UNIT-1

define network security in 3 short points

1. Network security is the practice of protecting a computer network from unauthorized access, use, disclosure, disruption, modification, or destruction.
2. This can include using technologies such as firewalls, intrusion detection systems, and encryption, as well as implementing policies and procedures for incident response, disaster recovery, and regular security assessments.
3. The goal of network security is to maintain the availability, integrity, and confidentiality of the network and the information it carr

key range and key size in 5 short points

1. Key range is the set of possible values that a key can have.
2. Key size is the number of bits in a key, which determines the number of possible key values.
3. Larger key sizes have greater number of possible key values, making it more difficult for an attacker to guess the correct key.
4. Key size is an important aspect of the security of a cryptographic system.
5. Key range and key size are related, a larger key size means a larger key range, and vice versa.

interuption vs interception

An interruption is a temporary halt or break in the continuity of an activity or process. An interception, on the other hand, refers to the act of intercepting or stopping something that is in transit, such as a pass in football or a communication transmission.

plain text vs cipher text

Plain text refers to the unencrypted or original text that is readable and understandable. It is the data or information in its original form before it is encrypted. Cipher text refers to the encoded or encrypted text that is not readable or understandable without the use of a key or algorithm. It is the result of encrypting plain text and is often used to protect sensitive information from unauthorized access. The process of encryption converts plain text to cipher text and decryption converts the cipher text back to plain text.

encryption vs decryption

Encryption is the process of converting plain text into coded or unreadable text using a specific algorithm or key. Decryption is the reverse process of encryption, where the encoded text is converted back into plain text using the same algorithm or key. Both encryption and decryption are important for maintaining the security and privacy of data and communications

compare substitution ciphers with transposition ciphers in 3 short points

1. Substitution ciphers involve replacing plaintext letters or characters with other letters or characters in a systematic way.
2. Transposition ciphers involve rearranging the positions of the letters or characters in the plaintext without changing their identity.
3. Substitution ciphers are considered to be relatively weak because they can be broken by frequency analysis, but transposition ciphers can be more difficult to break because the letters retain their original frequency and identity.

2 basic functions used in encryption algorithms IN 3 SHORT POINTS

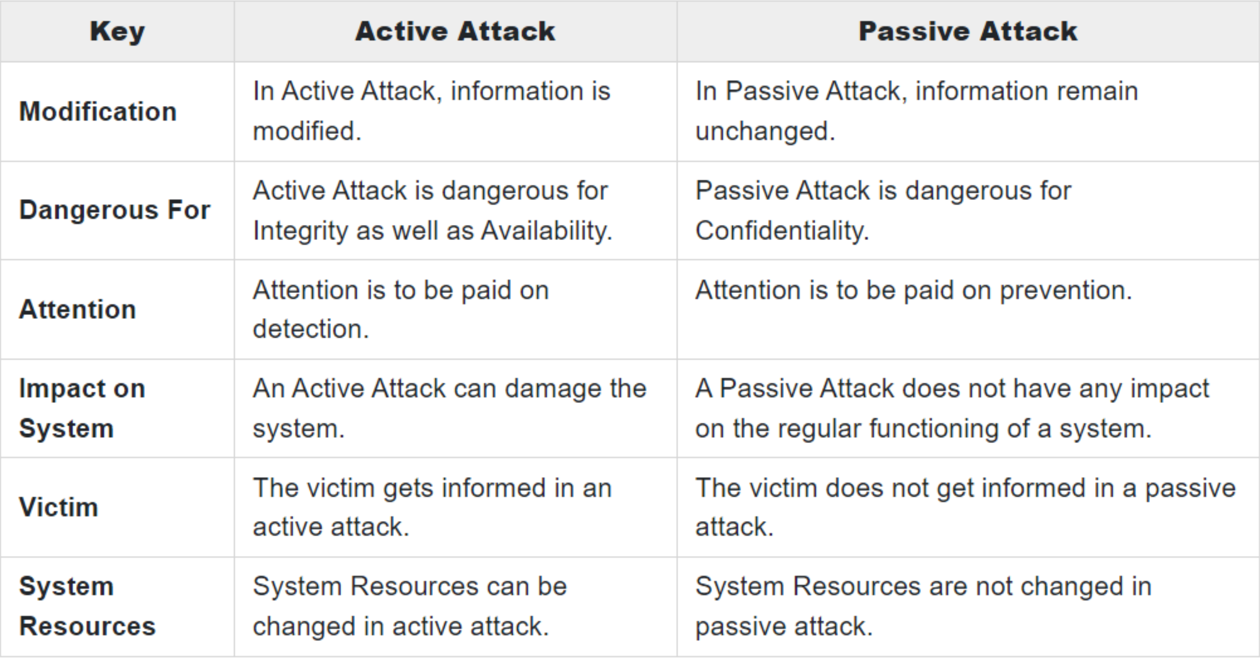
1. Key generation: the creation of a secret key that is used to encrypt and decrypt data.
2. Encryption/Decryption: the process of converting plaintext into ciphertext (encryption) and converting ciphertext back into plaintext (decryption) using the key.

These two functions are the basic functions used in encryption algorithms, more complex encryption algorithms use more functions to secure the data and make the encryption process more robust.

explain network security model in 3 short points

1. A network security model is a framework for protecting a computer network from unauthorized access, use, disclosure, disruption, modification, or destruction.
2. These models typically include multiple layers of security controls, such as firewalls, intrusion detection systems, and encryption, that work together to protect the network.
3. A network security model can also include policies and procedures for incident response, disaster recovery, and regular security assessments to ensure the ongoing protection of the network.

differences between passive attacks and active attacks



Key	Active Attack	Passive Attack
Modification	In Active Attack, information is modified.	In Passive Attack, information remain unchanged.
Dangerous For	Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
Attention	Attention is to be paid on detection.	Attention is to be paid on prevention.
Impact on System	An Active Attack can damage the system.	A Passive Attack does not have any impact on the regular functioning of a system.
Victim	The victim gets informed in an active attack.	The victim does not get informed in a passive attack.
System Resources	System Resources can be changed in active attack.	System Resources are not changed in passive attack.

various security mechanisms

There are many different security mechanisms that can be used to protect computer networks and systems. Some of the most common include:

