CB3491- Cryptography and Cyber Security

Question Bank

Unit- I Introduction to security

PART-A

1. What is cryptography?
   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?
   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/Dec2017)
   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?
   1. Access control
   2. Data confidentiality
   3. Data Integrity
   4. Non Repudiation
   5. Authentication

5. How does simple columnar transposition work?
   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?
   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?
   Cipher text
   Only Known Plaintext
   Chosen Plaintext
   Chosen Cipher text
   Chosen Text

8. What is meant by Brute force attack?

   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?

   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?

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

11. What is meant by transposition technique?

    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?

    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 mono alphabetic and polyalphabetic cipher?

    In mono alphabetic 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?

    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. Define integrity and Non - repudiation?

    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.

17. Define the following terms.

    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

18. Define the two basic building blocks of encryption techniques.

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

19. Define Diffusion and confusion.

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.

20.Compare passive and active attack.(NOV/DEC2016)(APR/MAY2019)(NOV/DEC020) (NOV/DEC 2022)

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.

21. Why is asymmetric cryptography bad for huge data? Specify the reason. (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 (percore).

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

Threat: object, person, or other entity representing a constant danger to an asset Attack: a deliberate act that exploits a vulnerability

23. Calculate the cipher text for the following using one time padcipher.

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 + Keywordmod26: 18 2 21 2

Ciphertext: S C V C

24. What is Modern cryptography?

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.

25. What is Cryptanalysis?

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 crypto graphic algorithms.

26. Define Perfect Security

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=Ek(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.

27. What are the components of Cryptosystem?
    - Plaintext
    - Encryption Algorithm
    - Ciphertext
    - Decryption Algorithm
    - Encryption Key
    - Decryption Key

28. Define Product Cryptosystem.

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 plaintext.

c1 = (k11P1 + k12P2 + k13P3) mod 26
c2 = (k21P1 + k22P2 + k23P3) mod 26
c3 = (k31P1 + k32P2 + k33P3) mod 26

This can be expressed in term of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

or

C = KP mod 26

2. Using Playfair cipher algorithm encrypt the message using the key "MONARCHY " and explain?

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	O	S	T
U	V	W	X	Z

3. What is Steganography? Describe the various techniques used in steganography. (APR/MAY 2019)
    - Character marking
    - Invisible ink
    - Pin punctures
    - Typewriter correction ribbon

4. What is monoalphabetic cipher/Examine how it differs from Cesar cipher. (APR/MAY 2019)

(NOV/DEC 2020)

Caesar Cipher

Let us assign a numerical equivalent to each letter:

a	B	C	d	e	f	g		h	i	j	K	L	m
0	1	2	3	4	5	6		7	8	9	10	11	12

n	O	P	q	r	s	t	u	v	w	X	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$C = E(k, p) = (p + k) \bmod 26$$
$$p = D(k, C) = (C\ k) \bmod 26$$

5. Explain the substitution encryption techniques in detail? (NOV/DEC 2021)
   a.Caesar Cipher
   b.Playfair Cipher
   c.Hill Cipher
   d.Polyalphabetic Ciphers

6. Explain the OSI security architecture with an example? (NOV/DEC 2016) (APR/MAY 2019))[NOV/DEC 2020] (NOV/DEC 2022)

- Security attack
  - PASSIVE ATTACKS
  - ACTIVE ATTACKS
- Security mechanism
  - AUTHENTICATION
  - ACCESS CONTROL
  - DATA CONFIDENTIALITY
  - DATA INTEGRITY
- Security service
  - Encipherment
  - Digital Signature
  - Access Control
  - Data Integrity

Unit –II SYMMETRIC CIPHERS

PART A

1. What are the principle elements of a public key cryptosystem? (APR/MAY2019)

The principle elements of a cryptosystem are:

1. Plain text
2. Encryption algorithm
3. Public and private key
4. Ciphertext
5. Decryption algorithm

2. 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

3. Specify the applications of the public key cryptosystem? (APR/MAY2019)

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.

4. What requirements must a public key cryptosystem to fulfill to a secured algorithm?

The requirements of public-key cryptosystem are as follows:

1. It is computationally easy for a party B to generate a pair (Public key KUb, Private keyKRb)
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=EKUb(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 privatekey, KRb.
5. It is computationally infeasible for an opponent, knowing the public key, KUb, and a ciphertext,C, to recover the originalmessage,M.
6. The encryption and decryption functions can be applied in either order:M=EKUb[DKRb(M)]=DKUb[EKRb(M)]

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

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.

