CS6701 – Cryptography and Network Security

UNIT 1 – 2 MARKS

1. Define cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

2. Define cryptanalysis.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code."

3. Define security Attack, mechanism and service

• **Security attack:** Any action that compromises the security of information owned by an organization.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

4. Distinguish Threat and Attack

Threat -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.

Attack -An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

5. Differentiate active attacks and passive attacks.

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are the release of message contents and traffic analysis.

An active attack attempts to alter system resources or affect their operation. It can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

6. Specify the components of encryption algorithm

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

7. Describe security mechanism.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

8. Differentiate block and stream cipher

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

9. **What are the essential ingredients of a symmetric cipher?**

• **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

• **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

• **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.

• **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

10. Specify four categories of security threats

- Interruption
- Interception
- Modification
- Fabrication

11. What is brute-force attack?

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

12. List the types of cryptanalysis attack

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

13. Compare Substitution and Transposition techniques.

➔ **A substitution technique** is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Example: Caesar cipher, monoalphabetic cipher, Playfair cipher,

➔ A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Example: rail fence

14. Define Steganography.

A plaintext message may be hidden . The methods of **steganography** conceal the existence of the message

Example Techniques: character marking, invisible ink, pin punctures, type writer correction ribbon

15. Quote Euler's theorem.

Euler's theorem states that for every and that are relatively prime:

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$$

16. Quote Fermat's theorem.

If ***p*** is prime and **a** is a positive integer not divisible by ***p*** , then

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

17. Write algorithm for testing for primality

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

18. Define primitive root.

it is said that the base integer ***a*** generates (via powers) the set of nonzero integers modulo 19. Each such integer is called a primitive root of the modulus 19.More generally, we can say that the highest possible exponent to which a number can belong (mod n) is pie(n). If a number is of this order, it is referred to as a **primitive root** of n.

19. Find GCD(24140,16762)

20. Fine GCD(4655,12075)

21. Using the extended Euclidean algorithm, find the multiplicative inverse of

a) **1234 mod 4321**
b) **24140 mod 40902**
c) **550 mod 1769**

22. Using Fermat's theorem, find 3^201 mod 11

16 MARKS

1. **State and Describe**

(i) Fermat's theorem. (8)

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

$$a^{p-1} \equiv 1 \pmod{p} \tag{8.2}$$

Proof: Consider the set of positive integers less than p: $\{1, 2, \ldots, p-1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this, assume that $ja \equiv ka \pmod{p}$, where $1 \leq j < k \leq p-1$. Because a is relatively prime[5] to p, we can eliminate a from both sides of the equation [see Equation (4.3)] resulting in $j \equiv k \pmod{p}$. This last equality is impossible, because j and k are both positive integers less than p. Therefore, we know that the $(p-1)$ elements of X are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p-1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$a \times 2a \times \ldots \times (p-1)a \equiv [(1 \times 2 \times \ldots \times (p-1)] \pmod{p}$$
$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

We can cancel the $((p-1)!$ term because it is relatively prime to p [see Equation (4.5)]. This yields Equation (8.2), which completes the proof.

(ii) Euler's theorem. (8)

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

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{8.4}$$

Proof: Equation (8.4) is true if n is prime, because in that case, $\phi(n) = (n-1)$ and Fermat's theorem holds. However, it also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as

$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation[6] of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.

2. There are no duplicates in S. Refer to Equation (4.5). If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

which completes the proof. This is the same line of reasoning applied to the proof of Fermat's theorem.

2. (i) Tabulate the substitution Techniques in detail. (12)

Definition , example and disadvantages

- Caesar cipher
- monoalphabetic cipher
- playfair cipher
- hill cipher
- polyalphabetic ciphers –vigenere and vernam cipher
- one time pad

(ii) Describe the Transposition Techniques in detail. (4)

Rail fence

3. (i) List the different types of attacks and explain in detail.(8)

1. A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are

- The release of message contents and
- traffic analysis.

