secure communication to possess the secret key only.

27. What is Cryptanalysis? (Remember)

Cryptanalysis is the study of cipher text, ciphers and cryptosystems with the aim of understanding how they work and improving techniques for defeating or weakening them. For example, Cryptanalysis seek to decrypt cipher text without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it; cryptanalysis also target Secure hashing, digital signatures and other cryptographic algorithms.

28. Define Perfect Security (Remember)

Perfect Security is a special case of information-theoretic security, for an encryption algorithm, if there is ciphertext produced that uses it, no information about the plaintext is provided without knowledge of the key.

If *E* is a perfectly secure encryption function, for any fixed message *m*, there must be, for each ciphertext *c*, at least one key *k* such that $c=E_k(m)$

Mathematically, let *m* and *c* be the random variables representing the plaintext and ciphertext messages, respectively; then, we have that $I(m;c)=0$

where $I(m;c)=0$ is the mutual information between m and c. In other words, the plaintext message is independent of the transmitted ciphertext if we do not have access to the key. It has been proved that any cipher with the perfect secrecy property must use keys with effectively the same requirements as one-time pad keys.

29. What are the components of Cryptosystem?

- Plaintext
- Encryption Algorithm
- Ciphertext
- Decryption Algorithm
- Encryption Key
- Decryption Key

30. Access the following cipher text using Brute Force attack. CMTMROOEOORW (Understand) (Hint : Rail Fence Technique)

Divide the given cipher text into two halves (Here n=12)
First half ☾ CMTMRO Second half ☾ OEOORW

C		M		T		M		R		O	
	O		E		O		O		R		W

Read the character in Zig Zag Manner.

Encrypted Text ☾ COME TOMORROW

31. Define Product Cryptosystem. (Remember)
A product cryptosystem is a block cipher that repeatedly performs substitutions and permutations, one after the other, to produce cipher text.

PART-B

1. Encrypt the message "PAY" using hill cipher with the following key matrix and show the decryption to get the original plain text**.(Understand)**

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}.$$

2. Using playfair cipher algorithm encrypt the message using the key "MONARCHY "and explain? **.(Understand)**
3. What is steganography? Describe the various techniques used in steganography. **(APR/MAY 2019) (Remember)**
4. **What is** monoalphabetic cipher/Examine how it differs from Cesar cipher. **(APR/MAY 2019) (Remember)**
5. Explain the Cesar cipher and monoalphabetic cipher? **.(Understand)**
6. What are the different types of attacks? Explain? **(Remember)**
7. Explain the substitution encryption techniques in detail? **(Remember)**
8. Describe the classical cryptosystems and its types? **(Remember)**
9. Explain the OSI security architecture with an example?**(NOV/DEC 2016) (APR/MAY 2019) (Remember)**
10. Describe the various security mechanisms**. (NOV/DEC 2016) (Remember)**
11. Encrypt the following using play fair cipher using the keyword MONARCIIY.
    "SWARAJ IS MY BIRTH RIGHT'. Use X for blank spaces**(NOV/DEC 2017) (Understand)**
12. Explain public key cryptography and when it is preferred? .**(APR/MAY 2019)**
13. Explain classical encryption techniques with symmetric cipher and Hill cipher model. **(Understand)**   **(APRIL/MAY 18)**
14. Describe   (i) Playfair cipher   (ii) Railfence cipher   (iii)Vignerecipher
    (APR/MAY 2017) (Remember)
15. Perform Encryption & decryption using Hill Cipher for the following. Message PEN and Key: ACTIVATED **(Understand) (NOV/DEC 18)**
16. Elaborate on the following topics **(Remember)**
       i) Perfect Security
       ii) Information Theory
       iii) Product Cryptosystem
17. Write a note on different types of Security Attacks and Services in Detail **(Remember) (NOV/DEC 19)**

PART-C

1. Using the positional value of alphabets represent them in 5 bit binary. Apply the transformation $c_1 = k_i \oplus P_i$, $p_i = c_i \oplus k_i$ where p_i = "scheme",k_i = Cipher. Find the cipher text. (Evaluate)
2. Applying   Caesar   Cipher   and   k=5   decrypt   the   given   Cipher   Text "YMJTYMJWXNIJTKXNQJSHJ".
3. Applying Vigenere Cipher, encrypt the word "explanation" using the key "leg".

ASSIGNMENT - 1

1. Using playfair cipher algorithm encrypt the message "HIDE THE GOLD" using the key "EXAMPLE "and explain? **(Understand)**
2. Using playfair cipher algorithm encrypt the message " Semester result" using the key "Examination "and discuss the rules to be followed.**(APR/MAY 2019)** **(Understand)**

UNIT II – SYMMETRIC KEY CRYPTOGRAPHY

PART A

1. Differentiate public key and conventional encryption? (APR/MAY 2017)(Analysis)

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

2. What are the principle elements of a public key cryptosystem?(Remember) (APR/MAY 2019)
The principle elements of a cryptosystem are:
  1. Plain text
  2. Encryption algoritm
  3. Public and private key
  4. Cipher text
  5. Decryption algorithm

3. What are roles of public and private key? (Remember)
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

4. Specify the applications of the public key cryptosystem? (Remember)(APR/MAY 2019)

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.

5. What requirements must a public key cryptosystem to fulfill to a secured algorithm? (Remember)

The requirements of public-key cryptosystem are as follows:

1. It is computationally easy for a party B to generate a pair (Public key KU_b, Private key KR_b)

2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext: $C=EKU_b(M)$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: $M=DKRb(C)=DKRb[EKUb(M)]$

4. It is computationally infeasible for an opponent, knowing the public key,KUb,to determine the private key,KRb.

5. It is computationally infeasible for an opponent, knowing the public key,KUb, and a ciphertext, C, to recover the original message,M.

6. The encryption and decryption functions can be applied in either order: $M=EKUb[DKRb(M)]=DKUb [EKRb(M)]$

6. What is a one way function? (Remember)

One way function is one that map the domain into a range such that every function value has a unique inverse with a condition that the calculation of the function is easy where as the calculations of the inverse is infeasible.

7. What is a trapdoor one way function? (Remember)

It is function which is easy to calculate in one direction and infeasible to calculate in other direction in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time. It can be summarized as: A trapdoor one way function is a family of invertible functions fk, such that

$Y= fk(X)$ easy, if k and X are known

$X=fk -1(Y)$ easy, if k and y are known

$X= fk -1(Y)$ infeasible, if Y is known but k is not known

8. List four general characteristics of schema for the distribution of the public key? (Remember)

The four general characteristics for the distribution of the public key are

1. Public announcement

2. Publicly available directory

3. Public-key authority

4. Public-key certificate

9. What is a public key certificate? (Remember)

The public key certificate is that used by participants to exchange keys without contacting a public key authority, in a way that is as reliable as if the keys were obtained directly from the

public-key authority. Each certificate contains a public key and other information, is created by a certificate authority, and is given to a participant with the matching private key.

10. Find gcd (1970, 1066) using Euclid's algorithm? (Apr/May 17 & NOV/DEC 2016) (Remember)

gcd (1970,1066) = gcd (1066,1970 mod 1066) = gcd (1066,904) = 2

11. What is the primitive root of a number? (Remember)

We can define a primitive root of a number p as one whose powers generate all the integers from 1 to p-1. That is p, if a is a primitive root of the prime number p then the numbers.

12. Plan on number of keys that are required by two people to communication via a cipher (Understand)

For Symmetric Single key is used to encrypt and decrypt while communicating via cipher while in asymmetric two key are used, one for encryption and one for decryption. So in symmetric sender and receiver uses same keys while in asymmetric sender uses one while receiver uses different to decrypt the cipher text.