6. List the uses of RC4. (NOV/DEC 2013)(NOV/DEC 2021-read detail 13 mark)

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

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

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

8. What are the disadvantages of double DES? (NOV/DEC2012)

- Meet-in-the-middle attack is possible in triple DES.
- Need more memory space for encryption and decryption.

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

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

10. 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.

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

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.

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

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).

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

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.

14. Give the five modes of operations in block cipher.(Apr/May 2017)(NOV/DEC2020)(NOV/DEC 2022)

i) Electronic Codebook(ECB) Mode

ii) CBC (Cipher-Block Chaining) Mode
iii) CFB (CipherFeedback)Mode
iv) OFB (Output Feedback)Mode,
v) CTR (Counter) Mode

15. Why is trap door one way function used? (NOV/DEC18)

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.

16. Why the middle portion of triple DES is a decryption rather than encryption?

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.

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

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.

18. When is encryption scheme unconditionally and computationally secure?

An encryption scheme is unconditionally secure if the cipher text generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text 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.

19. If a bit error occurs in the transmission of a cipher text character in 8-bit CFB mode, how far does the error propagate?

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

20. Why a large quantity of random keys is undesirable?

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.

21. What are the requirements needed for secure use of Conventional Encryption.

(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.

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

The parameters of AES includes

· Keysize(words/bytes/bits)

· Plaintext Blocksize(words/bytes/bits)

· Number of rounds
· Round key size(words/bytes/bits)
· Expanded key size(words/bytes)

23. Difference between linear and differential cryptanalysis? (APR/MAY2012)(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

24. Briefly define a Group, a Ring and a Field. [NOV/DEC 19][NOV/DEC 2020]

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.

25. List the entities that are to be kept secret in conventional encryption techniques (NOV/DEC19)

- 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)[NOV/DEC 2020]

C=E(K1,D(K2,E(K1,P)))
P=D(K1,E(K2,D(K1,C)))

2. Describe the working principles of simple DES with an example.(MAY/JUNE 2014)/ (APR/MAY 2015) (NOV/DEC 2021)

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

3. Discuss in detail the encryption and decryption process of AES. (NOV/DEC 2016)

The parameters of AES includes
Keysize(words/bytes/bits)
Plaintext Blocksize(words/bytes/bits)
· Number of rounds

· Round key size(words/bytes/bits)
Expanded key size(words/bytes)

4. Give the five modes of operations in block cipher. (Apr/May 2017)(NOV/DEC2020)(NOV/DEC 2022)
   i) Electronic Codebook(ECB) Mode
   ii) CBC (Cipher-Block Chaining) Mode
   iii) CFB (CipherFeedback)Mode
   iv) OFB (Output Feedback)Mode,
   v) CTR (Counter) Mode

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)

   a) DES is an implementation of a Feistel Cipher.
   b) It uses 16 round Feistel structure.
   c) The block size is 64-bit. Though, key length is 64-bit,
   d) DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bitsonly).

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)[NOV/DEC 2020]

AES Parameters

- Block Size is 128
- No. of Rounds is 10
- Key Size is 128 bits (4 Words/16 Bytes)
- No. of Sub keys is 44 (128 bit)
- Each subkey Size is 32 bits/ 1 word/ 4 bytes
- Each Round there is 4 subkeys, total 40 subkeys
- Pre round calculation, 4 Subkeys were used
- Cipher Text is 128 bits

7. Describe DES algorithm and explain with neat diagram and explain the steps.(APR/MAY 2017)(NOV/DEC 2022)

$$f_K(L,R) = (L \oplus F(R,SK),R)$$

UNIT III – ASYMMETRIC CRYPTOGRAPHY

PART – A.

1. Write the difference between public key and private key crypto systems? (APR/MAY 2012&APR/MAY2017)(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.

2. State whether symmetric and asymmetric cryptographic algorithms need key exchange? (APR/MAY2014)(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.

3. List the Authentication requirements? (APR/MAY 2014) (NOV/DEC2016)

The authentication is provided for the following attacks

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

4.Point out the types of cryptanalytic attacks?(**NOV/DEC 2014)**

The two types of cryptanalytic attacks includes the

- Attacks on hash functions
- Attacks on message authentication codes

5. What is Man in the Middle attack?

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.

