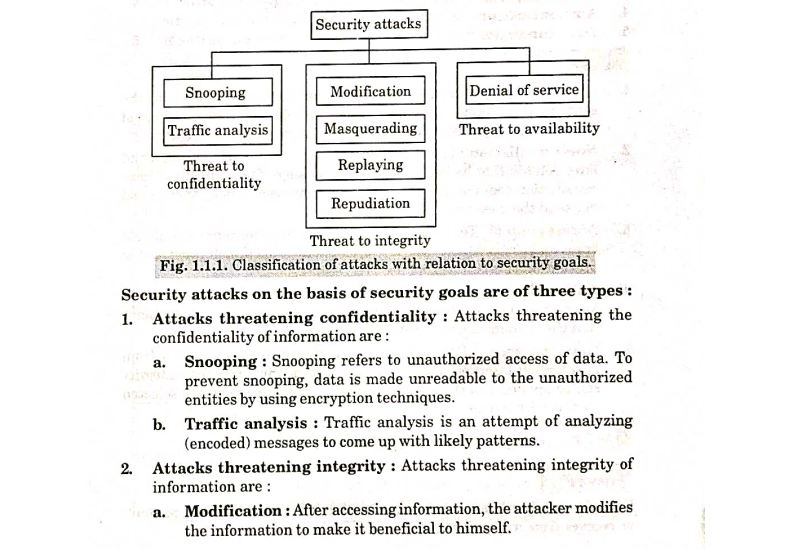
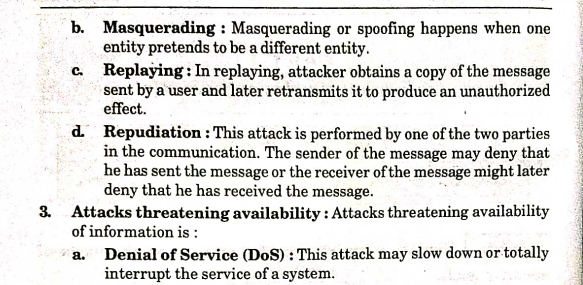
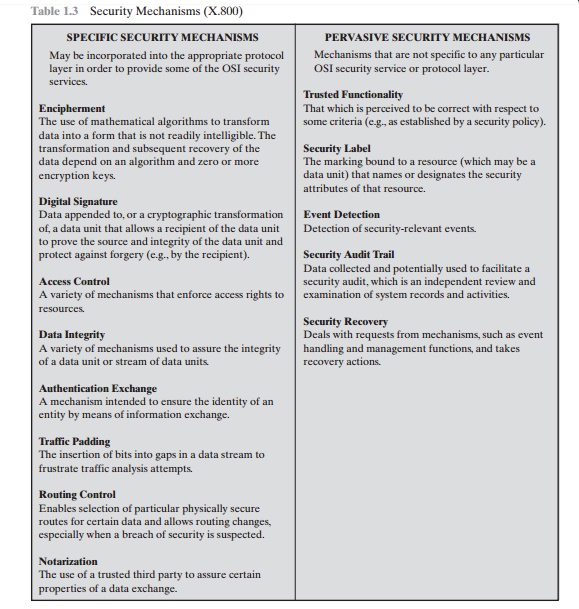
UNIT-1st

Qus1. Explain network security attacks on the basis of security goals?

Ans. security attacks refer to the sets of actions that the threat actors perform to gain any unauthorised access, cause damage to systems/computers, steal data, or compromise the computer networks.  




Qus2. Discuss security mechanisms?  
Ans. 

Hiding or covering the data.
Two techniques : Cryptography and Steganography
This mechanism appends to the data a check value created by a specific
process from the data itself.
 The receiver receives the data and the check value – creates a new
check value from the received data and compares with the received one.
If they are same then the integrity of the data is preserved.
 