2. **An active attack** attempts to alter system resources or affect their operation. It can be subdivided into four categories:

- masquerade,
- replay,
- modification of messages, and
- denial of service.
-

(ii) Describe in detail about the types of cryptanalytic attack. (8)

- Cipher text only
- Known plain text
- Chosen plaintext

- Chosen cipher text Chosen text

4. (i) Evalute3^21 mod 11 using Fermat's theorem. (6)
(ii) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT. (10)
X=2(mod 3)
X=3(mod 5)
X=2(mod 7)

5. (ii) Discuss about the Groups, Rings and Field (8)
6. (i) Solve using playfair cipher. Encrypt the word "Semester Result" with the keyword "Examination". List the rules used. (8)
(ii) Demonstrate the encryption of the message "PAY" using hill cipher with the following key matrix and show the decryption. (8)

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

UNIT 2- 2 MARKS

1. **What is the difference between a block cipher and a stream cipher?**
   A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.
2. **What is the difference between diffusion and confusion?**
   In **diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected by many plaintext digits. **confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key.This is achieved by the use of a complex substitution algorithm.
3. **Whar are the design parameters of a Feistel cipher?**
   - Block size
   - Key size
   - Number of rounds
   - Subkey generation algorithm
   - Round function F
   - Fast software encryption/ Decryption
   - Ease of analysis
4. **Explain the 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. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.
5. **What is the strength of DES?**
   - The use of 56 bit keys
   - The nature of DES algorithm
   - Timing attacks
6. **Define product cipher**
   product cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.
7. **What is substitution and permutation?**
   Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
   Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.
8. **Give 5 modes of operation in block cipher**
   - Electronic Codebook(ECB)
   - Cipher Block Chaining(CBC)

- Cipher Feedback(CFB)
- Output Feedback(OFB)
- Counter(CTR)

9. **State advantages of counter mode.**
   *Hardware Efficiency
   * Software Efficiency
   *Preprocessing
   * Random Access
   * Provable Security
   * Simplicity.
10. **Define Multiple Encryption.**
    It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES. In the first instance, plaintext is converted to ciphertext using the encryption algorithm. This ciphertext is then used as input and the algorithm is applied again. This process may be repeated through any number of stages.
11. **Specify the design criteria of block cipher.**
    - Number of rounds
    - Design of the function F
    - Key scheduling
12. **Define Reversible mapping.**
    Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.
13. **What is Triple Encryption? How many keys are used in triple encryption?**
    Triple Encryption is a technique in which encryption algorithm is performed three times using three keys.
14. **List the schemes for the distribution of public keys.**
    - Public announcement
    - Publicly available directory
    - Public key authority
    - Public-key certificates
15. **Drawback of 3-DES.**
    - Algorithm is sluggish in software
    - The number of rounds in thrice as that of DES
    - 3DES uses 64 bit block size
    - To have higher efficiency and security a larger block size is needed.
16. **List out the attacks to RSA.**
    - **Brute force -** Trying all possible private keys.
    - **Mathematical attacks -** The approaches to factor the product of two prime numbers.
    - **Timing attack -** Depends on the running time of the decryption algorithm.

17. **What is traffic Padding? What is its purpose?**
    Traffic padding produces ciphertext output continuously, even in the absence of the plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible to for an attacker to distinguish between true dataflow and padding and therefore impossible to deduce the amount of traffic.
18. **List the evaluation criteria defined by NIST for AES?**
    The evaluation criteria for AES is as follows:

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

19 Table 9.2 Conventional and Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

20 **What is one way function?**

A **one-way function**3 is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible:

$Y = f(X)$ easy

$X = f^{-1}(Y)$ infeasible

21 **What is a trap-door one-way function?**

a **trap-door one-way function**, which is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.We can summarize as follows: A trapdoor one-way function is a family of invertible functions f_k, such that