6. What is the Fermat's theorem? (Nov/Dec 2017)? (NOV/DEC 2022)

Fermat"s theorem states the following: If *p* is prime and *a* is a positive integer not divisible by *p*, then

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

7. What is the use of Fermat's theorem?(NOV/DEC 2021)

- 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, orby 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.
-

8. Describe Chinese remainder theorem.

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.

9. Define Euler's theorem and it's application? (APRIL/MAY 18)

Euler's theorem states that for every **a** and **n** that is relatively prime:

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

10. Define Euler's totient function or phi function and their applications?

The Eulers totient function states that, it should be clear for a prime number p,

$\Phi(p) = p-1$

11. Describe in general terms an efficient procedure for picking a prime number?

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 step1.
4. If n has passed a sufficient number of tests, accept n; otherwise, go to step2.

12. Define Fermat Theorem? (Apr/May 17)

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

13. What is discreteLogarithm?

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.

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

Y_A	$=\alpha^{X_A}$ **modq**	= 25mod 11	=3
Y_B	$= \alpha^{X} K_B$ **modq**	= 125mod 11	=4
	$= (Y_A)^{X} K_B$ **modq**	= 27mod 11	=5
	$= (Y_B)^{X_A}$ **modq**	= 16mod 11	=5

15. Perform encryption and decryption using RSA Alg. for the following. (**NOV/DEC 2017**) **P=7; q=11;e=17;M=8. (APRIL/MAY18)**

Soln:

n = pq

n = 7*11=77

Φ(n) =(p-1)(q-1)

=6*10 =60

e =17 , d =27

$C = M^e \bmod n$

C = 817 mod 77

= 57

$M = C^d \bmod n$

= 5727 mod 77

= 8

16. What is an elliptic curve? (NOV/DEC 2016) (NOV/DEC 2022)

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.

17. Define Euler's phi function.

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

a. If n is a prime number, thenϕ(n)=n-1.
b. If n is a composite number, then
   i. Find the prime factors of that number and compute the phi function value as used in Step1.

otherwise,

   ii. 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})

18. Mention any three Primality Testing Methods.

1. Naïve Algorithm
2. Fermat's Primality Test
3. Miller-Rabin Primality Test

19. Write the formula for Encryption and Decryption in RSA (NOV/DEC 2021).

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

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

20. Consider the RSA encryption method with p=11 and q=17 as the two primes.Find n and ϕ(n). (Evaluate) [NOV/DEC19](NOV/DEC 2020)

$n = p \times q = 17 \times 11 = 187$

$\phi(n) = (p-1)(q-1) = (17-1)(11-1)$

$= 16\ (10)$

$= 160.$

21. What are the functions used to produce an authenticator? (NOV/DEC 2022)

Conventional encryption can serve as Authenticator. Conventional encryption provides authentication aswell as confidentiality .Requires recognizable plaintext or other structure to distinguish between well- formed legitimate plaintext and meaningless random bits.

PART – B

1. Write short notes on Fermat's theorem, Euler's theorem and Chinese remainder theorem? **(NOV/DEC 2016) [NOV/DEC 2020]**

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

$(n) = (n- 1)$ and Fermat's theorem holds. However, it also holds for any integer n. (n) is the number of positive integers less than n that are relatively prime to n.

Consider the set of such integers, labeled as $R = \{x_1, x_2, \ldots\ldots, \Phi(n)\}$

$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots , (ax_{\phi(n)} \bmod n)\}$ $Zm1^{\times} Zm2^{\times} \ldots .^{\times} Zmk.$

That is, for every integer A such that $0 \leq A \leq M$, there is a unique k-tuple$(a1, a2, \ldots., ak)$ with $0 \leq ai < mi$ that represents it, and for every such k-tuple $(a1, a2, \ldots.. ak)$,

2. State Chinese Remainder theorem and find X for the given set of congruent equationsUsing CRT. **(NOV/DEC2016)[NOV/DEC 2020]**

X=2(mod3)

X=3(mod5)

X=2(mod7)

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

Theorem: Euclidean algorithm

Either m is a multiple of n, or there is a positive integer k, and integers $q_1, q_2, \ldots\ldots, q_k, r_1, r_2, \ldots\ldots r_{k-1}$ (and $r = 0$) such that

$m = q_1 n + r_1 \quad (0 \le r_1 < |n|)$

$n = q_2 r_1 + r_2 \quad (0 \le r_2 < r_1)$

……

$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \quad (0 \le r_{k-1} < r_{k-2})$

$r_{k-2} = q_k r_{k-1} \quad (0 \le r_k < r_{k-1})$

4.