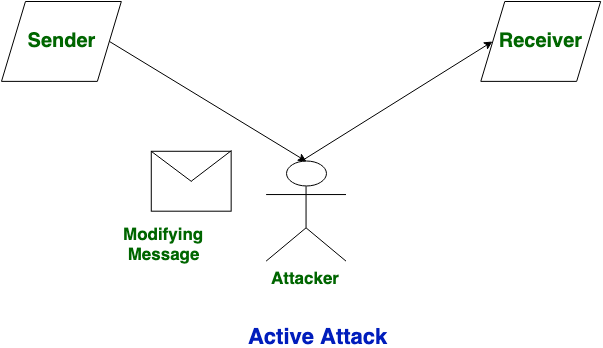
It is a means by which the sender can electronically sign the data and the
receiver can electronically verify the data.
Two entities exchange some messages to prove their identity to each
other.
It means inserting some bogus data into the data traffic to thwart the
adversary’s attempt to use the traffic analysis.
 

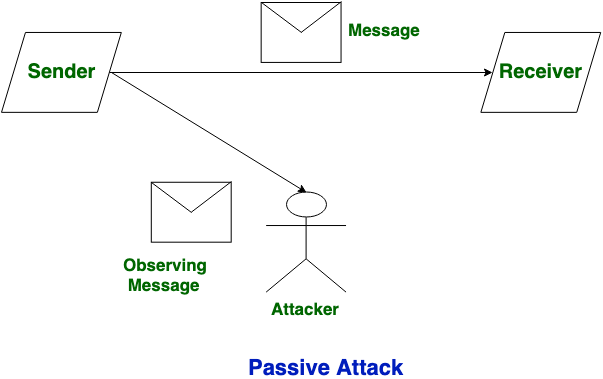
It means selecting and changing different available routes between the
sender and the receiver.
 Notarization means selecting a trusted third party to control the
communication between the two entities.
It uses methods to prove that a user has access rights to the data.
Example : Passwords, PINs
 

Qus3. Difference between active attacks and passive attacks?

Ans.

| **Active Attack** | **Passive Attack** |
| --- | --- |
| In an active attack, Modification in information takes place. | While in a passive attack, Modification in the information does not take place. |
| Active Attack is a danger to **Integrity** as well as **availability**. | Passive Attack is a danger to **Confidentiality**. |
| In an active attack, attention is on prevention. | While in passive attack attention is on detection. |
| Due to active attacks, the execution system is always damaged. | While due to passive attack, there is no harm to the system. |
| In an active attack, Victim gets informed about the attack. | While in a passive attack, Victim does not get informed about the attack. |
| In an active attack, System resources can be changed. | While in passive attack, System resources are not changing. |
| Active attack influences the services of the system. | While in a passive attack, information and messages in the system or network are acquired. |
| In an active attack, information collected through passive attacks is used during execution. | While passive attacks are performed by collecting information such as passwords, and messages by themselves. |
| An active attack is tough to restrict from entering systems or networks. | Passive Attack is easy to prohibit in comparison to active attack. |
| Can be easily detected. | Very difficult to detect. |
| The purpose of an active attack is to harm the ecosystem. | The purpose of a passive attack is to learn about the ecosystem. |
| In an active attack, the original information is modified. | In passive attack original information is Unaffected. |
| The duration of an active attack is short. | The duration of a passive attack is long. |
| The prevention possibility of active attack is High | The prevention possibility of passive attack is low. |
| Complexity is High | Complexity is low. |





Qus4. What is cryptanalysis? Explain the types of cryptanalysis attack?

Ans. Cryptanalysis is the study of cryptographic algorithms to find weaknesses and decrypt ciphertext without the secret key. Cryptanalysts study ciphers, cryptosystems, and ciphertext to understand how they work, and then use that knowledge to find ways to weaken or defeat them.

Here are some types of cryptanalysis attacks:

* **Chosen plaintext attack**

The attacker chooses some or all of the plaintext messages to be encrypted with a secret key. The attacker then analyzes the resulting ciphertexts to recover the key or some information about the plaintext.

* **Ciphertext-only attack**

The attacker only has access to the encrypted message and tries to recover the original plaintext or the key used to encrypt it.

* **Linear cryptanalysis**

The attacker studies the linear approximations of parity bits of the plaintext, ciphertext, and the secret key.

* **Cache side channel attack**

The attacker continuously monitors the memory addresses associated with the victim's secret information.

* **Frequency analysis**

The attacker uses the frequency of letters to translate ciphertext to plaintext.

Qus.5 Explain the term steganography in brief?

Ans. Steganography is the practice of hiding a secret message within another message or object to keep it private. The word comes from the Greek words steganos, meaning "hidden or covered", and graphein, meaning "to write".