13. Solve 11^7 mod 13. (Evaluate)

Split the power, $\quad 11^2$ mod 13 = 121 mod 13 = 4

11^4 mod 13 = 11^2 mod 13 x 11^2 mod 13 = 4 x 4 mod 13 = 3

11^7 mod 13 = (11^1 x 11^2 x 11^4) mod 13 = 132 mod 13 = 2.

Therefore, 11^7 mod 13 = 2.

14. What are the modes of DES? (NOV/DEC 2013) (Remember)

Four modes, called the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

15. List the uses of RC4. (NOV/DEC 2013) (Remember)

RC4 is used in
1. Secure Sockets Layer/Transport Layer Security (SSL/TLS)standards,
2. Wired Equivalent Privacy(WEP) protocol,
3. WiFi Protected Access (WPA) Protocol

16. What is optimal Asymmetric Encryption Padding? (MAY/JUNE 2014) (Remember)

In cryptography, Optimal Asymmetric Encryption Padding (OAEP) is a padding scheme often used together with RSA encryption.

17. What are the disadvantages of double DES? (NOV/DEC 2012)

➢ Meet-in-the-middle attack is possible in triple DES. **(Remember)**
➢ Need more memory space for encryption and decryption.

18. State few applications of RC4 algorithm. (APR/MAY 2015) (Remember)

➢ Secure Sockets Layer/Transport Layer Security (SSL/TLS)standards,
➢ Wired Equivalent Privacy(WEP) protocol,
➢ WiFi Protected Access (WPA) Protocol

19. Is it possible to use the DES algorithm to generate message authentication code? Justify. (NOV/DEC 2014) (Analysis)

Data Authentication Algorithm (DAA) is a widely used MAC based on DES-CBC using IV=0 and zero-pad of final block encrypt message using DES in CBC mode and send just the final block as the MAC or the leftmost M bits (16_M_64) of final block but final MAC is now too small for security.

20. State whether symmetric and asymmetric cryptographic algorithms need key exchange. (MAY/JUNE 2014) (Analysis)

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key.

21. Brief the strength of Triple DES. (NOV/DEC 2016) (Remember)

Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).

22. Give the significance of hierarchical key control. (NOV/DEC 2017) (Remember)

There can be local KDC responsible for small domain in the large networks. When the two principals are in the same domain the local KDC does the key distribution. When the two principals are in different domain, the local KDC communicates to the global KDC. The key selection can be done by anyone KDC. The numbers of layers depend upon the network size.

23. List the parameters (block size, key size and no of rounds) for the three AES versions. (Remember)

(APRIL/MAY 18)

Key size	4/16/128	6/24/192	8/32/256
Plaintext block size	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size	4/16/128	4/16/128	4/16/128

24. Give the five modes of operations in block cipher.(Apr/May 2017) (Remember)

i) Electronic Codebook(ECB) Mode, ii) CBC (Cipher-Block Chaining) Mode,
iii) CFB (Cipher Feedback) Mode,   iv) OFB (Output Feedback) Mode,
v) CTR (Counter) Mode.

25. Compare DES and AES. (Remember) (NOV/DEC 18)

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

26. Why is trap door one way function used? (Remember) (NOV/DEC 18)

A trapdoor one-way function is a function that is easy to compute in one direction, yet believed to be difficult to compute in the opposite direction (finding its inverse) without special information, called the 'trapdoor". Trapdoor functions are widely used in cryptography.

27. Why the middle portion of triple DES is a decryption rather than encryption? (Understand)

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 by repeating the key.

28. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? (Understand)

In some modes, the plaintext does not pass through the encryption functions, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

29. When is encryption scheme unconditionally and computationally secure? (Understand)

An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be **computationally secure** if

- 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.

30. If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate? (Understand)

Nine plaintext characters are affected. The plaintext character corresponding to the ciphertext character is obviously altered. In addition, the altered ciphertext character enters the shift register and is not removed until the next eight characters are processed.

31. Why a large quantity of random keys is undesirable? (Understand)

There is the practical problem of making large quantities of random keys.

Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is significant task.

Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

32. What are the requirements needed for secure use of Conventional Encryption. (Understand)

(i). A strong encryption algorithm is needed. It is desirable that the algorithm should be in such a way that, even the attacker who knows the algorithm and has access to one or more cipher texts would be unable to decipher the ciphertext or figure out the key.

(ii).The secret key must be distributed among the sender and receiver in a much secured way. If in any way the key is discovered and with the knowledge of algorithm, all communication using this key is readable.

33. List out the parameters of AES (NOV/DEC 2011) (Understand)

The parameters of AES includes

- Key size(words/bytes/bits)
- Plaintext Block size(words/bytes/bits)
- Number of rounds
- Round key size(words/bytes/bits)
- Expanded key size(words/bytes)

34. Difference between linear and differential cryptanalysis? (APR/MAY 2012)(Analysis)

      i) With differential cryptanalysis, the known plaintext/cipher text pairs must be organized in pairs where both plaintexts differ by a specific difference. Successful differential cryptanalysis normally requires **chosen** plaintext/cipher text pairs

      ii) With linear cryptanalysis, the approximation is a linear formula which links together some input bits, some output bits and some key bits, with a probability somewhat higher than what could be obtained with pure random. For linear cryptanalysis, known random plaintexts are sufficient, but differential cryptanalysis requires chosen plaintexts

35. Briefly define a Group, a Ring and a Field. (Remember) [NOV/DEC 19]

A **Group** is a set of elements that is closed under a binary operation and that is associative and that includes an identity element and an inverse element.

A **Ring** is a set of elements that is closed under two binary operations, addition and multiplication, with the following: the addition operation is a group that is commutative; the multiplication operation is associative and is distributive over the addition operation.

A **Field** is a ring in which the multiplication operation is commutative, has no zero divisors and includes an identity element and an inverse element.

36. Does the set of residue classes modulo 3 forms a group. (Analyze) [NOV/DEC 19]

      (a) with respect to addition?

      (b) with respect to multiplication?

Here are the addition and multiplication tables

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	2	0	1

(a) Yes. The Identity element is 0, and the inverses of 0, 1, 2 are respectively 0, 2, 1.

(b) No. The Identity element is 1, but 0 has no inverse.

37. Prove that [(a mod n) - (b mod n)] mod n = (a - b) mod n. (Evaluate)

Let c = a mod n and d = b mod n. Then

      c = a + kn; d = b + mn; c - d = (a - b) + (k - m) n

Therefore (c - d) = (a - b) mod n.

38. List the entities that are to be kept secret in conventional encryption techniques (Understand) (NOV/DEC 19)

- Plaintext
- The type of operations used for performing plaintext to ciphertext (Encryption Algorithm)
- The number of keys used. (Key Generator)
- The way in which plaintext is processed.
- Decryption Algorithm

PART – B

1. Write down Triple DES algorithm and explain with neat diagram. **(NOV/DEC 2013)/ (MAY/JUNE 2013) (APR/MAY 2019) (Remember)**
2. Describe the working principles of simple DES with an example.**(MAY/JUNE 2014)/ (APR/MAY 2015) (Understand)**
3. Briefly explain Diffie-Hellman Key Exchange. **(MAY/JUNE 2014)/ (NOV/DEC 2012) (APR/MAY 2017) (Understand)**
4. Discuss in detail the encryption and decryption process of AES**. (NOV/DEC 2016) (Understand)**
5. Brief out the encryption and decryption process of DES and depict the general structure. List out the strength and weakness of the same. **(NOV/DEC 2014) (Understand)**
6. What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example. **(APRIL/MAY 18) (Understand)**
7. Describe DES algorithm and explain with neat diagram and explain the steps.**(APR/MAY 2017) (Understand)**
8. Describe in detail the key generation in AES algorithm and its expansion format. **(APR/MAY 2019) (Understand)**
9. Discuss the properties that are to be satisfied by Groups, Rings and Fields. **(NOV/DEC 2017) (Create)**
10. Explain in detail about the entities in the symmetric cipher model with their requirements for secure usage of the model. **(Remember) [NOV/DEC 19]**
11. Demonstrate that the set of polynomials whose coefficients form a field is a ring. **(Understand) [NOV/DEC 19]**

PART-C

1. For each of the following elements of DES, indicate the comparable element in AES if available.

    i) XOR of subkey material with the input to the function.

    ii) f function.

    iii) Permutation p.

    iv) Swapping of halves of the block. **(Analysis)**   **(NOV/DEC 2017)**

2. How the counter mode is used for enhancing the effect of a cryptographic algorithm? **(Understand)**

3. Given 10 bit 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? **(Evaluate)**

ASSIGNMENT – 2

1. Formulate Triple DES and its applications and design the key discarding process of DES. **(Understand)**

2. Discuss about Differential and Linear Cryptanalysis. **(Remember)**

3. Describe the Meet-in-the-Middle Attack **(Understand)**

UNIT III – PUBLIC KEY CRYPTOGRAPHY

PART – A.