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

$X = f_k^{-1}(Y)$ easy, if k and Y are known

$X = f_k^{-1}(Y)$ infeasible, if Y is known but k is not known

22 **Formulate few applications of RC5**

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

Key size(words/bytes/bit)	**4/16/128**	**6/24/192**	**8/32/256**
Plaintext Block size(words/bytes/bit)	**4/16/128**	**4/16/128**	**4/16/128**
Number of rounds	**10**	**12**	**14**
Round key size(words/bytes/bit)	**4/16/128**	**4/16/128**	**4/16/128**
Expanded key size (words/bytes)	**44/176**	**52/208**	**60/240**

15 MARKS

1. **Explain in detail about working of DES encryption and decryption**
   - Definition
   - Encryption- Diagram
   - Initial Permutation
   - Details of Single Round- diagram , S-box
   - decryption
2. **Explain in detail about working of AES**
   Definition
   Structure – diagram and its explanation (10 pt)
   Transformation function
3. **Explain in detail about AES key expansion**
4. **Explain briefly about the block cipher modes of operations**
   Diagram , adv and disadv for each
   - Electronic Codebook(ECB)
   - Cipher Block Chaining(CBC)
   - Cipher Feedback(CFB)
   - Output Feedback(OFB)
   - Counter(CTR)
5. **Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:**
   a. $p = 3; q = 11, e = 7; M = 5$
   b. $p = 5; q = 11, e = 3; M = 9$
   c. $p = 7; q = 11, e = 17; M = 8$
   d. $p = 11; q = 13, e = 11; M = 7$
   e. $p = 17; q = 31, e = 7; M = 2$

5. In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

6. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7.

a. If user A has private key $X_a = 5$, what is A's public key Y_a ?
b. If user B has private key $X_b = 12$, what is B's public key Y_b ?
c. What is the shared secret key?

7. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2

a. Show that 2 is a primitive root of 11.
b. If user A has public key $Y_a = 9$, what is A's private key X_a?
c. If user B has public key $Y_b = 3$, what is the secret key K shared with A?

8. Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7. (16)
(i) If user A has private key XA=3.What is A's public key YA?
(ii)If user B has private key XB=6. What is B's public key YB?
(iii) What is the shared secret key? Also write the algorithm.

9. Explain in detail about RC5 algorithm

10. Brief about Blowfish algorithm

UNIT 3 -2 MARKS

1. **What is a hash in cryptography?**
   A **hash function** H accepts a variable-length block of data M as input and produces a fixed-size hash value h= H(M) called as message digest as output. It is the variation on the message authentication code
2. **What is the role of a compression function in a hash function?**
   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 values of the chaining variable is the hash value usually b>n; hence the term compression
3. **What is cryptography hash function?**
   The kind of hash function needed for security applications is referred to as a **cryptographic hash function**. A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed.
4. **What are the applications of cryptographic hash function?**
   - Message Authentication
   - Digital Signatures
   - pseudorandom function (PRF) or a pseudorandom number generator (PRNG).
5. **What are the requirements for message authentication?**
   - Disclosure
   - Traffic analysis
   - Masquerade
   - Content modification
   - Sequence modification
   - Timing modification
   - Source repudiation
   - Destination repudiation
6. **What is collision resistant attack or birthday paradox?**
   For a collision resistant attack, an adversary wishes to find two messages or data blocks, *x* and , that yield the same hash function:H(x)= H(y). This turns out to require considerably less effort than a preimage or second preimage attack. The effort required is explained by a mathematical result referred to as the **birthday paradox**. In essence, if we choose random variables from a uniform distribution in the range 0 through N-1, then the probability that a repeated element is encountered exceeds 0.5 after root(N) choices have been made. Thus, for an m -bit hash value, if we pick data blocks at random, we can expect to find two data blocks with the same hash value within root(2^m) = $2^{m/2}$ attempts
7. **List the processing logic of SHA-512**
   1. Append padding bits
   2. Append padding length
   3. Initialize hash buffer
   4. Process message in 1024 bits(128-words) blocks
   5. Output
8. **What are the security requirement for cryptography hash function?**

Table 11.1 Requirements for a Cryptographic Hash Function H

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	$H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that $H(y) = h$.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.
Pseudorandomness	Output of H meets standard tests for pseudorandomness.