Here are some examples of steganography:

* Embedding a secret message in a picture
* Hiding a secret message in a Word or Excel document
* Writing a message on a wood tablet and covering it with wax
* Hiding a secret message under the postage stamp on an envelope

Steganography is different from cryptography, which involves scrambling data or using a key. Steganography doesn't protect data from being read or modified, it just conceals the data's existence.

Steganography can be used to hide almost any type of digital content, including text, images, videos, audio, and network data. Digital images are a popular target because they contain a lot of redundant data that can be manipulated without noticeably altering the image's appearance.

Steganography can be combined with encryption for extra protection.  
  
Qus.6 Write as short note on block cipher and stream cipher?  
Ans. **Block Cipher** and **Stream Cipher** belong to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext. The main difference between a **Block cipher** and a **Stream cipher** is that a block cipher converts the plain text into cipher text by taking the plain text’s block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.

**Block Cipher:**

A block cipher encrypts data in fixed-size blocks typically 64 or 128 bits at a time. The encryption algorithm processes each block of data separately using the cryptographic key to transform the plaintext into the ciphertext. The Block ciphers use complex mathematical operations and permutations to the ensure the security of the encrypted data.

**Stream Cipher:**

A stream cipher encrypts data one bit or byte at a time rather than in fixed-size blocks. It generates a keystream that is combined with the plaintext to the produce ciphertext. The Stream ciphers are designed for the scenarios where data needs to be encrypted in the continuous stream making them suitable for the real-time applications.

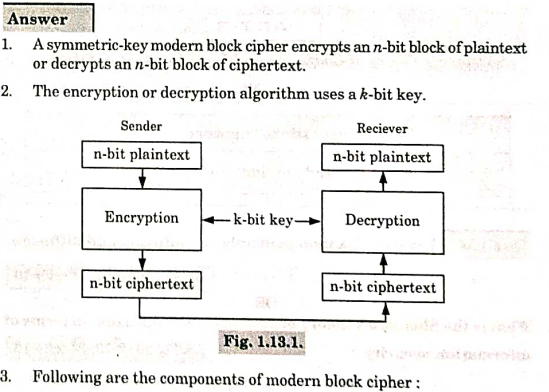
| **Block Cipher** | **Stream Cipher** |
| --- | --- |
| [Block Cipher](https://www.geeksforgeeks.org/block-cipher-modes-of-operation/) Converts the plain text into cipher text by taking plain text’s block at a time. | [Stream Cipher](https://www.geeksforgeeks.org/stream-ciphers/) Converts the plain text into cipher text by taking 1 bit plain text at a time. |
| Block cipher uses either 64 bits or more than 64 bits. | While stream cipher uses 8 bits. |
| The complexity of block cipher is simple. | While stream cipher is more complex. |
| Block cipher Uses confusion as well as diffusion. | While stream cipher uses only confusion. |
| In block cipher, reverse encrypted text is hard. | While in-stream cipher, reverse encrypted text is easy. |
| The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining). | The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback). |
| Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc. | While stream cipher works on substitution techniques like  Caesar cipher, polygram substitution cipher, etc. |
| Block cipher is slow as compared to a stream cipher. | While stream cipher is fast in comparison to block cipher. |
| Suitable for applications that require strong encryption, such as file storage and internet communications. | Suitable for applications that require strong encryption, such as file storage and internet communications. |
| More secure than stream ciphers when the same key is used multiple times. | Less secure than block ciphers when the same key is used multiple times. |
| key length is typically 128 or 256 bits. | key length is typically 128 or 256 bits. |
| Operates on fixed-length blocks of data. | Encrypts data one bit at a time. |

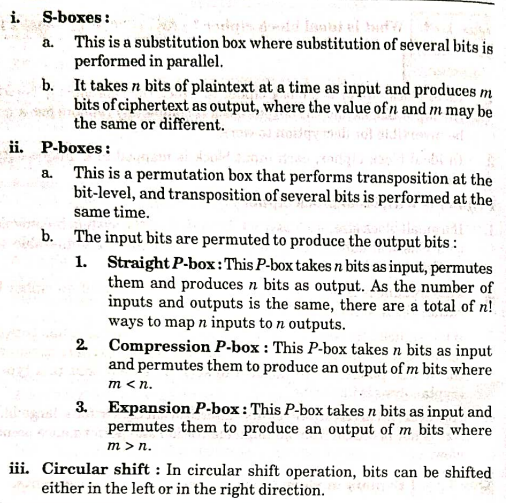
Qus.7 What is ideal cipher?