- **Firewalls**: A firewall is a network security system that monitors and controls incoming and outgoing network traffic often used to block unauthorized access and protect against external threats.
- **Intrusion Detection and Prevention Systems (IDPS)**: When an IDPS detects a potential threat, it can take a variety of actions, such as logging the event, blocking the traffic, or alerting a security administrator.
- **Encryption**: Encryption is the process of converting plaintext into coded text, which can only be read by someone with the proper decryption key. used to protect data
- **Access control**: Access control is the process of granting or denying access to network resources based on a set of predefined security rules.
- **Virtual Private Network (VPN):** A VPN is a secure, encrypted connection between two devices over a public network. It allows users to access a private network as if they were connected to it directly, but with added security and privacy benefits.
- **Antivirus software**: Antivirus software scans files and system resources for known malware signatures and can also monitor network traffic for malicious activity.

write notes on one time pad subsitution technique

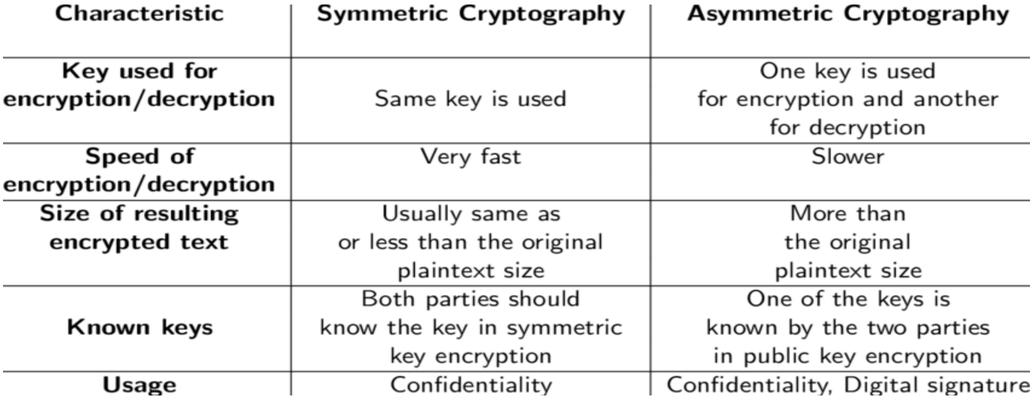
1. One-time pad (OTP) is a symmetric-key encryption technique that uses a truly random key that is at least as long as the plaintext message.

2. OTP is considered to be unbreakable if the key is truly random and is used only once.
3. OTP has some practical limitations, such as the difficulties in generating and distributing keys, especially for large amounts of data or for long-term use, and the need for a secure way to share the key between sender and receiver.

define confidentiality, integrity and availability IN VERY SHORT POINTS

1. Confidentiality: protecting against unauthorized access to information.
2. Integrity: protecting against unauthorized modification of information.
3. Availability: ensuring information is accessible to authorized parties when needed.

difference between symmetric and asymmetric key cryptography



Characteristic	Symmetric Cryptography	Asymmetric Cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plaintext size	More than the original plaintext size
Known keys	Both parties should know the key in symmetric key encryption	One of the keys is known by the two parties in public key encryption
Usage	Confidentiality	Confidentiality, Digital signature

define the terms security attacks in 3 short points

1. Security attacks are any attempts to exploit vulnerabilities in a system in order to gain unauthorized access, disrupt service, or steal sensitive information.
2. There are many types of security attacks, including malware, phishing, denial of service, and SQL injection.
3. These attacks can be targeted at networks, devices, applications, and individuals and can have a wide range of impacts, from minor inconvenience to major data breaches

define the term traffic analysis in 3 short points

1. Traffic analysis is the process of collecting, analyzing, and interpreting network data in order to understand network behavior and identify potential security threats.

2. This can include analyzing packet headers and payloads, monitoring network traffic patterns, and identifying anomalies or suspicious activity.
3. It can also involve tracking the source, destination, and path of network traffic in order to identify potential malicious actors or communication patterns.

what is passive attack, list types of passive attacks

A passive attack is a type of security threat in which an attacker listens in on network traffic without altering it. The attacker is typically trying to gather information from the network, such as usernames, passwords, or other sensitive data. Passive attacks do not disrupt the availability or integrity of the data, but rather aim to gain unauthorized access to sensitive information.

list types of passive attacks each 1 point

1. Sniffing: Capturing and analyzing network traffic in order to gather information
2. Traffic analysis: Collecting, analyzing, and interpreting network traffic data to understand the behavior of networked systems and identify potential security threats.
3. Traffic monitoring: Monitoring network traffic to gather information about network usage and performance and detect security incidents
4. Spying: Gathering information about a network, its users, or its systems without knowledge or permission of the parties involved.

discuss about principles of security one point each

1. **Confidentiality:** Ensures sensitive information is protected from unauthorized disclosure.
2. **Integrity:** Ensures data and resources are protected from unauthorized modification or alteration.
3. **Availability:** Ensures data and resources are accessible to authorized parties when needed.
4. **Authentication:** Verifies the identity of a user, device, or service.
5. **Non-repudiation**: Ensures parties involved in a transaction cannot deny their actions later.

define steganography in 3 points

1. Steganography is the practice of hiding information within other, seemingly innocent media.
2. The goal of steganography is to conceal the existence of the hidden information from unauthorized parties.
3. Common forms of steganography include hiding text or files within images, audio, and video files.

Unit 2

comparision between block ciphers and stream ciphers in 3 short points

1. Block ciphers encrypt fixed-sized blocks of data at a time, while stream ciphers encrypt individual bits or bytes of data as they are received.
2. Block ciphers can be more efficient for encrypting large amounts of data, while stream ciphers are better for real-time, continuous streams of data.
3. Block ciphers typically use a more complex encryption algorithm, while stream ciphers use a simpler algorithm that can encrypt data quickly and with less computational power.

rc5 vs blowfish in 4 short points

1. RC5 and Blowfish are both symmetric key encryption algorithms, which means that the same key is used for both encryption and decryption.
2. RC5 is a variable-key-size encryption algorithm and uses a variable number of rounds to increase security.
3. Blowfish is a symmetric key block cipher that is fast, well-suited for software and hardware implementations, it also uses a variable-key-size encryption algorithm.
4. Blowfish is considered to be more secure and faster than RC5 in software-only implementations.

write about strengths of DES algorithm IN VERY SHORT POINTS

1. Widely adopted and supported by various standard
2. Feasible for hardware implementation
3. High level of security (when key length is 56 bits)
4. Well-analyzed and understood