1. Define replay attack (NOV/DEC 2011) (Remember)

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

2. Write the difference between public key and private key crypto systems? (APR/MAY 2012&APR/MAY 2017)(Analysis)

Private Key encryption uses a single key to both encrypt and decrypt messages. It must be present at both the source and destination of transmission to allow the message to be transmitted securely and recovered upon receipt at the correct destination.

Public key systems use a pair of keys, each of which can decrypt the messages encrypted by the other. Provided one of these keys is kept secret (the private key), any communication encrypted using the corresponding public key can be considered secure as the only person able to decrypt it holds the corresponding private key.

3. State whether symmetric and asymmetric cryptographic algorithms need key exchange? (APR/MAY 2014)(Analysis)

Key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

Symmetric encryption requires the sender and receiver to share a secret key. Asymmetric encryption requires the sender and receiver to share a public key. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

4. List the Authentication requirements? (APR/MAY 2014) (NOV/DEC 2016)(Understand)

The authentication is provided for the following attacks

> ➢ Disclosure
> ➢ Traffic analysis
> ➢ Masquerade
> ➢ Content modification
> ➢ Sequence modification
> ➢ Timing Modification
> ➢ Source repudiation
> ➢ Destination Repudiation

5. Point out the types of cryptanalytic attacks?(NOV/DEC 2014) (Remember)

The two types of cryptanalytic attacks includes the

> ➢ Attacks on hash functions
> ➢ Attacks on message authentication codes

6. What is Man in the Middle attack? (Remember)

This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function.

7. Specify the various types of authentication protocols.(Apr/May 2017) **(Remember)**
- PAP - Password Authentication Protocol.
- CHAP - Challenge-handshake authentication protocol.
- EAP - Extensible Authentication Protocol.
- TACACS, XTACACS and TACACS+
- RADIUS.
- DIAMETER.
- Kerberos (protocol)

8. What is the Fermat's theorem? (Nov/Dec 2017)? (Remember)
Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1(\mathrm{mod}\,p)$$

9. What is the use of Fermat's theorem? (Remember)
- ➢ This theorem is central to the calculus method of determining maxima and minima: in one dimension, one can find extreme by simply computing the stationary points (by computing the zeros of the derivative), the non- differentiable points, and the boundary points, and then investigating this set to determine the extreme.
- ➢ One can do this either by evaluating the function at each point and taking the maximum, or by analyzing the derivatives further, using the first derivative test, the second derivative test, or the higher-order derivative test.
- ➢ In dimension above 1, one cannot use the first derivative test any longer, but the second derivative test and higher-order derivative test generalize.

10. Describe Chinese remainder theorem.(Understand)
The Chinese remainder theorem is a result about congruences in number theory and its generalizations in abstract algebra. In its basic form, the Chinese remainder theorem will determine a number n that when divided by some given divisors leave given remainders.

11. Define Euler's theorem and it's application? (APRIL/MAY 18) (Remember)
Euler's theorem states that for every **a** and **n** that is relatively prime:

$$a^{\Phi(n)} \equiv 1 \bmod n$$

12.Define Euler's totient function or phi function and their applications? (Remember)
The Euler's totient function states that, it should be clear for a prime number p,

$$\Phi(p) = p-1$$

13. Describe in general terms an efficient procedure for picking a prime number? (Remember)
The procedure for picking a prime number is as follows:

1. Pick an odd integer n at random (eg., using a pseudorandom number generator).

2. Pick an integer a<n at random.

3. Perform the probabilistic primality test, such as Miller-Rabin. If n fails the test, reject the value n and go to step 1.

4. If n has passed a sufficient number of tests, accept n; otherwise, go to step 2.

14. Define Fermat Theorem? (Apr/May 17) (Remember)

Fermat Theorem states the following: If p is prime and a is a positive integer not divisible by p, then $A^{p-1} \equiv 1 \bmod p$

15. What is discrete Logarithm?(Remember)

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm. Consider the equation

$$y = g^x \bmod p$$

Given *g*, *x*, and *p*, it is a straightforward matter to calculate *y*. At the worst, we must perform *x* repeated multiplications, and algorithms exist for achieving greater Efficiency.

16. User A and B exchange the key using Diffie-Hellman algorithm. Assume ☐ = 5 q=11 X_A =2 X_B =3. Find the value of Y_A , Y_B and k?(Analysis)

Y_A	$= \square^{X}_{A} \bmod q$	= 25 mod 11	= 3
Y_B	$= \square^{X}_{B} \bmod q$	= 125 mod 11	= 4
$K = (Y_A)^{X}_{B} \bmod q$		= 27 mod 11	= 5
$K = (Y_B)^{X}_{A} \bmod q$		= 16 mod 11	= 5

17. Perform encryption and decryption using RSA Alg. for the following. (NOV/DEC 2017) P=7; q=11; e=17; M=8.   (APRIL/MAY 18)

  Soln:

$$n = pq$$
$$n = 7*11 = 77$$
$$\Phi(n) = (p-1)(q-1)$$
$$= 6*10 = 60$$

e =17 , d =27

$$C = M^e \bmod n$$
$$C = 817 \bmod 77$$
$$= 57$$
$$M = C^d \bmod n$$
$$= 5727 \bmod 77$$
$$= 8$$

18. What is an elliptic curve? (NOV/DEC 2016) (Remember)

The principle attraction of ECC compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.

19. Define Euler's phi function. (Remember)

Euler's phi function ⋅(n) returns the number of integers from GCD 1 to n that are relatively prime to n. The phi function is computed ⋅(n) using various methods. They are

1. If n is a prime number, then ⋅(n)=n-1.

2. If n is a composite number, then

2.1 Find the prime factors of that number and compute the phi function value as used in Step 1.

otherwise,

2.2 Find prime powers (P^a) of the given number n, for computing the phi value of prime powers we have to use ($P^a - P^{a-1}$)

20. Mention any three Primality Testing Methods. (Remember)

1. Naïve Algorithm

2. Fermat's Primality Test

3. Miller-Rabin Primality Test

21. Write the formula for Encryption and Decryption in RSA. (Remember)

For Decryption $C = M^e \bmod n$

For Encryption $M = C^d \bmod n$

22. Consider the RSA encryption method with p=11 and q=17 as the two primes.
Find n and ·(n). (Evaluate) [NOV/DEC 19]

$$n = p \times q = 17 \times 11 = 187$$
$$·(n) = (p-1)(q-1) = (17-1)(11-1)$$
$$= 16\,(10)$$
$$= 160.$$

PART – B

1. Write short notes on Fermat's theorem, Euler's theorem and Chinese remainder theorem? **(NOV/DEC 2016)** (Understand)

2. State Chinese Remainder theorem and find X for the given set of congruent equations Using CRT. **(NOV/DEC 2016)(Understand)**