9.

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Note: All sizes are measured in bits.

10. Mention the various ways of producing authenticator or define the classes of message authentication function

• **Hash function:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator

• **Message encryption:** The ciphertext of the entire message serves as its authenticator

• **Message authentication code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator

11. What do you meant by MAC?

It involves the use of a secret key to generate a small fixed-size block of data, known as a **cryptographic checksum** or MAC, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key .When A has a message to send to B, it calculates the MAC as a function of the message and the key: **MAC = MAC(*K*, *M*)**

where

M = input message

C = MAC function

K = shared secret key

MAC = message authentication code

12. **Differentiate MAC and Hash function?**

MAC: In MAC , the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.

Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

13. **List any three hash algorithm.**
    - MD5(message Digest version 5) algorithm
    - SHA_1 (Secure Hash algorithm)
    - RIPEMD_160 algorithm

14. **What is the difference between weak and strong collisions resistance?**

Weak collisions resistance: for any given block x, it is computationally infeasible to find y * x with H(y) = H(x). it is proportional to 2^n .

Strong collision resistance: it is computationally infeasible to find any pair (x,y) such that H(x)= H(y). it is proportional to $2^{n/2}$

15. **Differentiate internal and external error control**.

Internal error control:

In internal error control, an error detecting code also known as frame check sequence or checksum.

External error control:

In external error control, error detecting codes are appended after encryption.

16. **What is the meet 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.

17. **Compare MD5, SHA1 and RIPEMD-160 algorithm.**

	MD5	SHA-1	RIPEMD160
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
No.of steps	64(4 rounds of 16)	80(4 rounds of 20)	160(5 pairs rounds of 16)
Maximum message size	infinity	2^{64}-1 bits	2^{64}-1 bits
Primitive logical function	4	4	5
Additive constant used	64	4	9
Endianess	Little endian	Big endian	Little endian

18. **Distinguish between direct and arbitrated digital signature?**

Direct digital signature	Arbitrated Digital Signature
1.The direct digital signature involves only the communicating parties. 2.This may be formed by encrypting the entire message with the sender's private key.	1.The arbiter plays a sensitive and crucial role in this digital signature. 2. 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.

19. **What are the properties a digital signature should have?**

- It must verify the author and the data and time of signature.
- It must authenticate the contents at the time of signature.
- It must be verifiable by third parties to resolve disputes.

20. 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 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.

21. What is digital signature?

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

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

The purpose of dual signature is to link two messages that intended for two different recipients. To avoid misplacement of orders.

15 MARKS

1. **Describe Secure hash Algorithm in detail. (16)**
2. **Describe the MD5 message digest algorithm with necessary block diagrams. (16)**
3. **(i)Summarize CMAC algorithm and its usage.(8)**
   (ii)Describe any one method of efficient implementation of HMAC. (8)
4. **Describe digital signature algorithm and show how signing and verification is done using DSS. (16)**
5. **Explain in detail ElGamal Digital Signature scheme with an example. (16)**
6. **Explain in detail about different ways of distribution of public keys**
7. **Consider prime field q=19, it has primitive roots { 2,3,10,13,14,15}, if suppose α=10. Then write key generation by she choose X_A=16. And also sign with hash value m=14 and alice choose secret no K=5. Verify the signature using Elgamal digital Signature Scheme**

UNIT 4- 2 MARKS

1. **Define Kerberos.**
   Kerberos is an authentication service developed as part of project Athena at MIT. The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.
2. **What is Kerberos? What are the uses?**
   Kerberos is an authentication service developed as a part of project Athena at MIT.Kerberos provide a centralized authentication server whose functions is to authenticate servers.
3. **What 4 requirements were defined by Kerberos?**
   - Secure
   - Reliable
   - Transparent
   - Scalable
4. **In the content of Kerberos, what is realm?**
   - A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:
   - The Kerberos server must have user ID and hashed password of all participating users in its database.
   - The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".
5. **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.
6. **List the 3 classes of intruder?**
   Classes of Intruders
   - Masquerader
   - Misfeasor
   - Clandestine user
7. **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:
   - Parasitic virus
   - Memory-resident virus
   - Boot sector virus
   - Stealth virus
   - Polymorphic virus
   - Metamorphic virus
8. **What is application level gateway?**
   An application level gateway also called a proxy server; act as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
9. **List the design goals of firewalls?**
   - 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.