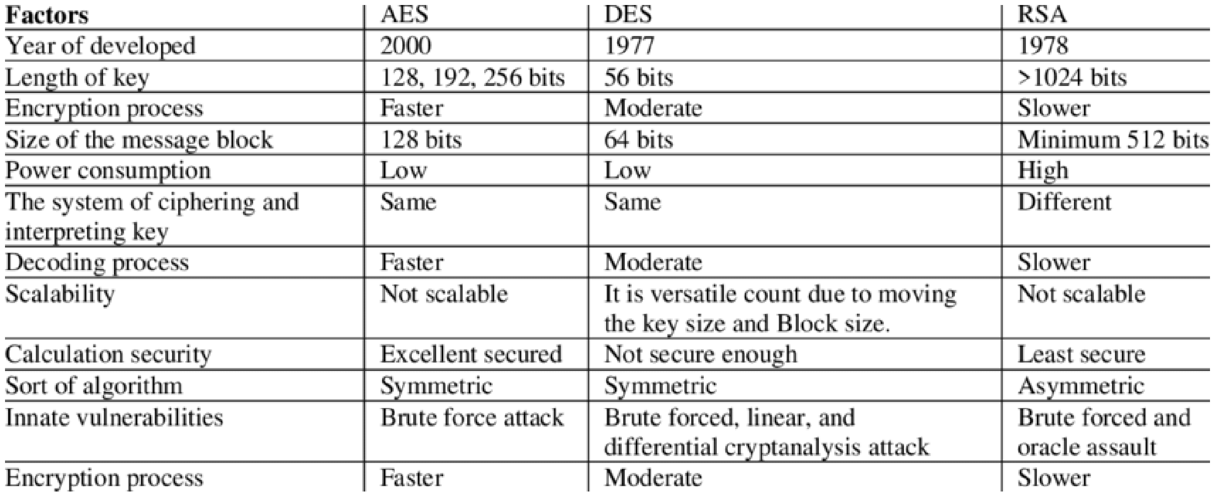
what are the principles of public key cryptosystem

1. **Public key and private key**: use two different keys, one for public-encryption and one for private-decryption.
2. **Key distribution**: rely on a method for distributing the public key to authorized parties.
3. **Asymmetry**: encryption and decryption keys are different.
4. **One-way functions:** infeasible to determine the private key from the public key.
5. **Digital signatures:** authenticate the identity of the sender and ensure the integrity of the message.
6. **Key exchange**: allowing for the secure exchange of messages without prior knowledge of a shared secret key.

advantages of key distribution in 3 short points

1. Key distribution allows for secure and efficient communication between parties, as the keys are needed for encryption and decryption of messages and data.
2. It increases security by protecting the keys from being intercepted or stolen by unauthorized parties.
3. Key distribution methods such as public key infrastructure (PKI) enables secure communication between parties that have not previously interacted, allowing for easy and secure communication with new entities.

differences between des and aes



Factors	AES	DES	RSA
Year of developed	2000	1977	1978
Length of key	128, 192, 256 bits	56 bits	>1024 bits
Encryption process	Faster	Moderate	Slower
Size of the message block	128 bits	64 bits	Minimum 512 bits
Power consumption	Low	Low	High
The system of ciphering and interpreting key	Same	Same	Different
Decoding process	Faster	Moderate	Slower
Scalability	Not scalable	It is versatile count due to moving the key size and Block size.	Not scalable
Calculation security	Excellent secured	Not secure enough	Least secure
Sort of algorithm	Symmetric	Symmetric	Asymmetric
Innate vulnerabilities	Brute force attack	Brute forced, linear, and differential cryptanalysis attack	Brute forced and oracle assault
Encryption process	Faster	Moderate	Slower

compare rc4 and rc5 in 3 short points

1. RC4 and RC5 are both symmetric key block ciphers developed by Ron Rivest of RSA Security.
2. RC4 is a stream cipher, meaning that it encrypts data one byte at a time, while RC5 is a block cipher, meaning that it encrypts data in fixed-size blocks.
3. RC4 is considered to be faster and less complex than RC5, but it has been found to be less secure, having known weaknesses and vulnerabilities. RC5, on the other hand, is considered more secure and has been used in various security protocols and applications.

comparisions between aes and des in 3 short points

1. AES uses a larger block size (128 bits) and key size (128, 192 or 256 bits) compared to DES (64-bit block size and 56-bit key size).
2. AES is considered more secure than DES due to its larger key size and the use of more advanced encryption techniques.
3. AES is more efficient than DES and is widely used in various security protocols and applications, such as SSL/TLS, IPsec, and wireless networks.

various attacks of rsa in 1 point each

1. **Brute-force attack:** Trying every possible combination of private key to decrypt the ciphertext.

2. **Factoring attack:** Attempting to factor a large composite number into its prime factors.
3. **Timing attack:** Exploiting differences in time to deduce information about the private key.
4. **Side-channel attack:** Exploiting information leaked during execution of RSA to deduce information about the private key.

write notes on key distribution in 3 short points

1. Key distribution is the process of securely distributing cryptographic keys to the parties that need to use them.
2. It is important for ensuring the security of communications and transactions, as the keys are needed for encryption and decryption of messages and data.
3. There are various methods for key distribution, such as using a central key server, public key infrastructure (PKI), and key agreement protocols

why rsa is secure in 3 short points

1. RSA's security relies on the mathematical properties of large prime numbers, making it difficult for an attacker to factorize a large composite number and determine the private key.
2. RSA uses a public key for encryption and a private key for decryption, making it more secure than symmetric key algorithms.
3. RSA is widely used and has been extensively studied and analyzed, and is considered to be a secure encryption method.