   $X=2(\bmod\ 3)$

   $X=3(\bmod\ 5)$

   $X=2(\bmod\ 7)$

3. Solve gcd (98,56)using Extended Euclidean algorithm. Write the algorithm also. **(Understand) (NOV/DEC 18)**

4. Explain about the RSA algorithm with the example as: **(NOV/DEC 2013)(Understand)**
   p=11, q=5, e=3 and PT=9.

5. Demonstrate Encryption and Decryption for the RSA algorithm parameters p=3, q=11, e=7, d=?, M=5. **(MAY/JUNE 2014)/ (NOV/DEC 2012) (APR/MAY 2019) (Analysis)**

6. 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 X_A=5, what is A's public key Y_A?. **(MAY/JUNE 2014)/ (MAY/JUNE 2013)(Analysis)**

7. Explain RSA algorithm in detail, for the given values trace the sequence of calculations in RSA. P=7, q=13, e=5, and M=10. **(APR/MAY 2015) (Understand)**

8. Describe the mathematical foundations of RSA algorithm. Perform encryption and decryption for the following, p=17, q=7, e=5, n=119, message ="6". Use extended Euclid's algorithm to find the private key. **(NOV/DEC 2014) (APR/MAY 2019) (Analysis)**

9. With a neat sketch explain the Elliptic curve cryptography with an example. **(APRIL/MAY 18) (Understand)**

10. Perform encryption & decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 88. **(Understand)**   **(NOV/DEC 2018)**

11. Find the secret key shared between user A & user B using Diffie Hellman algorithm for the following.

    Q = 353, α (primitive root) = 3, X_A = 45 & X_B = 50 **(Understand) (NOV/DEC 2018)**

12. Demonstrate Encryption and Decryption for the RSA algorithm parameters p=3, q=11, e=7, d=?, M=5 **(Evaluate)**

12. Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime
q = 83 and a primitive root □= 5. **(Analyze)**
  i) If Alice has a private key Xa = 6, what is Alice's public key?
  ii) If Bob has a private key Xs = 10, what is Bob's public key?
  iii) What is the shared secret key?
13. Explain Diffie-Hellman Key exchange algorithm in detail **(Remember) [NOV/DEC 19]**
14. Explain the working of RSA and choose an application of your choice for RSA and show how
encryption and decryption is carried out. **(Understand) [NOV/DEC 19]**

PART – C

1. State Chinese Remainder theorem and find X for the given set of congruent
 equations using CRT. **(APR/MAY 2017) (Understand)**
  X=2(mod 3)
  X=1(mod 5)
  X=1(mod 5)
  X=3(mod 9)
  X=4(mod 11)
2. State and prove the Chinese remainder theorem. What are the last two digits of 49^{19}? (Evaluate)
(APRIL/MAY 18)
3. Consider the elliptic curve E11 (1, 6); that is the curve is defined by y2=x3+x+6with a module
of P=11. Calculate all the points in E11 (1, 6). Start by calculation by the right hand side of the
equation for all the values of n? **(Evaluate)**
4. Explain RSA algorithm, perform encryption and decryption to the system with p=7, q=11,
e=17, M=8. **(Understand) (NOV/DEC 2016) (NOV/DEC 2017)**
5. Why ECC is better the RSA? However, why is it not widely used? Defend it. **(Understand)**
(NOV/DEC 2018)

ASSIGNMENT - 3

1. Explain MILLER RABIN PRIMALITY Algorithm. **(Understand)**
2. 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 X_A=5, what is A's public key Y_A?. **(Evaluate)**
3. Alice wants to generate a pair of RSA public and private keys. She starts by selecting two
primes p = 5 and q = 7. **(Evaluate)**
(a) Compute n, □1(n)?
(b) In selecting a decryption (private) key d, Alice decides d = 3 is not good. Why? She selects d
= 11 instead. Which is correct encryption (public) key, e1 = 11 or e2 = 13?
(c) Suppose Bob wants to send a message M = 33 to Alice, Which key should he use? What's the
cipher text he sends to Alice?
(d) After Alice receives the cipher text, how does she decrypt?
(e) If Alice wants to send B a signed message, given M' = 6, what would Alice send?
(f) How does Bob verify the message sent by Alice?

UNIT IV – MESSAGE AUTHENTICATION AND INTEGRITY

PART - A

1. What are the functions used to produce an authenticator? (APR/MAY 2019) (NOV/DEC 2009) (Remember)

The functions that are used to produce the message authenticator includes,
- ➤ Message Encryption function
- ➤ Message Authentication code
- ➤ Hash Function

2. List the properties a digital signature should possess?   (NOV/DEC 2009)

The digital signature must have the following properties:
- ➤ It must verify the author and the date and time of the signature.
- ➤ It must authenticate the contents at the time of the signature.
- ➤ It must be verifiable by third parties, to resolve disputes

3. What do you mean by MAC? (Remember)

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

$$MAC = C_k(M)$$

Where M = variable length message K = secret key shared by sender and receiver. $C_K(M)$ = fixed length authenticator.

4. What is meant by Hash function? (APRIL/MAY 18) (Remember)

A hash function H accepts a variable-length block of data M as input and produces a fixed-size hash value h = H(M). The principal objective of a hash function is data integrity. A change to any bit or bits in M results, with high probability, in a change to the hash code. The kind of hash function needed for security applications is referred to as a cryptographic hash function.

5. Mention the fundamental idea of HMAC. (APR/MAY 2009) (Remember)

The fundamental idea behind HMAC is to reuse the existing message digest algorithm such as MD5 and SHA – 1. It treats the message digest as a black box. Additionally it uses the shared symmetric key to encrypt the message digest which produces the output MAC.

6. What do you mean by one way property in hash function? (APR/MAY 2011)(NOV/DEC 2012) (Remember)

The one way property of hash function indicates that it is easy to generate a code given a message, but virtually impossible to generate a message given a code. This property is important if the authentication technique involves the use of a secret value.
- ➤ For any given value h, it is computationally infeasible to find x such that
  H(x) = h – one way property.
- ➤ For any given block x, it is computationally infeasible to find y ≠ x
  with H(y) = H(x) – weak collision resistance.

It is computationally infeasible to find any pair (x, y) such that H(x) = H(y) – strong collision property

7. What are the two approaches of digital signature? (NOV/DEC 2012) (Remember)

The two approaches of digital signature includes,
- ➤ Direct Digital Signature
- ➤ Arbitrated Digital signature

8. What is weak collision Resistance? (**APR/MAY 2013**) (**Remember**)

For a hash value, h=H(x) we say that x is the pre image of h. That is x is a data block whose hash function, using the function H, is h. Because H is a many-to-one mapping, for any given hash value h, there will in general be multiple pre images. A collision occurs if we have x≠y and H(x) = H(y).The weak collision resistance states that for any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x).

9. List any three hash algorithm.(Understand)
1. MD5 (Message Digest version 5) algorithm.
2. SHA_1 (Secure Hash Algorithm).
3. RIPEMD_160 algorithm.

10. What is the role of compression function in hash function? (APR/MAY 2017)
(Remember)

The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value usually b>n; hence the term compression.

11. What requirements should a digital signature scheme should satisfy? (Remember)
- The signature must be bit pattern that depends on the message being signed.
- The signature must use some information unique to the‧ sender, to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

12. What are the requirements of the hash function? (Remember)
- H can be applied to a block of data of any size.
- H produces a fixed length output.
- H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

13. How is the security of a MAC function expressed ? (**NOV/DEC 2017**)(**Understand**)

The security of a MAC function expressed in terms of the probability of successful forgery with a given amount of time spent by the forger and a given number of message-MAC pairs created with the same key.

14. Mention the significance of signature function in Digital Signature Standard (DSS)
approach. (**NOV/DEC 2017**) (**Remember**)

A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key.

15. How a digital signature differs from authentication protocols? (APRIL/MAY 18) (Remember)

MACs can be created from unkeyed hashes (e.g. with the HMAC construction), or created directly as MAC algorithms.