4.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)**

5. 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)**

$C = M^e \bmod R \quad 0 <= d <= R$

Decryption of a ciphertext C to recover the message M is:

- $M = C^d = M^{e.d} = M^{1+n.[[phi]](R)} = M \bmod R$

UNIT IV – INTEGRITY AND AUTHENTICATION ALGORITHMS

PART - A

1. **What are the functions used to produce an authenticator? (APR/MAY 2019) (NOV/DEC2009)(NOV/DEC 2021)**

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? (NOV/DEC 2020)

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)

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)

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)

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 $y \neq x$ withH(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)

The two approaches of digital signature includes,

- Direct Digital Signature
- Arbitrated Digital signature

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

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 $y \neq x$ with H(y) =H(x).

9. List any three hash algorithm.

1. MD5 (Message Digest version 5)algorithm.
2. SHA_1 (Secure Hash Algorithm).
3. RIPEMD_160algorithm.

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

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?

- The signature must be bit pattern that depends on the message being signed.
- The signature must use some information unique to theϖ 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?

- 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/DEC2017)

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)

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) MACs can be created from unkeyed hashes (e.g. with the HMAC construction), or createddirectly 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. (NOV/DEC2018)

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. (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 versionSHA-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)(NOV/DEC 2020)

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.

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?

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?

- Secure
- Reliable
- Transparent
- Scalable

22. 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 itsdatabase.
- 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 Kerberosprocedure.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?

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?

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)

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/DEC2017)(NOV/DEC 2021)(NOV/DEC 2022)

Applications

- WWW,
- Electronic mail,
- User authentication,
- IPsec.

28. List the 3 classes of intruder? (NOV/DEC 2016) (APR/MAY2019)

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.

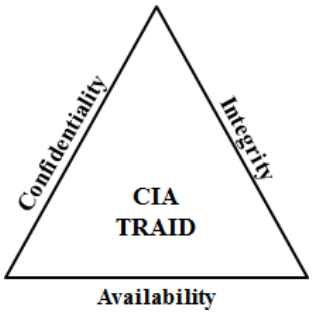


Fig. CIA Traid

30. State the requirements of a digital signature. [NOV/DEC19]

1. **Message Encryption:** The ciphertext of the entire message serves as itsauthenticator.
2. **Message Authentication Code (MAC):** A public function of the message and asecret key that produces a fixed length value that serves as theauthenticator.
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? [NOV/DEC19]

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.

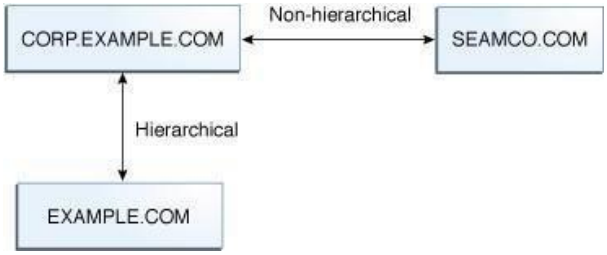


Fig. Kerberos Realm

32. What entities constitute a full service in Kerberos environment? [NOV/DEC19]

A full service environment consists of a

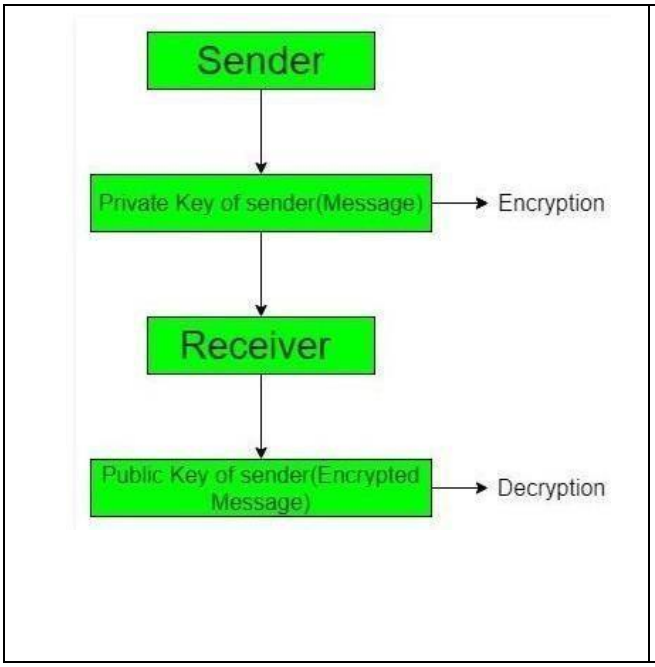
i) Kerberos server,
ii) Number of clients ,and
iii) Number of application servers.

