1. **What is confusion and diffusion in cryptography?**

In cryptography**, confusion and diffusion** are two properties of the operation of a secure cipher. Both Confusion and Diffusion are used to stop the deduction of the secret writing key, these properties, when present, work to prevent the application of statistics and other methods of cryptanalysis.

Confusion is a ***cryptographic mechanism*** that is utilized to increase the ***obscurity*** of the ciphertext. In simple words, the technique assures that the ciphertext has no information about the plaintext. The confusion technique keeps the relationship between the ***encrypted text's statistics*** and the ***encryption key's value*** as complex as possible.

Diffusion may be used to define the property that the repetition in the plaintext statistics ***"dissipates"*** in the ciphertext statistics. In diffusion, the output bits must be challengingly dependent on the input bits so that if the plaintext is modified by only one bit, the ciphertext must change in an ***unanticipated*** or ***unreliable*** way.

2. **What do you mean by packet sniffing?**

When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender’s node called *data packets* and reassembled at receiver’s node in original format. Packet sniffing is the action of detecting, reading, and recording packets of data being sent across a network. Network administrators or cyber criminals engage in packet sniffing by using packet sniffers, which are either physical devices or software applications. Packet sniffing is used to capture data such as web browsing histories, usernames and passwords, bandwidth usage, and much more.

3. **What is Reflection Attack?**

A reflection attack is a type of cyber attack in which the attacker sends a large number of requests to a server, each with the victim's IP address as the source address. The server responds to these requests, sending a large number of responses back to the victim. This can cause the victim's network connection to become overloaded, disrupting their access to the Internet or other network resources. Reflection attacks are often used in conjunction with amplification attacks, in which the attacker uses a server with a large response capacity (such as a DNS server) to amplify the effect of the attack.

Example:

DNS reflection attacks –These attacks use the Domain Name System (DNS) to amplify the traffic load on the victim's network connection. The attacker sends a large number of requests to a DNS server, each with the victim's IP address as the source address. The DNS server responds with a large number of responses, which can overwhelm the victim's network connection.

4. **What is euler totient function?**

Euler's totient function is the mathematical multiplicative function that counts the positive integers up to the given integer, generally called 'n,' which is a prime number (co-prime) to 'n.' One may use the function to know the number of prime numbers that exist up to the given integer 'n.'

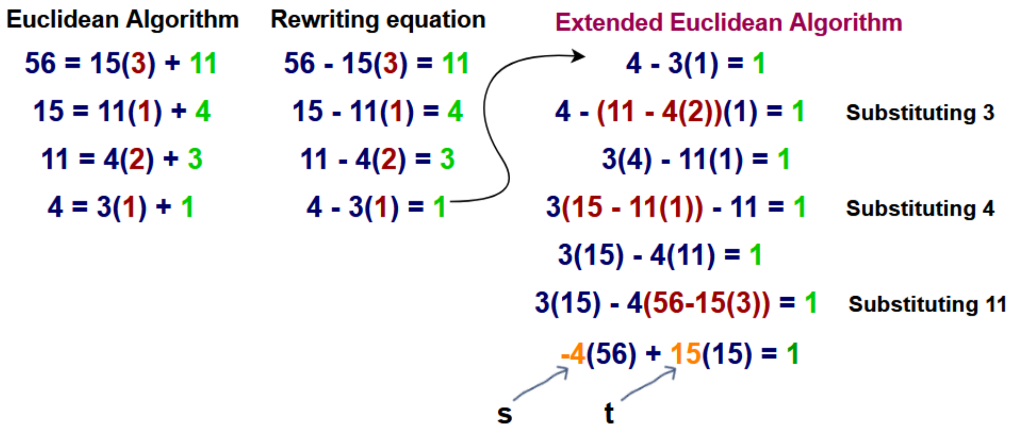
$$\varphi(n) =\mid \{a \in N \mid 0 \leq a < n : gcd(a,n) = 1\} \mid$$

5. **State the Extended Euclidian algorithm? What is its application in cryptography?**

Extended Euclidean Algorithm is an extension of the *Euclidean Algorithm* that computes the greatest common divisor (GCD) of integers a and b. GCD is the largest integer that divides both a and b without any remainder. In addition to computing GCD, Extended Euclidean Algorithm also finds integers s and t such that as+bt=gcd(a,b). Extended Euclidean Algorithm finds s and t by using back substitutions to recursively rewrite the division algorithm equation until we end up with the equation that is a linear combination of our initial numbers. Bézout's Identity guarantees the existence of s and t.

Example:

How to use the Extended Euclidean Algorithm to find the GCD of 56 and 15 to find s and t such that 56s+15t=gcd(56,15)?



Euclidean Algorithm	Rewriting equation	Extended Euclidean Algorithm	
56 = 15(3) + 11	56 - 15(3) = 11	4 - 3(1) = 1	
15 = 11(1) + 4	15 - 11(1) = 4	4 - (11 - 4(2))(1) = 1	Substituting 3
11 = 4(2) + 3	11 - 4(2) = 3	3(4) - 11(1) = 1	
4 = 3(1) + 1	4 - 3(1) = 1	3(15 - 11(1)) - 11 = 1	Substituting 4
		3(15) - 4(11) = 1	
		3(15) - 4(56-15(3)) = 1	Substituting 11
		-4(56) + 15(15) = 1	

The extended Euclidean algorithm is also the main tool for computing multiplicative inverses in simple algebraic field extensions. An important case, widely used in cryptography and coding theory.

6. **Is AES a Feistel cipher? Justify your answer?**

No, AES is not a feistel cipher.