10. **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.
11. **What is dual signature? What it is purpose?**
    The purpose of the dual signature is to link two messages that intended for two different recipients. To avoid misplacement of orders.
12. **What is the need for authentication applications?**
    - Security for E-mail
    - Internet protocol security
    - IP address security.
13. **What do you mean by SET? What are the features of SET?**
    SET is an open encryption and security specification designed to protect credit card transaction on the Internet.
14. **Write any 3 hash algorithm?**
    - MD5 algorithm
    - SHA-I
    - RIPEMD-160 algorithm.
15. **List out the four phases of virus.**
    - Dormant phase
    - Propogation phase
    - Triggering phase
    - Execution phase
16. **What is worm?**
    A worm is a program that can replicate itself and send copies from computer to computer across network connections. it also perform some unwanted function. The network worm programs use network connections to spread from system to systems
17. **What is Bastion host?**
    Bastion host is a system identified by firewall administrator as critical strong point in network security. Serves as platform for application level/ circuit level gateways.
18. **What is trusted software?**
    Trusted software a system that enhances the ability of a system to defend against intruders and malicious programs by implementing trusted system technology.
19. **Four general techniques of firewall.**
    - Security control
    - Direction control

- User control
- Behaviour control

20. **Three types of firewall.**
    - Packet filter
    - Application level gateway
    - Circuit level gateway.
21. **List down the firewall configuration**
    - Screened host firewalls-single homed bastion
    - Screened host firewall system(dual-homed bastion)
    - Screened subnet firewall system
22. **List approaches for intrusion detection.**
    - Statistical anomaly detection
    - Rule based detection
23. **What is intruder?**
    An intruder is an attacker who tries to an unauthorized access to a system.
24. **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:
    a). Confidentiality of information
    b). Integrity of data
    c). Cardholder account authentication
    d). Merchant authentication
25. **What is Zombie?**
    A Zombie is programs that securely takes over another internet-attached computer and then uses that computer to launch attacks are difficult to trace the Zombie's creator.
26. **What is firewall and list its characteristics?**
    It means of protecting a local system (or) network of system from network based security.
    1. Physically blocks all access to local network except via firewall
    2. Only authorized traffic will be allowed to pass
    3. It is immune to penetration
27. **Illustrate** when the certificates are revoke in X.509.
    1. The user's private key is assumed to be compromised.
    2. The user is no longer certified by this CA. Reasons for this include that the subject's name has changed, the certificate is superseded, or the certificate was not issued in conformance with the CA's policies.
    3. The CA's certificate is assumed to be compromised.

15 MARKS

1. What is Kerberos? Explain how it provides authenticated service.
2. Explain the format of the X.509 certificate.
3. Explain the technical details of firewall and describe any three types of firewall with neat diagram.
4. Write short notes on Intrusion Detection.
5. Define virus. Explain in detail.
6. **Explain** Secure Electronic Transaction with neat diagram.
7. What is a trusted system? **Explain** the basic concept of data access control in trusted systems. (8)

UNIT 5 – 2 MARKS

1. **Define key Identifier?**
   PGP assigns a key ID to each public key that is very high probability unique with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.
2. **List the limitations of SMTP/RFC 822?**
   1. SMTP cannot transmit executable files or binary objects.
   2. It cannot transmit text data containing national language characters.
   3. SMTP servers may reject mail message over certain size.
   4. SMTP gateways cause problems while transmitting ASCII and EBCDIC.
   5. SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.
3. **Define S/MIME?**
   Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME
4. **What are the different between SSL version 3 and TLS?**

SSL	TLS
In SSL , the minor version is zero and major version is 3	In TLS, the major version is 3 and the minor version is 1
SSL use HMAC algorithm, except that the padding bytes concatenation	Make use of the same algorithm
SSL supports 12 various alert codes	It supports all of the alert codes defined in SSL3 with the exception of no-certificate.