Ans. An ideal cipher is a block cipher that has a completely random relationship between the input and output blocks. It must also be invertible, meaning that each input block is mapped to a unique output block.

The ideal cipher model (ICM) is a construction that uses block cipher invocations and XOR operations to create a secure block cipher. The ICM is a well-known model that has been used to prove the security of cryptographic protocols and objects.

The ICM is equivalent to the Random Oracle model, and both are useful tools for designing cryptographic protocols. The ICM's power comes from the fact that it provides a large random table and allows the user to "program" it in their proofs.   
  
Qus.8 Explain modern block cipher with its components?





Qus.9 Explain Shannon principle of confusion and diffusion.  
Ans. The Shannon principle of confusion and diffusion are two properties of a secure cipher that Claude Shannon identified in his 1945 report A Mathematical Theory of Cryptography. These properties work together to make it difficult to use statistics and other cryptanalysis methods to break a cipher.

Here's what confusion and diffusion mean:

* **Confusion**

Makes it difficult to see the relationship between the plaintext and ciphertext by changing how the key is applied to the data. For example, if one bit of the key changes, about half of the bits in the ciphertext should change.

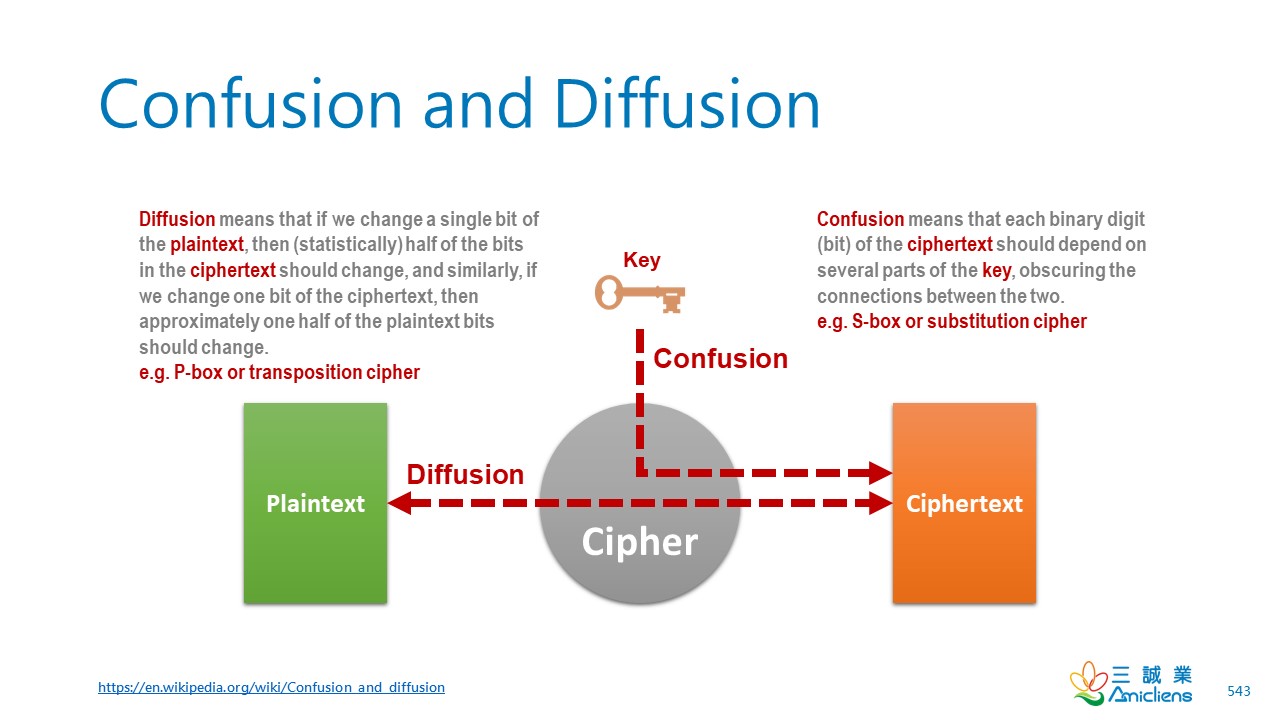
* **Diffusion**

Spreads the plaintext statistics throughout the ciphertext. For example, if one bit of the plaintext changes, about half of the bits in the ciphertext should change.