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a

Feistel network. AES is a variant, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. Most AES calculations are done in a particular finite field. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

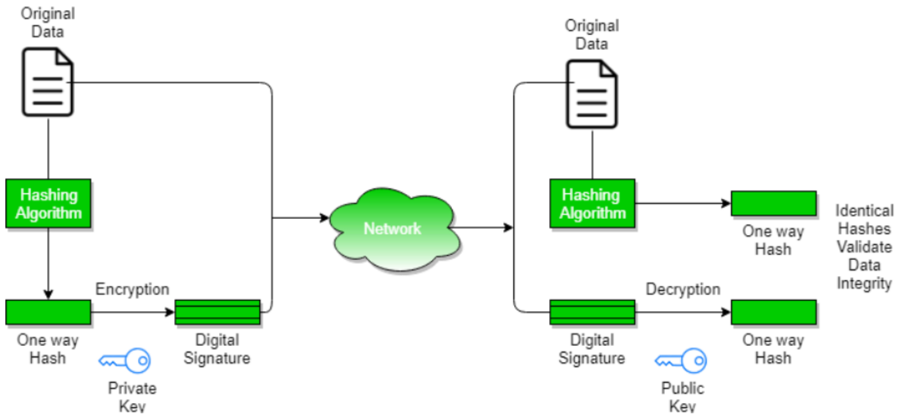
7. Find out the multiplicative inverse of each non-zero element in Z_5 ?

As 5 is prime, every non-zero element of Z/*p* will have an inverse. 1 and −1 are always self-inverse and (for primes >3) the other numbers form pairs of inverse elements. As there are only two elements remaining in Z/5, the inverse table is simple:

a	**a^{-1} (Z_5)**
1	1
2	3
3	2
4	4

8. What do you mean by digital signature?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. Digital signatures are the public-key primitives of message authentication. A digital signature is a technique that binds a person/entity to the digital data. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.



9. Difference between message digest and message authentication code?

Message Authentication code	**Message Digest Algorithm**
A message authentication code algorithm takes two inputs, one is a message and another is a secret key which produces a MAC, that allows us to verify and check the integrity and authentication of the message	A message digest algorithm takes a single input, like a message and produces a message digest which helps us to verify and check the integrity of the message

Any change in the secret key, or the message, results in different MAC being generated	Any change in the input message, results in different hash being generated
An attacker cannot identify and validate the correct MAC without the secret key	An attacker has no clue about the message, once a hash is generated
Most popular MAC are HMAC and MAC using DES in CBC mode	Most popular message digest algorithms are MD5 and SHA-1

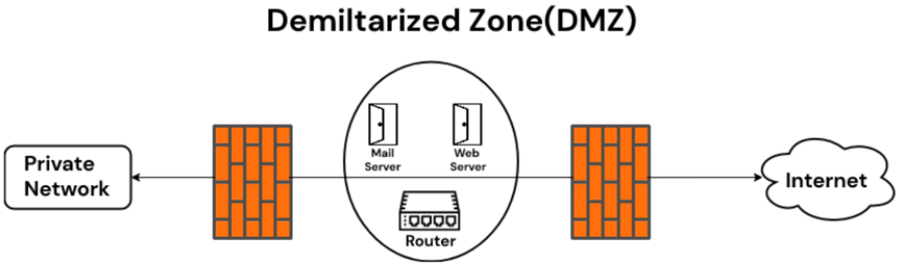
10. State the difference between http and https?

HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol.	HTTPS for HyperText Transfer Protocol Secure.
HTTP uses port number 80 for communication.	HTTPs uses 443 port number for communication.
HTTP is considered to be unsecure.	HTTPs is considered as secure.
HTTP works at Application Layer.	HTTPS works at Transport Layer.
In HTTP, Encryption is absent.	Encryption is present in HTTPS.
HTTP does not require any certificates.	HTTPS needs SSL Certificates.
HTTP does not improve search ranking	HTTPS helps to improve search ranking
HTTP faster than HTTPS	HTTPS slower than HTTP
HTTP does not use data hashtags to secure data.	While HTTPS will have the data before sending it and return it to its original state on the receiver side.
In HTTP Data is transfer in plaintext.	In HTTPS Data transfer in ciphertext.
HTTP Should be avoided.	HTTPS Should be preferred.
Search engines do not favour the insecure website.	Improved reputation of the website in search engine.
HTTP Does not require SSL/TLS or Certificates	HTTPS Requires SSL/TLS implementation with Certificates.
In HTTP Users ar worried about their data.	In HTTPS Users are confident about the security of their data.

11. What is DMZ or Demilitarized zone?

In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet. Any service provided to users on the public internet should be placed in the DMZ network. Servers and resources in the DMZ are accessible from the internet, but the rest of the internal LAN remains unreachable. This approach provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data from the internet.

A DMZ is typically created on a company’s internal network to isolate the company from external threats. The DMZ is a network barrier between the trusted and untrusted network in a company’s private and public network. The DMZ acts as a protection layer through which outside users cannot access the company’s data.



12. State the purpose of DMZ?

- A DMZ provides a buffer from the outside world for your computer systems.
- Creating a buffer zone between your systems and the internet allows you to function normally without being susceptible to external attacks. Keeping your internal systems inside a DMZ also makes it difficult for hackers to steal data.
- Hackers often seek out companies with weak computer security; this is why many organizations use a DMZ to protect their internal systems.
- The DMZ makes it easy for ethical hackers to find vulnerabilities and gain access to designated targets once they’re inside the buffer zone.

13. What do you mean by Firewall? State the purpose of Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules, it either accepts, rejects or drops that specific traffic. It acts as a barrier between internal private networks and external sources (such as the public Internet).

Some of the purposes of firewall are as follows,

- **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors.
- **Prevention of malware and other threats:** Firewalls can be set up to block traffic linked to known malware or other security concerns.
- **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity.
- **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.
- **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.