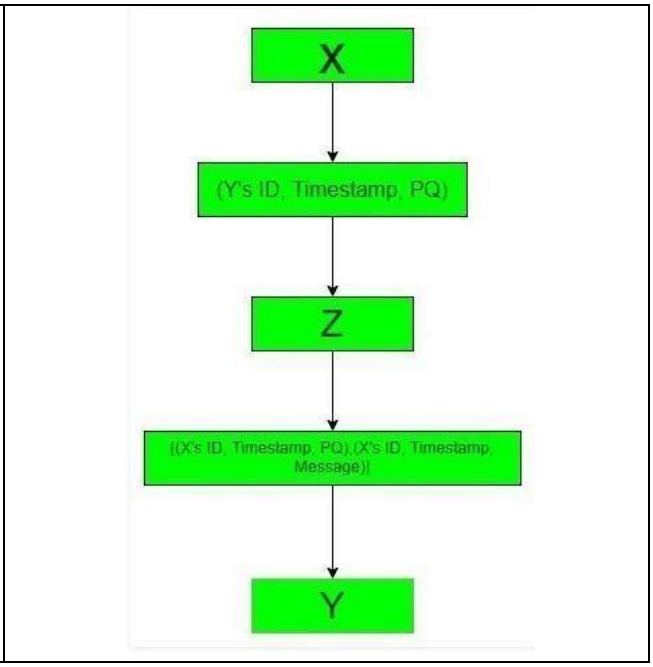
33. Differentiate transport and tunnel mode in IP Sec.[NOV/DEC22]

Transport Mode:
Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet.
Tunnel Mode:
Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header.

34. Compare Direct and Arbitrated digital signature. [NOV/DEC19]

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

i) public key signature schemes

ii) the private-key signs (creates) signatures, and the public-key verifies signatures

iii) only the owner (of the private-key) can create the digital signature, hence it can be used toverify who created a message

iv) anyone knowing the public key can verify the signature

v) usually don't sign the whole message but justa **hash** of the message

vi) digital signatures can provide non-repudiation of message origin, since an asymmetric algorithm is used in their creation, provided suitable timestamps and redundancies are incorporated in the signature

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

I. A and B share a symmetric (secret) key K, which is not known to anyone else. A calculates theMAC by applying key K to the message M.

2. A then sends the original message M and the MAC Hl to B.

3. When B receives the message, B also uses K to calculate its own MAC H2 over M.

4. B now compares HI with H2. If the two match, B concludes that the message M has not been changed during transit. However, if HI ≠ H2, B rejects the message, realizing that the message was changed duringtransit.

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

4.Illustrate about SHA algorithm and explain? **(NOV/DEC 2011) (APR/MAY2013)**
NOV/DEC 2013) **(**NOV/DEC 2017)

- pad message so its length is a multiple of 512 bits
- initialise the 5-word (160-bit) buffer (A,B,C,D,E) to
- process the message in 16-word (512-bit) chunks, using 4 rounds of 20 bit operationseach on the chunk & buffer
- output hash value is the final buffer value

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

$$\Pr[\mathrm{MAC}(K, M) = \mathrm{MAC}(K, M')] = 2^{-n}$$

another message and fool the receiver. Thus the user has to try about 2^{63}combination

6. Describe about hash functions? **(NOV/DEC 2012)** (**NOV/DEC 2013)**
One-way: For any given code h, it is computationally infeasible to find x such that

H(x) = h.

Weak collision resistance: For any given block x, it is computationally infeasible to findy x with H(y) = H(x).

Strong collision resistance: It is computationally infeasible to find any pair (x, y) Such that H(x) = H(y).