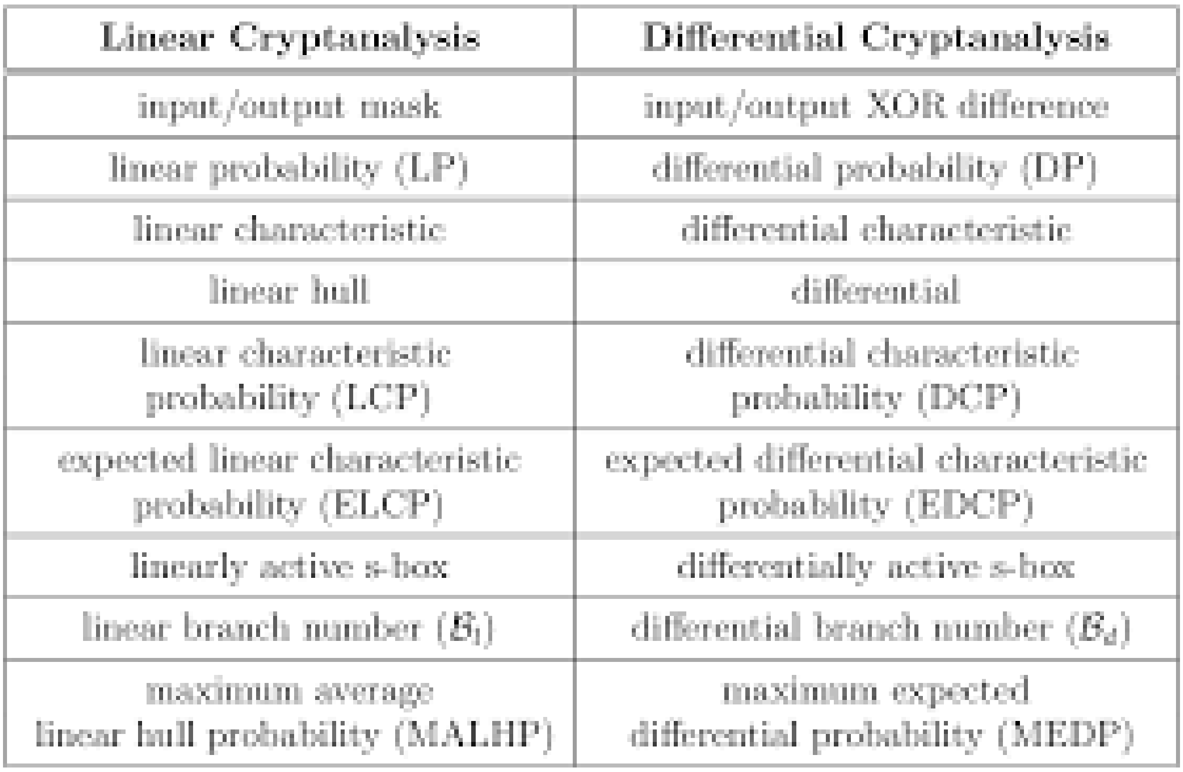
note on location of encryption devices IN 3 SHORT POINTS

1. Encryption devices can be located at various points within a network depending on the specific security requirements and architecture of the network.
2. Common locations for encryption devices include at the perimeter of the network, within the internal network, and on endpoints such as laptops and mobile devices.
3. The location of encryption devices can affect the overall security of the network, as well as the performance and management of the encryption process.

purpose of s boxes in DES explain the avalanche effect in 3 short points

1. S-boxes in the Data Encryption Standard (DES) are non-linear substitution boxes that are used to introduce diffusion in the encryption process, making it more resistant to certain types of cryptographic attacks.
2. The avalanche effect refers to the property of a cryptographic system, where a small change in the plaintext or key results in a significant change in the ciphertext.
3. This effect is important in making the encryption more secure as it makes it harder for an attacker to determine the plaintext from the ciphertext, even if they know a small part of the key or the plaintext.

difference between differential cryptanalysis and linear cryptanalysis



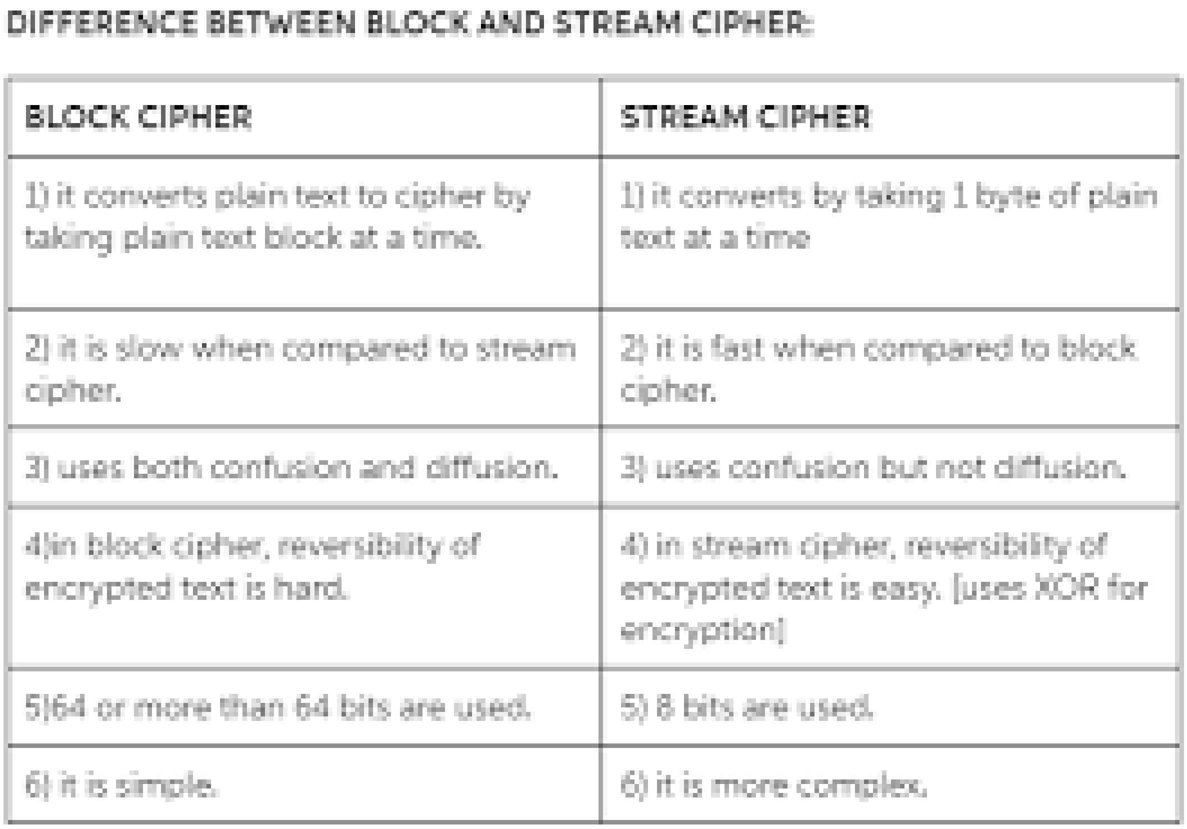
Linear Cryptanalysis	Differential Cryptanalysis
input/output mask	input/output XOR difference
linear probability (LP)	differential probability (DP)
linear characteristic	differential characteristic
linear hull	differential
linear characteristic probability (LCP)	differential characteristic probability (DCP)
expected linear characteristic probability (ELCP)	expected differential characteristic probability (EDCP)
linearly active s-box	differentially active s-box
linear branch number (B_l)	differential branch number (B_d)
maximum average linear hull probability (MALHP)	maximum expected differential probability (MEDP)

Why do some block cipher modes of operation only use encryption while others use both **encryption and decryption IN 3 SHORT POINTS**

1. Some block cipher modes of operation, such as Electronic Code Book (ECB) and Cipher Block Chaining (CBC), only use encryption to scramble the plaintext.