A (digital) signature is created with a private key, and verified with the corresponding public key of an asymmetric key-pair. Only the holder of the private key can create this signature, and normally anyone knowing the public key can verify it. Digital signatures don't prevent the replay attack mentioned previously.

16. Define the term message digest. (Understand)   (NOV/DEC 2018)

A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula

17. Contrast various SHA algorithms. (Understand)   (NOV/DEC 2018)

SHA-0: The original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.

SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm.

SHA-2: A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.

SHA-3: It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

18. What are birthday attacks? (APR/MAY 2014) (Remember)

If an encrypted 64 bit hash code C is transmitted with the corresponding unencrypted message M , then an opponent would need to find an $M^{'}$ such that $H(M^{'}) = H(M)$ to substitute another message to substitute another message and fool the receiver. Thus the user has to try about 2^{63} combinations to find one that matches the hash code of the intercepted message. This is called as Birthday attack.

19. Define Kerberos. (Understand)

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.

20. What is Kerberos? What are the uses? (Understand)

Kerberos is an authentication service developed as a part of project Athena at MIT.Kerberos provides a centralized authentication server whose functions is to authenticate servers.

21. What 4 requirements were defined by Kerberos? (Remember)

> ➢ Secure

> ➢ Reliable

> ➢ Transparent

> ➢ Scalable

22. In the content of Kerberos, what is realm? (Understand)

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".

23. Assume the client C wants to communicate server S using Kerberos procedure.
How can it be achieved? (Analyze)

Dialogue between client 'C' , server 'S' and authentication server(AS) are given below

a) C → AS: [IDc|| Pc || IDs]
b) AS → C: Ticket
c) C → S: [IDc || ADc || IDs]
Ticket = EKs [IDc ||ADc || IDs]

Step 1: The user logon to workstation and request access to the server S. The client module C in the workstation request user password and sends message to AS that includes user ID(IDc), server ID(IDc) and its password.

Step 2: Now the AS verify users password against its password database, if it is valid. AS sends the ticket to C that includes user ID(IDc), server ID(IDs) and the address of the client workstation (ADc) are encrypted with key which is shared by both AS and server(S).

Step 3: Now the client use the ticket to server S, to send the message to S with IDc to access service

24. What is the purpose of X.509 standard? (Remember)

X.509 defines framework for authentication services by the X.500 directory to its users.X.509 defines authentication protocols based on public key certificates.

25. What you mean by VeriSign certificate? (Understand)

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

26. Write a simple authentication dialogue used in Kerberos. (NOV/DEC 2017) (Understand)

C   AS: $ID_C||P_C||ID_V$

(1) AS   C: Ticket
(2) C   V: $ID_C||Ticket$
Ticket = $E(K_v, [ID_C||AD_C||ID_V])$

27. List any 2 applications of X.509 Certificates. (NOV/DEC 2017)

Applications

➢ WWW,
➢ electronic mail,
➢ user authentication,
➢ IPsec.

28. List the 3 classes of intruder? (NOV/DEC 2016) (Remember) (APR/MAY 2019)

1) Masquerader
2) Misfeasor
3) Clandestine user.

29. Define CIA.

Confidentiality, Integrity and Availability also known as the CIA triad, is a model designed to guide policies for information security within an organization.

Confidentiality ☾ Is a set of rules that limits access to information.

Integrity ☾ Assurance that the information is trustworthy and accurate

Availability ☾ Is a guarantee of reliable access to the information by authorized people.
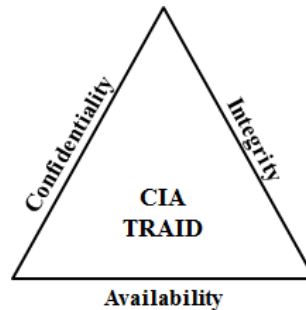
Fig. CIA Traid

30. State the requirements of a digital signature. (Remember) [NOV/DEC 19]

1. **Message Encryption:** The ciphertext of the entire message serves as its authenticator.
2. **Message Authentication Code (MAC):** A public function of the message and a secret key that produces a fixed length value that serves as the authenticator.
3. **Hash Functions:** A public function that maps a message of any length into a fixed length hash value, which serves as the authenticator

**31. What is realm in Kerberos? (Understand) [NOV/DEC 19]**

A realm is a logical network, similar to a domain that defines a group of systems under the same master KDC. The Figure below shows how realms can relate to one another. Some realms are hierarchical, where one realm is a superset of the other realm. Otherwise, the realms are non-hierarchical (or "direct") and the mapping between two realms must be defined. Kerberos cross-realm authentication enables authentication across realms. Each realm only needs to have a principal entry for the other realm in its KDC (Key Distribution Centre).

(OR)

Consider the following:

- A participant is registered with a Kerberos database, and this participant has their user ID (UID) and hashed password stored in a Kerberos server
- The Kerberos server shares a secret key with other Kerberos servers.

Therefore, A Kerberos realm is a set of these managed "nodes" that share the same Kerberos database.
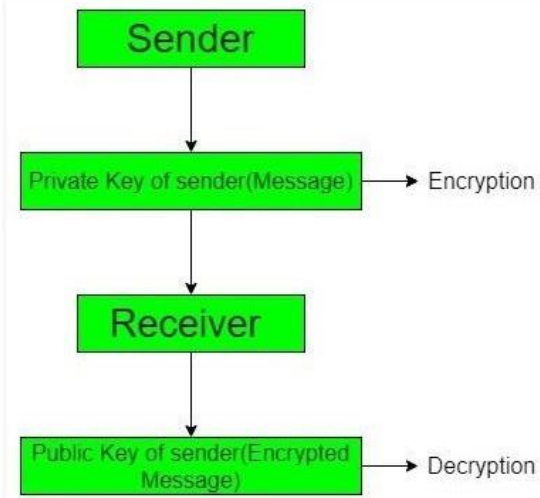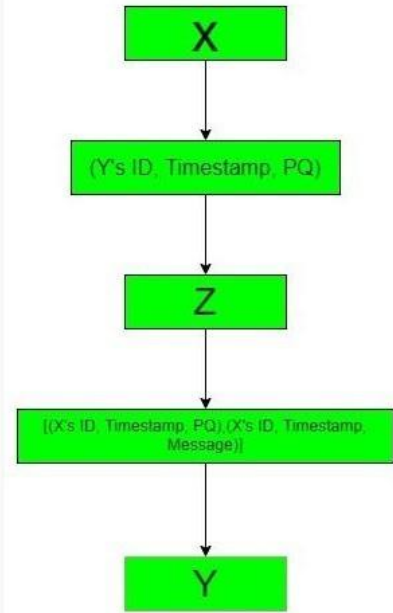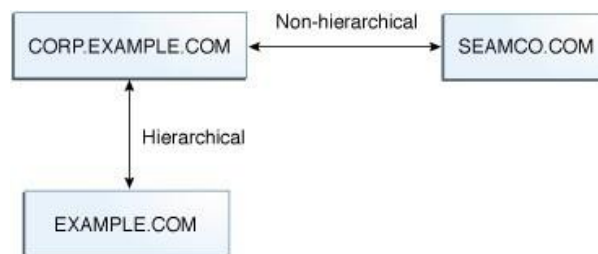

Fig. Kerberos Realm

32. What entities constitute a full service in Kerberos environment? (Remember) [NOV/DEC 19]

A full service environment consists of a

      i) Kerberos server,

      ii) Number of clients, and

      iii) Number of application servers.

33. Compare Direct and Arbitrated digital signature. (Understand) [NOV/DEC 19]

Direct Digital Signature	Arbitrated Digital Signature
A **direct digital signature** involves only the communicating parties (source, destination). It is assumed that the destination knows the public key of the source. A digital signature may be formed by encrypting the entire message with the sender's private key or by encrypting a hash code of the message with the sender's private key.	An **arbitrated digital signature** operates as follows. Every signed message from a sender X to a receiver Y goes first to an arbiter A, who subjects the message and its signature to a number of tests to check its origin and content. The message is then dated and sent to Y with an indication that it has been verified to the satisfaction of the arbiter.