For a hash code of length n, the level of effort required, as we have seen is proportionalto the following:

One way	2^n
Weak collision resistance	2^n
Strong collision resistance	$2^{n/2}$

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

a) **Padding**
b) **Append Length**
c) **Divide the input into 512-bit blocks**
d) **Initialize chaining variables**

- EIgamaI Digital Signature Scheme.
- Schnorr Digital Signature Scheme.

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

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

10. Illustrate SHA512 in detail. **(NOV/DEC2018)(NOV/DEC 2021)**

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

12. 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)**

13. i) ComparetheusesofMACandHashfunction.Representthemusingappropriatediagrams. **[NOV/DEC 19]**

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

14. List the design objectives of HMAC and explain the algorithm in detail **[NOV/DEC19]**

UNIT V – CUBER CRIME AND CYBER 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]**

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

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

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.

3. What are the function areas of IP security?

- Authentication
- Confidentiality
- Key management

4. Give the application of IP security?

- Provide secure communication across private & public LAN.
- Secure remote access over the Internet.
- Secure communication to other organization.

5. Give the benefits of IP security? (APRIL/MAY 17) (APR/MAY2019)(NOV/DEC2020)

- 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 toend-user.
- IP security can provide security for individualuser.

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

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

7. Specify the IP security services?

i) Access control.

ii) Connectionless integrity.

iii) Data origin authentication

iv) Rejection of replayed packet.

v) Confidentiality.

vi) Limited traffic for Confidentiality.

8. What do you mean by Security Association? Specify the parameter 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 3parameters:
  - Security Parameter Index(SPI).
  - IP Destination Address.
  - Security Protocol Identifier.

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

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

10. Differentiate Transport and Tunnel mode in IPsec?(May2015) (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.

11. What is Authentication Header? Give the format of the IPsec Authentication Header?

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)		

12. List the steps involved in SSL record protocol?(Understand)(NOV/DEC 2020)

- SSL record protocol takes application data as input and fragments it.
- Apply lossless Compression algorithm.
- Compute MAC for compressed data.
- MAC and compression message is encrypted using conventional algorithm.

13. What are the different between SSL version 3 and TLS? (APRIL/MAY 18) (Analyze)

SSLTLS

- In SSL the minor version is 0 and * In TLS, the major version is 3 and the major version is 3 minor version is1.
- 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. defined in SSL3with the exception of no _certificate.

14. 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:

i) Confidentiality of information

ii) Integrity of data
iii) Cardholder account authentication
iv) Merchant authentication

15. What are the steps involved in SET Transaction?

- 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.

16. What is dual signature? What it is purpose?

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.

17. Expand and define SPI .(APR/MAY 2013)

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.

18. What are the key features of SET?

(i) Confidentiality of Information

(ii) Integrity of data

(iii) Card holder account authentication

(iv) Merchant authentication

19. What is Web Security?

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.

20. Define virus. Specify the types of viruses?

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

21. What is an 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.

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

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

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

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

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

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.

25. Differentiate spyware and virus. (MAY/JUNE 2014)

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.

26. What are Zombies? (MAY/JUNE 2014)(NOV/DEC 2016))(NOV/DEC 2022)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.

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

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.

28. List down the four phases of virus.

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).

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

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.

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

- Bad trans
- Blaster,
- CodeRed, Dabber, etc

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

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 insecurity.

32. Differentiate macro virus and boot virus. (NOV/DEC2014)(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.

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

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

34. 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

35. List various types of firewall. (NOV/DEC2018)

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

36. Discriminate statistical anomaly detection & rule based detection. (NOV/DEC2018)

- 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.

37. 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/DEC19]

- 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 about virus and related threats in detail. **(MAY/JUNE 2013)**

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

2. Explain in briefly about trusted system. **(MAY/JUNE 2013)**
3. Explain the characteristics and types of firewalls. **(APR/MAY 2015)(NOV/DEC 2016)(APR/MAY 2019).**

   Packet filters

   Application-

   level gateways C

   Circuit-level gateways

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

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

6. Explain the format of the X.509 certificate. **(APR/MAY 2019)**
   - algorithm identifier (used to sign certificate)
   - issuer (CA)
   - period of validity (from - to dates)
   - subject (name of owner)
   - public-key (algorithm, parameters, key)

- signature (of hash of all fields in certificate)
- any user with access to CA can get any certificate from it
- only the CA can modify a certificate