2. Other block cipher modes, such as Counter (CTR) and Cipher Feedback (CFB), use both encryption and decryption to ensure that the ciphertext cannot be decrypted without the proper key.
3. The specific design of a block cipher mode of operation will determine whether it requires encryption only or both encryption and decryption to provide the desired level of security

Differentiate between block cipher and stream cipher



DIFFERENCE BETWEEN BLOCK AND STREAM CIPHER:

BLOCK CIPHER	STREAM CIPHER
1) it converts plain text to cipher by taking plain text block at a time.	1) it converts by taking 1 byte of plain text at a time
2) it is slow when compared to stream cipher.	2) it is fast when compared to block cipher.
3) uses both confusion and diffusion.	3) uses confusion but not diffusion.
4)in block cipher, reversibility of encrypted text is hard.	4) in stream cipher, reversibility of encrypted text is easy. [uses XOR for encryption]
5)64 or more than 64 bits are used.	5) 8 bits are used.
6) it is simple.	6) it is more complex.

List important design considerations for a stream ciphers IN 4 VERY SHORT POINTS

1. Key stream generation method
2. Synchronization technique
3. Key length and period
4. Resistance to known attacks and implementation simplicity

What are the essential ingredients of a public key directory? What is a public-key certificate

1. PKI
2. Public keys
3. Digital certificates
4. Management of certificate revocation list

What is a public-key certificate IN 3 VERY SHORT POINTS

1. Electronic document binding a public key with identity.
2. Signed by a certificate authority
3. Used to establish trust and verify identity.

UNIT-3

define HMAC in 3 short points

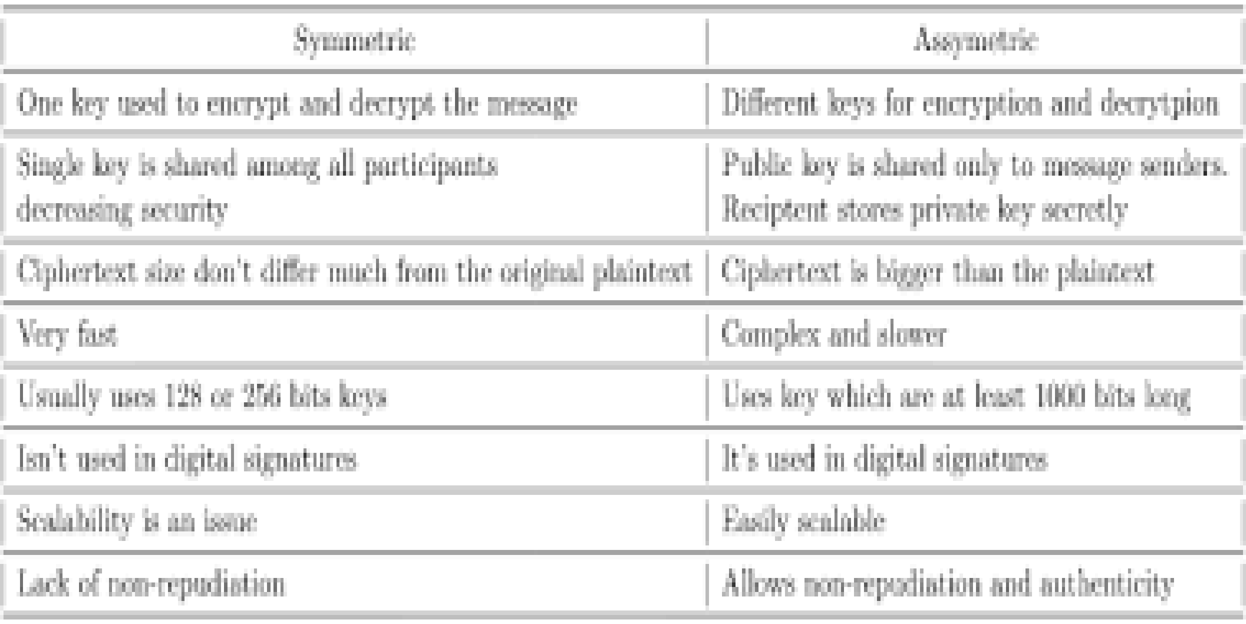
1. HMAC (Hash-based Message Authentication Code) is a type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key.
2. It is used to verify the integrity and authenticity of a message by comparing the message digest (hash) generated by the sender with the message digest generated by the recipient.
3. HMAC is widely used in various security protocols, such as SSL/TLS, SSH, and IPsec, to ensure the integrity and authenticity of digital communications and data.

define keberoes in 3 points

1. Kerberos is a network authentication protocol that provides secure authentication for client-server applications by using a central authentication server known as the Key Distribution Center (KDC)
2. Kerberos uses tickets, encrypted messages that contains the user's identity and a session key, to authenticate users to servers.
3. Kerberos uses symmetric key cryptography to secure communications, where each user and server has a unique secret key known only to the KDC and the specific entity.

discuss about SHA Algorithm in 3 points

1. SHA (Secure Hash Algorithm) is a family of cryptographic hash functions developed by the National Institute of Standards and Technology (NIST) and used for digital signature and data integrity verification.
2. There are several versions of SHA, including SHA-1, SHA-2, and SHA-3. Each version has a different message digest length and internal compression function.
3. SHA is widely used in various security protocols and applications, such as SSL/TLS, PGP, SSH, and IPsec, to ensure the integrity and authenticity of digital communications and data



Symmetric	Assymetric
One key used to encrypt and decrypt the message	Different keys for encryption and decrytpion
Single key is shared among all participants decreasing security	Public key is shared only to message senders. Recipient stores private key secretly
Ciphertext size don't differ much from the original plaintext	Ciphertext is bigger than the plaintext
Very fast	Complex and slower
Usually uses 128 or 256 bits keys	Uses key which are at least 1000 bits long
Isn't used in digital signatures	It's used in digital signatures
Scalability is an issue	Easily scalable
Lack of non-repudiation	Allows non-repodiation and authenticity

Compare and contrast Kerberos version 5 in 3 short points

1. Kerberos version 5 has improved security features such as replay cache and pre-authentication compared to version 4.
2. Version 5 supports multiple encryption types, while version 4 only supports one (DES).
3. Version 5 supports larger packet sizes, providing more scalability and flexibility for large-scale network deployments, unlike version 4.