PART - B

1. What are the properties a hash function must satisfy? (6) **(NOV/DEC 2009) (Remember)**

2. Explain MD5 Message Digest algorithm with its logic and compression function? (16) **(NOV/DEC 2009)(Understand)**

3. How does SHA-1 logic produce message digest? (10) **(APR/MAY 2009)(Analysis)**

4. Explain the challenges/ response approach in mutual authentication. (6) **(APR/MAY 2009) (Understand)**

5. Explain Digest signature algorithm (DSA) in detail. (10) **(APR/MAY 2009) (APR/MAY 2017) (Understand)**

6. What is Message Authentication? Explain. (6) **(APR/MAY 2009) (Remember)**

7. Discuss the discrete logarithm and explain Diffie – Hellman Key exchange algorithm with its merits and demerits **(APR/MAY 2011)**

8. Explain about MD5 in detail? **(APR/MAY 2011) (APR/MAY 2012) (APRIL/MAY 18) (Understand)**

9. Illustrate about SHA algorithm and explain? **(NOV/DEC 2011) (APR/MAY 2013)** **(NOV/DEC 2013)** **(NOV/DEC 2017) (Remember)**

10. Write a detailed note on digital signatures? **(NOV/DEC 2011) (Understand)**

11. Write notes on Birthday attack? **(APR/MAY 2012)** **(NOV/DEC 2013) (Understand)**

12. Describe about hash functions? **(NOV/DEC 2012)** **(NOV/DEC 2013) (Understand)**

13. Explain Digital signature with Elgamal Public key crypto systems? **(Understand)** **(NOV/DEC 2013)**

14. Explain Digital signature standard? **(APR/MAY 2014)(NOV/DEC 2016). (Understand)**

15. Describe MD5 algorithm in detail. Compare its performance with SHA-1. **(Understand).(NOV/DEC 2016) (APR/MAY 2019)**

16. Write down the steps involved in **(NOV/DEC 2017) (Understand)**

       i) EIgamaI Digital Signature Scheme.

       ii) Schnorr Digital Signature Scheme.

17. How Hash function algorithm is designed? Explain their features and properties. **(APRIL/MAY 18) (Understand)**

18. Describe digital signature algorithm and show how signing and verification is done using DSS**. (APR/MAY 2019) (Understand)**

19. Illustrate SHA2 in detail. (Remember) **(NOV/DEC 2018)**

20. Explain Elgamal digital signature scheme**. (Understand) (NOV/DEC 2018)**

21. Explain ElGamal public key crypto system with example. **(APR/MAY 2015) (Understand)**

22. i) Discuss the different methods involved in authentication of the source. (8) **(NOV/DEC 2017) (Analyze)**

   ii) Write about how the integrity of message is ensured without source authentication. (8) **(NOV/DEC 2017) (Analyze)**

23. i) Compare the uses of MAC and Hash function. Represent them using appropriate diagrams. **(Understand) [NOV/DEC 19]**

   ii) List down the advantages of MD5 and SHA Algorithm **(Remember) [NOV/DEC 19]**

24. List the design objectives of HMAC and explain the algorithm in detail **(Understand) [NOV/DEC 19]**

PART – C

1. Apply the MAC on the Cryptographic checksum method to authenticate build confidentiality of the message where the authentication is tied to the message M = 8376, K1 = 4892 and K2 = 53624071 (10) **(NOV/DEC 2009) (Analyze)**

2. Assume a client C wants to communicate with a server S using Kerberos protocol. How can it be achieved? **(NOV/DEC 2011) (APR/MAY 2014) (Evaluate)**

3. Compare the performance of RIPEMD-160 algorithm and SHA-1 algorithm. **(APR/MAY 2017) (Analysis)**

4. Summarize Client Server Mutual authentication, with example flow diagram **(OR)**
Discuss Client Server Mutual authentication, with example flow diagram. **(NOV/DEC 2016) (Understand)**

5. Explain breifly abouth the architecture and certification mechanisms in kerberos and X.509. **(APRIL/MAY 18) (Understand)**

6. Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer.

Transfer Amount	Cryptography Functions Required
1 - 2000	Message Digest
2001 - 5000	Digital Signature
5000 and above	Digital Signature and Encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations. **(Create) [NOV/DEC 19]**

7. Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption. **(Analyze) [NOV/DEC 19]**

ASSIGNMENT - 4

1. Illustrate about SHA algorithm and explain? **(Understand)**

2. Explain about MD5 in detail? **(Understand)**

3. Apply the MAC on the Cryptographic checksum method to authenticate build confidentiality of the message where the authentication is tied to the message M = 8376, K1 = 4892 and K2 = 53624071. **(Apply)**

UNIT V - SECURITY PRACTICE AND SYSTEM SECURITY

PART - A

1. What are the services provided by PGP services? (OR) List the five principal services provided by PGP. (APR/MAY 2013) (APRIL/MAY 18) (NOV/DEC 2018) [NOV/DEC 19] (Remember)

> ➢ Digital signature
> ➢ Message Encryption
> ➢ Compression
> ➢ E-mail compatibility
> ➢ Segmentation

2. Explain the reasons for using PGP? (Understand)

    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.
    c) E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128, IDEA, 3DES for conventional encryption, SHA-1for hash coding.
    d) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.
    e) It was not developed by nor is it controlled by any governmental or standards organization.

3. Why E-mail compatibility function in PGP needed? (Understand)

    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.

4. Name any cryptographic keys used in PGP? (Remember)

        a) One-time session conventional keys.

        b) Public keys.

        c) Private keys.

        d) Pass phrase based conventional keys.

5. Define key Identifier? (Remember)

    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.

6. List the limitations of SMTP/RFC 822?(NOV/DEC 2016) (Understand)

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

7. Define S/MIME? (Remember)

    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.

8. What are the elements of MIME? (Remember)

- 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.

9. What are the key algorithms used in S/MIME? (Remember)
   a) Digital signature standards.
   b) Diffie Hellman Key Exchange
   c) RSA algorithm.

**10. What are the headers fields define in MIME? (Remember) (APR/MAY 2019)**
   a) MIME version.
   b) Content type.
   c) Content Transfer encoding.
   d) Content id.
   e) Content description

11. Give the steps for preparing envelope data MIME? (Understand)
 Generate Ks.
   i) Encrypt Ks using recipient's public key.
   ii) RSA algorithm used for encryption.
   iii) Prepare the 'recipient info block'.
   iv)Encrypt the message using Ks