5. **What are the services provided by PGP services.**
   • Digital signature
   • Message encryption
   • Compression
   • E-mail compatibility
   • Segmentation
6. **Explain the reasons for using PGP?**
   - It is available free worldwide versions that run on a variety of platforms, including DOS/Windows, UNIX, Macintosh and many more
   - It is based on algorithms that have survived extensive public review and are considered extremely secure (eg). RSA,DSS
   - It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication
   - It was not developed by nor and is it controlled by any government or standard organization.
7. **Why E-mail compatibility function in PGP needed?** Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.
8. **Name any cryptographic keys used in PGP?**
   - One time session conventional keys
   - Public keys

- Private keys
- Pass phrase based conventional keys.

9. **List out the features of SET.**
    - Confidentiality
    - Integrity of data
    - Cardholder account authentication
    - Merchant authentication
10. **What is security association?**
    A security association (SA) is the establishment of shared security attributes between two network entities to support secure communication.
11. **What does Internet key management in IPSec?**
    Internet key exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.
12. **List out the IKE hybrid protocol dependence.**
    - ISAKMP - Internet Security Association and Key Management Protocols.
    - Oakley
13. **What does IKE hybrid protocol mean?**
    Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the internet protocol security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.
14. **What are the two security services provided by IPSec?**
    - Authentication Header (AH)
    - Encapsulating Security Payload (ESP).
15. **What are the fields available in AH header?**
    - Next header
    - Payload length
    - Reserved
    - Security parameter
    - Sequence number Integrity check value
16. **What is virtual private network?**
    VPN means virtual private network, a secure tunnel between two devices.
17. **What is ESP?**
    ESP- encapsulating security payload provides authentication, integrity and confidentiality, which protect against data tempering and provide message content protection. IPSec provides standard algorithms, such as SHA and MD5.
18. **What is Behavior-Blocking Software (BBS)?**
    BBS integrates with the OS of a host computer and monitors program behavior in real time for malicious actions.
19. **List password selection strategies.**
    - User education
    - Reactive password checking
    - Computer-generated password.
    - Proactive password checking.

20. **List out the applications of IPsec**
    - Secure branch office connectivity over the Internet
    - Secure remote access over the Internet
    - Establishing extranet and intranet connectivity with partners
    - Enhancing electronic commerce security
21. **Write down the benefits of IPsec**

    • When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

    • IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

    • IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

    • IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

    • IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.
22. **Differentiate Transport mode and Tunnel mode**

Transport mode	**Tunnel mode**
Provide the protection from upper layer between 2 hosts	Provide the protection for entire IP Packet
ESP in this mode encrypts and optionally authenticates IP Payload but not IP headers	ESP in this mode encrypt authenticate the entire IP packet
AH in this mode authenticate the IP payload and select the portion of IP header	AH in this mode authenticate the entire IP packet plus selected portion of outer IP header

23. **List services provided by IPsec?**

    • Access control

    • Connectionless integrity

    • Data origin authentication

    • Rejection of replayed packets (a form of partial sequence integrity)

    • Confidentiality (encryption)

    • Limited traffic flow confidentiality

15 MARKS

1. How IPSec ESP does provide transport and Tunnel Mode operation? Explain with a neat sketch. (16)
2. What is the need for security in IP networks? Describe the IPv6 authentication header.(16)
3. What is PGP? Show the message format of PGP(8)
4. Explain the operational description of PGP(10)
5. Describe about the PKI. (8)
6. Identify the fields in ISAKMP and explain it.(8)
7. Evaluate the different protocols of SSL. Explain Handshake protocol in detail.(16)
8. Describe the phases of Internet key exchange in detail. (16)
9. Explain in detail about S/MIME. (8)