List out Services of X.509 Authentication IN VERY SHORT POINTS

1. Authentication of end-entities

2. Authentication of CA
3. Management of certificate revocation
4. Time stamping
5. Secure communication for certificate requests and management
6. Validation of certificate path
7. Management of certificate policy and practice statement
8. Generation and distribution of public key material
9. Certificate archival
10. Management of key escrow

List out the Properties of Public Key IN VERY SHORT POINTS

1. Asymmetry
2. Uniqueness
3. Non-repudiation
4. Publicly available
5. Large key size
6. Complex mathematical structure
7. One-way function
8. Computationally infeasible to determine private key from public key
9. Can be used for digital signature, encryption, key exchange.

Define Elgamal Digital Signature in 3 short points

1. Elgamal digital signature is a public-key based digital signature algorithm.
2. Based on the computational difficulty of solving the discrete logarithm problem
3. The sender uses private key to sign the message, recipient uses public key to verify the signature.

Define digital signature? Explain its role in network security in 3 short points

1. Digital signature is a way to ensure authenticity and integrity of a digital message or document.
2. It provides non-repudiation, meaning sender cannot deny sending the message.

3. It plays a crucial role in ensuring the security of sensitive or confidential information sent over a network, and in verifying the authenticity of software update

WHAT IS A DIGITAL SIGNATURE IN 3 POINTS

1. A digital signature is a mathematical technique used to verify the authenticity and integrity of a digital message or document.
2. It uses the sender's private key to create a unique code, called a signature, that is appended to the message or document.
3. The recipient can then use the sender's public key to verify the signature and confirm that the message or document has not been tampered with and that it was indeed sent by the claimed sender.

PUBLIC KEYT CRYPTOGRAPHY 3 SHORT POINTS

1. Public key cryptography, also known as asymmetric cryptography, uses a pair of keys, one public and one private, to encrypt and decrypt data.
2. The public key is used to encrypt data and can be freely shared, while the private key is used to decrypt data and must be kept secret.
3. This type of cryptography is particularly useful for secure communication, digital signatures, and key exchange, as it eliminates the need for a secure pre-shared key.

EXPLAIN DSA ALGO IN SHORT POINTS

1. DSA stands for Digital Signature Algorithm, it is a standard for digital signatures and it is based on the mathematical properties of large prime numbers.
2. It uses a pair of keys, one private and one public, to generate and verify digital signatures.
3. The private key is used to create a digital signature, and the public key is used to verify it. DSA is considered to be more secure than RSA for digital signatures, but it is not commonly used for encryption.

explain HMAC algo in simple ways

HMAC (Hash-based Message Authentication Code) is a type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. As the name suggests, the technique involves using a cryptographic hash function in combination with a secret key. The input to the function is both the message (or data) being authenticated and the key, and the output is a fixed-length string of characters, known as the message authentication code (MAC). The recipient of the message and the MAC can then use the same key to verify that the message has not been tampered with by recomputing the hash and comparing it to the MAC.

In simple words, HMAC uses the key and a hash function to create a digital signature for a given message, which can be used to verify the integrity and authenticity of the message. It can be thought of as a secure way to check that a message has not been tampered with and that it came from the intended sender.

hmac vs cmac in short points

- HMAC (Hash-based Message Authentication Code) is a type of message authentication code (MAC) that uses a cryptographic hash function in combination with a secret key.
- CMAC (Cipher-based Message Authentication Code) is similar to HMAC, but it uses a symmetric block cipher in place of a hash function.
- The key is used in both the encryption and decryption process of CMAC while in HMAC it is used to create a digital signature.
- CMAC is faster than HMAC because it uses a block cipher, which is generally faster than a hash function.
- CMAC is more secure than HMAC as it uses a symmetric key block cipher and the block cipher encrypts the message while HMAC only creates a hash of the message.
- HMAC is more widely supported than CMAC and is available in many cryptographic libraries and protocols.
- CMAC is recommended for use in cryptographic protocols that require both integrity and authenticity protection like AES-CMAC, a variant of the Advanced Encryption Standard (AES) algorithm.

Elgamal Digital Signature in very short points

- ElGamal Digital Signature is a digital signature scheme based on the ElGamal encryption algorithm.
- It uses the same mathematical principles as ElGamal encryption but for digital signing.

- The private key is used to generate the signature, which can be verified using the corresponding public key.
- It provides both integrity and authenticity of the message
- The signature is a pair of large integers and relatively larger than other digital signature schemes.
- Based on the intractability of the discrete logarithm problem (DLP)
- Not widely used in practice due to larger signature size.

signature scheme in very short points

- Digital signature scheme is a method for ensuring authenticity and integrity of digital messages or documents.
- Uses a pair of keys, one public and one private, to encrypt and decrypt the signature.
- private key is used to generate the signature and public key is used to verify the signature.
- Provide a way to confirm the identity of the sender and ensure that the message has not been tampered with.
- Based on mathematical algorithms such as RSA, DSA, and ElGamal.
- Two types: symmetric and asymmetric (public key)

public key infrastructure in short points

Public Key Infrastructure (PKI) is a system for managing digital certificates and public-private key pairs. Here are a few key points about PKI:

- PKI provides a way to establish trust in the authenticity of digital certificates and the identity of the parties involved in a digital transaction.
- PKI uses a combination of digital certificates, certificate authorities (CA), and other related components to manage public keys and provide a secure infrastructure for digital communications.
- PKI enables secure communication and data exchange through encryption and digital signature.
- PKI is used in various applications such as secure email, VPNs, secure web browsing, and digital signatures.