12. What is the general format for PGP message? (Understand)
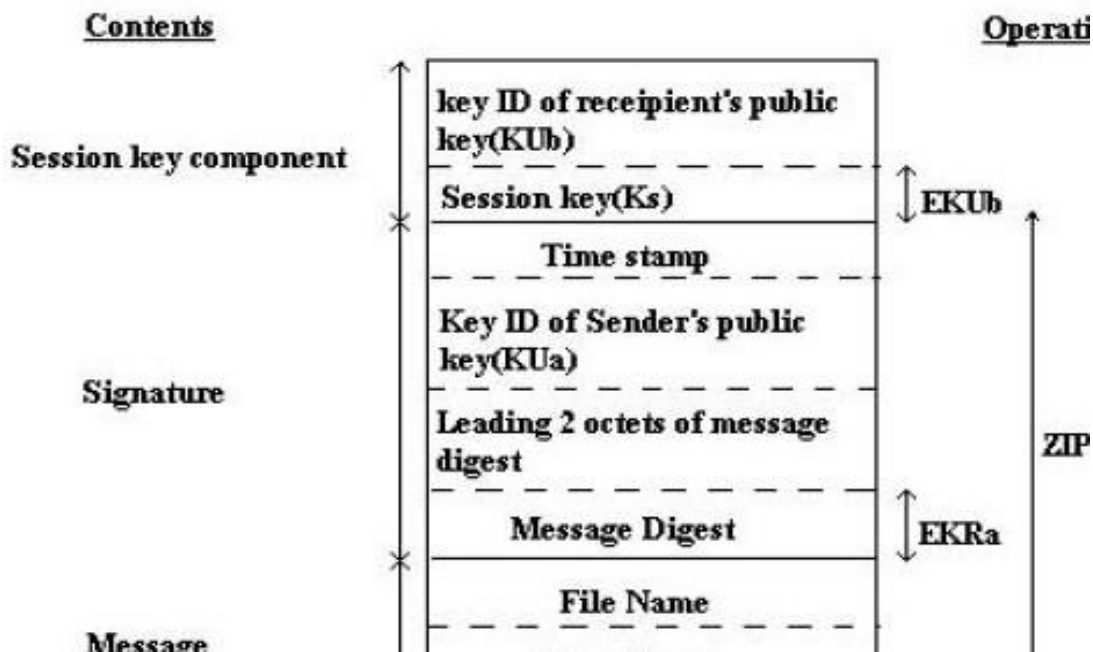
13. What is MIME content type and explain? (Remember)
   It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes.
   They are,
   1. Text type
   2. Multipart type
   3. Message type
   4. Image type
   5. Video type.
   6. Audio type.
   7. Application type

14. What you mean by Verisign certificate? (May 2015) (Understand)

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

15. What are the function areas of IP security? (Remember)

➢ Authentication

➢ Confidentiality

➢ Key management.

16. Give the application of IP security? (Remember)

➢ Provide secure communication across private & public LAN.

➢ Secure remote access over the Internet.

➢ Secure communication to other organization.

17. Give the benefits of IP security? (APRIL/MAY 17) (Remember) (APR/MAY 2019)

➢ 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.

18. What are the protocols used to provide IP security? (Remember)

➢ Authentication header (AH) protocol.

➢ Encapsulating Security Payload (ESP) protocol.

19. Specify the IP security services? (Understand)

i) Access control.

ii) Connectionless integrity.

iii) Data origin authentication

iv) Rejection of replayed packet.

v) Confidentiality.

vi) Limited traffic for Confidentiality.

20. What do you mean by Security Association? Specify the parameter that identifies the Security Association? (Understand)

➢ 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.

21. General format of IPsec ESP Format? (APRIL/MAY 17) (Remember)

Security Parameter Index(SPI)
Sequence Number(SN)
Payload Data (Variable)
Padding(0-255 bytes)
Authentication Data (variable)

22. Differentiate Transport and Tunnel mode in IPsec? (May 2015)   (NOV/DEC 2018) (Analyze)

Transport mode	Tunnel Mode
Provide the protection for upper layer protocol between two hosts.	Provide the protection for entire IP Packet.
ESP in this mode encrypts and optionally authenticates IP Payload but not IP Header.	ESP in this mode encrypt authenticate the entire IP packet.
AH in this mode authenticate the IP Payload and selected portion of IP Header.	AH in this mode authenticate the entire IP Packet plus selected portion of outer IP Header.

23. What is Authentication Header? Give the format of the IPsec Authentication Header? (Remember)

It provides the authentication of IP Packet, so authentication is based on the use of MAC.

First Header	Payload Length	Reserved
Security Parameter Index(SPI)		
Sequence number(SN)		
Authentication Data(Variable)		

25. List the steps involved in SSL record protocol? (Understand)

    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 algorithm.

26. Give SSL record format? (Remember)

Content type	Major Version	Minor Version	Compressed length
Plain Text(Optionally Compressed)			
MAC 0, 16 or 20 bytes.			

27. What are the different between SSL version 3 and TLS? (APRIL/MAY 18) (Analyze)
SSL TLS
- ➢ In SSL the minor version is 0 and * In TLS, the major version is 3 and the the major version is 3 minor version is 1.
- ➢ SSL use HMAC alg., except that * TLS makes use of the same alg. the padding bytes concatenation.
- ➢ SSL supports 12 various alert * TLS supports all of the alert codes codes. defined in SSL3 with the exception of no _ certificate.

28. What is mean by SET? What are the features of SET? (Understand)

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet.
Features are:
- i) Confidentiality of information
- ii) Integrity of data
- iii) Cardholder account authentication
- iv) Merchant authentication

29. What are the steps involved in SET Transaction? (Understand)
- ⁃ The customer opens an account
- ⁃ The customer receives a certificate
- ⁃ Merchants have their own certificate
- ⁃ The customer places an order.
- ⁃ The merchant is verified.
- ⁃ The order and payment are sent.
- ⁃ The merchant requests payment authorization.
- ⁃ The merchant confirm the order.
- ⁃ The merchant provides the goods or services.
- ⁃ The merchant requests payment.

30. What is dual signature? What it is purpose? (Remember)
The Dual Signature is a concept introduced with SET (Secure Electronic Transaction), the purpose of the dual signature is to link two messages that intended for two different recipients, and to avoid misplacement of orders.

31. Expand and define SPI .(APR/MAY 2013) (Understand)
The Security Parameter Index (SPI) is an identification tag added to the header while using IPsec for tunneling the IP traffic. This tag helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use.

The SPI is a required part of an IPsec Security Association (SA) because it enables the receiving system to select the SA under which a received packet will be processed. An SPI has only local significance, since it is defined by the creator of the SA; an SPI is generally viewed as an opaque bit string.

32. What are the key features of SET? (Understand)

    (i) Confidentiality of Information

    (ii) Integrity of data

    (iii) Card holder account authentication

    (iv) Merchant authentication

33. What is Web Security? (Remember)

       The types of security threats faced in web can be grouped into passive and active attacks. Passive attack is eaves dropping on the network traffic .Active attack is impersonating user, altering messages and altering the information on the website.

34. Specify the purpose of ID Payload in Phase I and. Phase II inherent in ISAKMP/ IKE Encoding. (NOV/DEC 2017) (Understand)

 ISAKMP defines payloads for exchanging key generation and authentication data. IDx is the identification payload for "x". x can be: "ii" or "ir" for the ISAKMP initiator and responder respectively during phase one negotiation; or "ui" or "ur" for the user initiator and responder respectively during phase two

35. Justify the following statement, (Analyze)

"With a Network Address Translation (NAT) box, the computers on your internal network do not need global IPV4 addresses in order to connect to the Internet".(NOV/DEC 2017)

Yes. Network Address Translation (NAT) boxes, the computers on your internal network do not need global IPV4 addresses in order to connect to the Internet

36. Define virus. Specify the types of viruses? (Understand)

       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

37. What is an application level gateway? (Understand)

       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.

38. List the design goals of firewalls? (OR) What is the main function of a firewall? (APRIL/MAY 18) (APRIL/MAY 17) (APR/MAY 2019) (Remember)

       1. All traffic from inside to outside, and vice versa, must pass through the firewall.

       2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.

       3. The firewall itself is immune to penetration.

39. What are the effects of malicious software? Write any two. (NOV/DEC 2013) (Remember)

Malicious software (malware) is any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, trojan, adware, spyware, root kit, etc. It provides a new perspective on the *impact of malicious* agents on the enterprise *software* industry

40. What is worm? (NOV/DEC 2013)/ (APR/MAY 2015) (Remember)

A *worm* is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. *Worms* use parts of an operating system that are automatic and usually invisible to the user.

41. Differentiate spyware and virus. (MAY/JUNE 2014) (Remember)

Spyware and Virus are most common among them. They are both forms of unwanted or malicious software, sometimes called "malware". Spyware collects information about you without appropriate notice and consent. A computer virus spreads software, usually malicious in nature, from computer to computer.

