1) State the use of Fermat's Theorem.

→ - It helps to compute powers of integers modulo prime numbers.
- It is a special case of Euler's theorem.
- For any prime no. p and any $1^{+ve}$ integer a that is not divisible by p then
$a^{p-1} \equiv 1 \bmod p$

2) Find 117 mod 13

→ $a \rightarrow 117$

$b \rightarrow 13$

$a \div b = 9$

Remainder = 0

$\therefore$ **117 mod 13 = 0**

3) State Euler's Theorem.

→ For every positive integer 'a' and 'n' which are said to be relatively prime

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

Example → $a = 3, n = 10$

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

$$3^{\phi(10)} \equiv 1 \bmod 10$$

$$\phi(10) = 4$$

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

$$= (2-1)(5-1)$$

$\phi(10) = 4$

$3^4 \equiv 1 \bmod 10$

$81 \equiv 1 \bmod 10$

4) Define Finite Field.

→ - Finite fields play a key role in cryptography
- It can show no. of elements in a finite field must be a power of a prime p.
- It is also known as Galois Fields
- It uses algebric methods based on rounds

5) Define Diffusion.

→ - It is utilized to generate obscure, plain texts
- It is achieved by transposition algorithm
- It is used by Block Cipher only
- It results in increased redundancy
- Statistical relationship between the plaintext and ciphertext is made as complicated as possible.

6) Diff. bet. public key & private key cryptosystems.

| Public Key | Private Key |
|---|---|
| → It is defined as the technique that uses 2 different keys for encryption and decryption | - It is defined as the technique that uses a single shared key to encrypt & decrypt the message |
| - It is asymmetric key encryption | - It is symmetric key encryption |
| - Less efficient | - More efficient |
| - Main purpose is to share the keys securely | - Main purpose is to transmit the bulk data |

7) Is it possible to use the DES algo. to generate MAC? Justify.

→ DES algorithm can be used to compute a Message Authentication Code as it provides the option for data integrity.

8) Application of Public Key Cryptography.

→ ① Digital signatures –

Content is digitally signed with an individual's private key and is verified by the individual's public key

② Encryption –

Content is encrypted using an individual's public key and can only be decrypted with individual's private key.

9) Diff. bet. Conventional & Pub-Key-Enc.

→

| Conventional | Pub Key Enc |
|---|---|
| ① It uses one single key to both encrypt and decrypt the message. | ① It uses a pair of keys to encrypt & decrypt the msg. |
| ② Enc. algorithms are faster. | ② Pub key Enc Algo. are comparitively slower |
| ③ Less Secure | ③ More Secure |
| ④ Sender and receiver shares the same secret key | ④ Only the public key can be shared and the private key remains confidential. |

10) Define Discrete Logarithm.

→ If a, b are non zero integers then, the problem of finding x such that $a^x \equiv b \bmod p$ is called Discrete logarithm where p is any prime number.

11) Message Authentication.

→ A message Authentication or digital signature mechanism can be viewed as having fundamentally two levels. At lower level, function produces an authenticator.

Message encryption → the cipher text of the entire message serves as its authenticator.

12) Define Timing Modification.

→ Timing modification refers to the delay or replay of messages sent between different parties.

13) Define Source & Destination Repudiation.

→ Source Repudiation → Denial of transmission of message by source

Destination Repudiation → Denial of transmission of message by destination.

14) What are the classes of message authentication function?

→ (1) Hash Function → maps a message into fixed length

(2) Message Encryption → The cipher text is served as authenticator

(3) MAC → Function of the message that produces a fixed length value

15) Define Hash function.

→ A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.

16)

| MAC | Hash |
|---|---|
| - Number of inputs is 2 | - Number of input is 1, i.e. single input |
| - Any change in message or key results in a different MAC. | - Any change in message results in diff hash |
| - Example - HMAC CBC-MAC | - Example - SHA1, MD5, SHA2 |

17) One way property in Hash function :

It is also known as message digest, is a mathematical function that takes a variable-length input string and converts it into a fixed length binary sequence that is computationally difficult to invert

18) Define Replay Attack.

-> It is a type of n/w attack in which an attacker captures a valid network transmission and then retransmit it later.

19) Define Digital Signature and its properties.

->

It is a cryptographic o/p used to verify the authenticity of data.

Properties —

1. Authentic
2. Not Reusable
3. Prevents repudiation
4. Unforgeable

20) List out the attacks related to Digital Signature.

→ 3 types of attacks

(1) Chosen-message Attack
(2) Known-message Attack
(3) Key-only Attack

21) Signature Function in DSS.

→ A signature function defines input and output of functions or methods. A signature can include parameters and their types, a return value and type.

22) Define Generic chosen message attack

→ In this, the attacker tricks the genuine user into digitally signing a message that the user doesnot normally intend to sign.