- PKI helps to protect against man-in-the-middle attack (MITM)
- PKI can be based on a hierarchical or web of trust model.
- PKI is a complex system that requires careful management and maintenance to ensure its continued effectiveness.

define hash function in 3 short points

1. Hash functions are mathematical functions that take an input (or 'message') and return a fixed-size string of characters, which is called the 'hash' or 'digest'.
2. The same input will always produce the same output, but even a small change to the input will produce a very different output.
3. Hash functions are widely used in computer science, cryptography, and information security applications to check the integrity of data, to generate unique identifiers and also in password storage.

objectives of hmac in 3 short points

1. HMAC (Hash-based Message Authentication Code) is a mechanism for message authentication using a secret key.
2. The main objectives of HMAC are to provide data integrity and authenticity of the message.
3. It uses a hash function in combination with a secret key to generate a message authentication code (MAC) that is appended to the message, allowing the receiver to verify the integrity and authenticity of the message.

differences between kerboes 4 and kerboes 5 in 3 short points

1. Kerberos is a network authentication protocol that provides secure authentication for client/server applications by using secret-key cryptography.
2. Kerberos version 4 and Kerberos version 5 are two different versions of the Kerberos protocol.
3. Kerberos v5 introduced several improvements over v4, such as stronger encryption, better error reporting, improved support for internationalization, and the ability to work with a wider variety of authentication mechanisms.

features of SHA ALGO in very short points

1. SHA (Secure Hash Algorithm) is a family of cryptographic hash functions.
2. It produces a fixed-size output, called a hash or digest, from an input of any size.
3. It uses a mathematical algorithm to transform the input into a unique output.
4. It is designed to be collision-resistant and one-way function.
5. It has various versions like SHA-1, SHA-2 and SHA-3.

how hash functions are different from public key cryptography and secret key cryptography in 3 short points

1. Hash functions are mainly used for data integrity and unique identification, while public key and secret key cryptography are mainly used for secure communication and confidentiality.
2. Hash functions use a one-way function to transform input into a unique output, while public key and secret key cryptography use a combination of encryption and decryption.
3. Hash functions use the same key for the input and output, while public key and secret key cryptography use different keys for encryption and decryption.

what is MAC in 4 short points

1. MAC (Message Authentication Code) is a mechanism for message authentication using a secret key.
2. It uses a cryptographic function to generate a fixed-size code that is based on the message and the secret key.
3. The recipient can use the same key and the same function to check the integrity and authenticity of the message.
4. It can be used in combination with encryption to provide both confidentiality and integrity of the message.

what are the authentication functions in short points

Authentication functions are the set of procedures or mechanisms used to verify the identity of a user, device, or system.

1. Knowledge-based authentication: password or a PIN.
2. Possession-based authentication: It is based on possession of a token, such as a smart card or a mobile phone
3. Inherence-based authentication: such as a fingerprint, voiceprint, or facial features.
4. Location-based authentication: It is based on the geographic location of the user or device, using GPS
5. Time-based authentication: It is based on the time of access attempts.
6. Two-factor authentication (2FA) : It is based on two different factors, such as something you know, something you have, something you are.

what properties does a hash func need to have which is useful for message authentication in short points

1. Collision-resistance
2. Preimage resistance
3. Deterministic
4. Quick computation
5. Fixed output size
6. Avalanche effect
7. One-way function
8. Publicly verifiable

UNIT 4

compare ssl and ip security in 3 short points

1. SSL (Secure Sockets Layer) and IPSec (Internet Protocol Security) are both protocols used to secure network communications.
2. SSL is primarily used to secure web traffic, while IPSec can be used to secure any IP-based communication.
3. SSL uses a combination of public key and symmetric key encryption to secure the connection, while IPSec uses only symmetric key encryption for security.

4 differences between ssl and tls in 4 short points

1. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are both cryptographic protocols used to secure network communications.

2. SSL was the original protocol, but it has been deprecated and replaced by TLS.
3. SSL uses a single encryption layer to secure the connection, while TLS uses multiple encryption layers for more robust security.
4. SSL is vulnerable to certain types of attacks, such as the "POODLE" attack, which is not possible with the newer version of TLS.

operations of ssl record protocol in very short points

1. The SSL Record Protocol is responsible for providing secure communication between the client and server using the SSL/TLS protocol.
2. It is responsible for the confidentiality and integrity of the data exchanged between the client and server.
3. It is responsible for fragmenting and encapsulating data, encrypting, and adding message authentication codes (MAC) before sending.
4. It also handles the process of decrypting and verifying the integrity of received data before passing it to the higher layers.

define wireless security and its advantages in 3 short points

1. Wireless security refers to the measures taken to protect wireless networks from unauthorized access and to safeguard the privacy of the data transmitted over the airwaves.
2. Advantages of wireless security include the ability to easily connect multiple devices to a network, increased mobility, and the ability to connect to a network from remote locations.
3. Implementing wireless security measures such as encryption, firewalls, and secure login credentials can help protect the network from hacking and other cyber attacks, and protect the privacy and integrity of the data being transmitted.

what protocol is used to covey ssl related alerts to the peer entity and describe the fields in 4 short points

1. **The Alert Pro**tocol is used to convey SSL-related alerts to the peer entity.
2. It is a simple protocol that is used to convey SSL-related alerts and error messages between the client and server.
3. It uses a single byte to indicate the alert level (warning or fatal) and another byte to indicate the specific alert message.
4. The peer entity can interpret the alert message and take appropriate action, such as shutting down the SSL connection or renegotiating the session.

fields of alert protocol

The Alert Protocol contains two fields:

1. Alert Level: This field is used to indicate the severity of the alert. It is a single byte and can have two values: warning or fatal.
2. Alert Description: This field is used to indicate the specific alert message. It is a single byte and can have a variety of values, such as "close_notify" to indicate that the SSL session is being closed, or "unexpected_message" to indicate that an unexpected message was received during the SSL Handshake.