42. What are Zombies? (MAY/JUNE 2014)(NOV/DEC 2016) (Remember)

A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction.

43. What is logic bomb? (MAY/JUNE 2013) (Remember)

A *logic bomb* is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

44. List down the four phases of virus. (Understand)

During it lifetime, a virus goes through four phases:

1) Dormant Phase
Here, the virus remains idle and gets activated based on a certain action or event(for example, a user pressing a key or on a certain date and time etc)

2) Propagation Phase
The virus starts propagating, that is multiplying itself. A piece of code copies itself and each copy starts copying more copies of self, thus propagating.

3) Triggering Phase
A Dormant virus moves into this phase when it gets activated, that is, the event it was waiting for gets initialized.

4) Execution Phase
This is the actual work of the virus. It can be destructive (deleting files on disk) or harmless (popping messages on screen).

45. What is an intruder? (NOV/DEC 2012) (Remember)

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

46. Give few examples of worm. (NOV/DEC 2012)/ (APR/MAY 2015) (Remember)

➢ Badtrans
➢ Blaster,
➢ CodeRed, Dabber, etc

47. What is the advantage of Intrusion Detection System over Firewalls? (APR/MAY 2015) (Understand)

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security.

48. Differentiate macro virus and boot virus. (NOV/DEC 2014)(Analyze)

Boot-sector viruses infect computer systems by copying code either to the boot sector on a floppy disk or the partition table on a hard disk. During startup, the virus is loaded into memory. Once in memory, the virus will infect any non-infected disks accessed by the system.

A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless.

49. What is a Threat? List their types. (APRIL/MAY 18) (Remember)

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

- ➢ Image Spam
- ➢ Phishing
- ➢ Email Spoofing
- ➢ Email-Borne Viruses

50. State the difference between threats and attacks. (APRIL/MAY 17) (Analyze)

A threat is a possible danger that might exploit vulnerability.

Attack is defined as an action that compromises the security of information owned by an organization

51. List various types of firewall. (Remember) (NOV/DEC 2018)

- Packet-filtering firewalls
- Circuit-level gateways
- proxy firewalls

52. Discriminate statistical anomaly detection & rule based detection. (Remember) (NOV/DEC 2018)

- Statistical anomaly detection involves the collection of data relating to the behavior of legitimate users over a period of time.
- With application of rule-based anomaly detection, historical audit records are analyzed to detect usage patterns and to create the rules that describe those patterns.

53. In SSL and TLS, why is there a separate change_cipher_spec protocol rather than including a change_cipher_spec message in the Handshake Protocol? (Analyze) [NOV/DEC 19]

- SSL uses *messages* which are encoded over *records*. Encryption is done on a per record basis. However, several messages of the same type (e.g. handshake messages) can be crammed together in the same record. Since the Change Cipher Spec message modifies encryption settings, a new record should begin immediately afterwards, so that the new settings are immediately applied (in particular, it is crucial for security that the Finished message uses the new encryption and MAC).

- Using a specific record type for Change Cipher Spec is a way to enforce this property. An SSL/TLS implementation cannot help but begin a new record for the finished message, since it uses a record type distinct from that of the Change Cipher Spec message. Such a specific record type *could* be avoided if all SSL/TLS implementations were disciplined enough to begin a new record where they need, and also to verify that the peer *also* began a new record. It is safer and more robust to make it unavoidable through the record type.

PART - B

1. Write short notes on Viruses & Firewalls. Counter measures of virus. **(NOV/DEC 2013)/ (NOV/DEC 2012) (NOV/DEC 2018) (Remember)**

2. Explain statistical anomaly detection and rule based intrusion detection system. **(MAY/JUNE 2014) (APR/MAY 2017) (Understand)**

3. Describe any two advanced anti-virus techniques in detail. **(MAY/JUNE 2014)/ (NOV/DEC 2014)(Evaluate)**

4. Write about virus and related threats in detail. **(MAY/JUNE 2013) (Remember)**

5. Explain in briefly about trusted system. **(MAY/JUNE 2013) (Understand)**

6. Write notes on classifications of viruses and Worm counter measures. **(APR/MAY 2015)/ (NOV/DEC 2014) (Remember)**

7. Explain the characteristics and types of firewalls. **(APR/MAY 2015)(NOV/DEC 2016) (APR/MAY 2019) (Remember).**

8. Discuss how firewa1ls help in the establishing a security framework for an organization. (**NOV/DEC 2017) (Analyze)**

9. Explain how secure electronic transaction (SET) protocol enables e-transactions in details. Explain the components involved. (**NOV/DEC 2017) (understand)**

10. What is Kerberos? Explain how it provides authenticated service**. (APR/MAY 2019) (Understand)**

11. Explain the format of the X.509 certificate. **(APR/MAY 2019) (Understand)**

12. Illustrate the working principle of SET. Relate SET for E-commerce applications. (**NOV/DEC 2018) (understand)**

13. Explain the operational description of PGP. (Apr/May 2011)(Nov/Dec 2011)(May 2014) **(NOV/DEC 2016) (APRIL/MAY 18) (Understand)**

14. Write Short notes on S/MIME (Apr/may 2013) **(NOV/DEC 2018) (Remember)**

15. Explain the Architecture of IP security. **(Nov/Dec 2010)(Apr/May 2011) (APR/MAY 2017) (APR/MAY 2019**) **(Remember)**

16. Write short notes on authentication header and ESP **(Apr/May 2010) (APR/MAY 2017)) (Remember)**

17. Explain in detail the operation of Secure Socket Layer (SSL/TLS) in detail. **(Nov/Dec 2011) (May 2015) (Nov/Dec 2018) (Understand)**

18. Explain Secure Electronic transaction with neat diagram. (OR) Write Short notes on the Secure Electronic Transaction **(Nov/Dec 2011) (Nov/Dec 2010) (NOV/DEC 2016) (APRIL/MAY 18) (Understand)**

19. Discuss about **X.509** authentication service in detail **(Apr/May 2013) (Understand)**

20. Explain about the Security standards. **(NOV/DEC 2013) (Understand)**

22. Illustrate how **PGP** encryption is implemented through a suitable diagram. **(Understand) (APRIL/MAY 18) (APR/MAY 2019)**

23. Discuss about the components involved in e-transactions using Secure Electronic Transaction protocol. Specify how it ensures the security during transactions. **(Understand) [NOV/DEC 19]**

24. Explain in detail about the types of Firewalls and mention the design criteria of a firewall to protect the host machines in an educational institution. **(Understand) [NOV/DEC 19]**

25. Using the PGP cryptographic functions, explain the security offered for e-mails in detail **(Remember) [NOV/DEC 19]**

26. Discuss in detail about IP Security architecture and the services offered by IPSec. **(Remember) [NOV/DEC 19]**

PART - C

1. Write the steps involved in the simplified form of the SSL/ILS protocol. **(NOV/DEC 2017) (Understand)**

2. Write the methodology involved in computing the keys in SSI/ILS protocol. **(NOV/DEC 2017) (Understand)**

3. Discuss the different types of virus in detail.Suggest scenario for deploying these in network scenario. **(APR/MAY 2017) (Analyze)**

4. How does screened host architecture for firewalls differ from screened subnet firewall architecture? Which offers more security for information assets on trusted network?Explain with neat sketch. **(APRIL/MAY 18) (Understand)**

5. Evaluate the performance of PGP. Compare it with S/MIME. **(NOV/DEC 2018) (Understand)**

ASSIGNMENT - 5

1. Elaborate the key rings and its significance in PGP**.** Compose the message generation from sender to receiver and explain with suitable diagram. **(Understand)**

2. Explain Secure Electronic transaction with neat diagram**. (Understand)**

3. Describe S/MIME. **(Remember)**

4. Explain the characteristics and types of firewalls **(Understand)**