List notations used in HTTPS? in short points

1. SSL/TLS
2. HTTP
3. HTTPS URL
4. SSL/TLS Certificates
5. Public Key Infrastructure (PKI)
6. Public and Private Key
7. Digital Signatures

describe SSH in 3 short points

1. SSH (Secure Shell) is a network protocol used to securely access and manage remote systems.
2. It uses encryption to secure the communication between the client and the server, allowing for secure remote login, file transfer, and other network services.
3. SSH is commonly used to remotely access and manage servers, network devices, and other systems in a secure manner

Differentiate between IEEE 802.11&802.11i in 3 short points

1. IEEE 802.11 is the standard for wireless local area networks (WLANs), also known as Wi-Fi. It specifies the physical and data link layers of the OSI model for wireless communication.
2. IEEE 802.11i is an amendment to the IEEE 802.11 standard that provides enhanced security for wireless networks. It defines the Advanced Encryption Standard (AES) for data encryption, as well as new key management protocols such as Temporal Key Integrity Protocol (TKIP) and Robust Security Network (RSN).
3. IEEE 802.11 provides a basic level of security for wireless networks, while IEEE 802.11i provides stronger security features like stronger encryption and key management protocols, making it more secure than 802.11

UNIT 5

Explain about Virtual Elections IN 4 SHORT POINTS

1. Virtual elections refer to the use of electronic means such as internet or telephone to conduct voting.
2. Virtual elections offer potential benefits such as increased voter turnout, cost savings, and accessibility.
3. Virtual elections raise concerns such as security, accessibility, and transparency.
4. Auditing and voter verifiability may also be a challenge in virtual elections

4 SHORT POINTS ON INTERNET KEY EXCHANGE

1. Internet Key Exchange (IKE) is a security protocol used to establish a secure connection between two devices.
2. IKE uses a combination of public key encryption and symmetric key encryption to securely exchange keys.
3. IKE is typically used in conjunction with IPsec to create a VPN connection.
4. IKE uses two phases (IKE phase 1 and phase 2) to establish a secure connection and IKEv2 is the latest version of it.

4 SHORT POINTS ON TRANSPORT MODE AND IP MODE IN IP SECURITY

1. In IPsec, there are two modes of operation: transport mode and tunnel mode.
2. Transport mode encrypts only the payload of the IP packet, used for host-to-host communication.

3. Tunnel mode encrypts the entire IP packet, including both the header and the payload, used for network-to-network communication and VPNs.
4. Tunnel mode provides more security than transport mode as it encrypts both header and payload of the IP packet.

WHAT IS PGP IN 3 VERY SHORT POINTS

1. PGP stands for "Pretty Good Privacy," a data encryption and decryption program.
2. PGP uses a combination of public and symmetric key encryption for secure data communication.
3. PGP was developed by Phil Zimmermann in 1991 and is commonly used for email encryption.

OPERATIONS OF PGP IN VERY SHORT POINTS

1. PGP uses public-key cryptography to encrypt and sign messages.
2. The recipient's public key is used to encrypt the message, and the private key is used to decrypt it.
3. PGP also uses symmetric key encryption for message integrity and confidentiality.
4. PGP creates a digital signature for the message using the sender's private key, which can be verified by the recipient using the sender's public key.
5. PGP also provides a way to manage and revoke public keys through key servers.
6. PGP encrypts data on the sender's side, and decrypts data on the recipient's side.

DESCRIBE THE PGP MESSAGE FORMAT IN VERY SHORT POINTS

1. PGP encrypts the original message using symmetric key encryption for confidentiality.
2. A digital signature is created using the sender's private key for message integrity.

3. The symmetrically encrypted message and digital signature are then encrypted using the recipient's public key.
4. ASCII Armor is added to the message for easy transmission.
5. A Message Integrity Check (MIC) is added to ensure the integrity of the message.
6. All these parts are combined into a single message that can be sent to the recipient.

MIME IN 3 SHORT POINTS

1. MIME (Multipurpose Internet Mail Extensions) is a standard that extends the format of email messages to support text and attachments of different types like audio, video, images and application programs.
2. MIME defines a set of headers that specify the type of data and encoding used in the body of an email message.
3. MIME allows for the transfer of multimedia content in email messages, which was not possible with the original plain-text email format.

SIME IN 3 SHORT POINTS

1. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data, which is used to secure email messages.
2. It uses X.509 digital certificates to authenticate the sender and encrypt the message.
3. The recipient can then use their private key to decrypt the message and verify the digital signature, ensuring that the message is both confidential and authentic.

WHAT IS INSECURITY IN 3 SHORT POINTS

1. Insecurity refers to a state of being vulnerable to danger, harm, or loss.
2. It can refer to physical safety, emotional well-being, or the protection of personal information and assets.
3. Insecurity can manifest in various forms, such as fear, anxiety, or mistrust, and can have negative impacts on an individual's life.

compare AH and ESP in 3 short points

1. AH (Authentication Header) and ESP (Encapsulating Security Payload) are both protocols used to provide security for IP communications as part of IPsec.
2. AH provides integrity and authentication for IP packets while ESP provides confidentiality, integrity, and authenticity.
3. ESP is more versatile than AH because it can also provide confidentiality through encryption while AH only provide integrity and authentication.

describe esp format in 4 short points

1. ESP (Extensible System Profile) is a firmware-level interface specification for computer motherboards.
2. It defines interfaces and protocols for communication between firmware and hardware components.
3. It allows the firmware to control and configure components during the boot process.
4. ESP typically includes a FAT32 file system for storing files like drivers and utilities.

what is key management in 4 short points

1. Key management is the process of creating, distributing, storing, and managing encryption keys.
2. It is an important aspect of security because encryption keys are used to secure sensitive data such as communication, financial transactions and personal information.
3. Key management includes generation, exchange, storage, use, and replacement of keys.
4. It must ensure that keys are kept secret and are only accessible to authorized parties.

Discuss about Cross Site Scripting in 3 short points

1. Cross-Site Scripting (XSS) is a type of security vulnerability that allows an attacker to inject malicious code into a web page viewed by other users.
2. The injected code can be used to steal user data, such as cookies and session tokens, or to perform actions on behalf of the user, such as making unauthorized transactions.
3. XSS can be prevented by properly validating user input and encoding any user-supplied data before displaying it on a web page

describe the security combining association in 3 short points

1. Security Association (SA) is a set of security attributes that define a secure communication channel between two devices.
2. Security combining association is the process of combining multiple SAs, each providing a different level of security, to provide a more robust security solution.
3. By combining different SA attributes such as encryption, integrity protection, and authentication, it can provide a higher level of security than a single SA.

Why is the segmentation and reassembly function in pgp needed in 3 short points

1. To support large data transfer.
2. To overcome limitations of some systems in handling large data packets.
3. To improve the reliability of data transfer by allowing for retransmission of individual segments if they are lost or corrupted during transmission.

explain about e mail compatibility in 3 short points

1. Email compatibility refers to the ability of email clients and servers to successfully send and receive email messages without errors.
2. It depends on the compatibility of the email client and server software, as well as the adherence to email standards such as SMTP (Simple Mail Transfer Protocol) and MIME (Multipurpose Internet Mail Extensions).
3. Email compatibility also includes the ability to handle different types of attachments, email formats, and character encodings.