Some examples of ciphers that use only confusion or diffusion include:

* **One-time pad**: A cipher that relies entirely on confusion
* **Substitution cipher**: A cipher that uses confusion only
* **Transposition cipher**: A cipher that uses diffusion only

Modern block ciphers use both confusion and diffusion.



Qus.10 Explain DES algorithm with diagram?

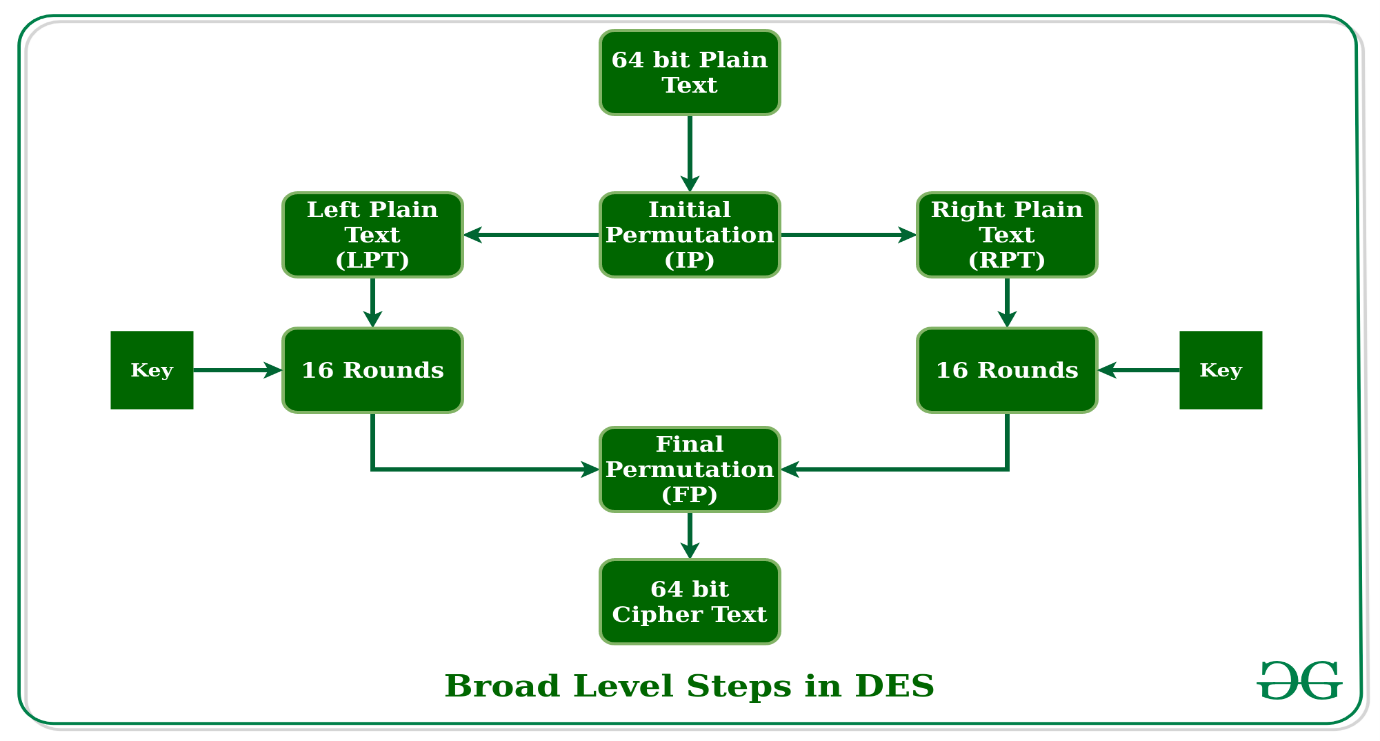
Ans. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher.

DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and [decryption](https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/), with minor differences. The key length is **56 bits**.

DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

* In the first step, the 64-bit plain text block is handed over to an initial [Permutation](https://www.geeksforgeeks.org/permutation/) (IP) function.
* The initial permutation is performed on plain text.
* Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
* Now each LPT and RPT go through 16 rounds of the encryption process.
* In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
* The result of this process produces 64-bit ciphertext.

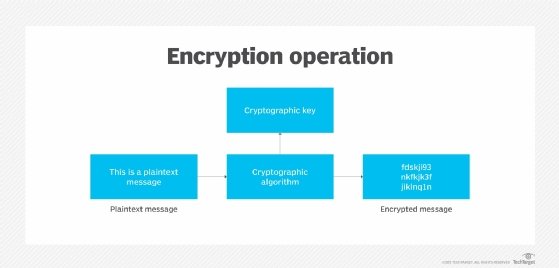
****

Qus.11 Write a short note on IDEA.  
Ans. The International Data Encryption Algorithm (IDEA) is a symmetric key [block cipher](https://www.techtarget.com/searchsecurity/definition/block-cipher) [encryption](https://www.techtarget.com/searchsecurity/definition/encryption) [algorithm](https://www.techtarget.com/whatis/definition/algorithm) designed to encrypt text to an unreadable format for transmission via the internet. It uses a typical block size of 128 bits and takes 64 bits as an input, i.e., 64-bit data.

It uses a series of mathematical operations, including modular arithmetic, bit shifting, and exclusive OR (XOR) operations, to transform the plaintext into ciphertext. The cipher is designed to be highly secure and resistant to various types of attacks, including differential and linear cryptanalysis.

The Simplified **International Data Encryption Algorithm (IDEA)** is a [**symmetric key**](https://www.geeksforgeeks.org/symmetric-key-cryptography/)**block**cipher that:

* **Plaintext block size:** 16 bits (divided into 4-bit chunks)
* **Key length:** 32 bits
* **Output:** 16-bit ciphertext
* **Processing:** Four complete rounds plus one half-round



Qus.12 Different modes of block cipher operations ?

Ans. An algorithm that uses a block cipher to offer information security, such as confidentiality or authenticity, is known as a block cipher mode of operation in cryptography.

Block cipher processes are classified into five categories: CFB (Cipher Feedback), OFB (Output Feedback), CTR (Counter), CBC (Cipher Block Chaining), and ECB (Electronic Code Block).

* **ECB Mode** − ECB is the simplest block cipher to operate. As each block of input plaintext is directly encrypted and the output is in the form of blocks of encrypted ciphertext.
* **CBC Mode** − Since ECB compromises certain security requirements, such as a direct connection between the cipher text and the plain text that makes it easier for attackers to decrypt the encoded information, CBC is the advanced mode of ECB.
* **CFB Mode** − In this case, the cipher is sent as feedback for the subsequent encryption block.
* **OFB Mode** − With the exception of sending the encrypted output as feedback rather than the actual cipher, which is the XOR output, the OFB operates in a manner very similar to that of the CFB.
* **CTR Mode** − An implementation of a basic counter-based block cipher is the CTR.

UNIT:2

Qus.1 Define group field and fine field of the form GF(p).

Ans. **Group**

A **group** is a set G*G* equipped with a binary operation ∗∗ that satisfies the following properties:

1. **Closure:** For all a,b∈G*a*,*b*∈*G*, a∗b∈G*a*∗*b*∈*G*.
2. **Associativity:** For all a,b,c∈G*a*,*b*,*c*∈*G*, (a∗b)∗c=a∗(b∗c)(*a*∗*b*)∗*c*=*a*∗(*b*∗*c*).
3. **Identity Element:** There exists an element e∈G*e*∈*G* such that a∗e=e∗a=a*a*∗*e*=*e*∗*a*=*a* for all a∈G*a*∈*G*.
4. **Inverse Element:** For every a∈G*a*∈*G*, there exists an a−1∈G*a*−1∈*G* such that a∗a−1=a−1∗a=e*a*∗*a*−1=*a*−1∗*a*=*e*.

Example: The integers ZZ under addition form a group.

**Field**

A **field** is a set F*F* equipped with two operations, ++ (addition) and ×× (multiplication), satisfying the following:

1. F*F* forms an abelian group under addition.
   * Closure, associativity, identity (additive identity: 0), and inverses (additive inverse: −a−*a*) are satisfied.
2. F∗=F∖{0}*F*∗=*F*∖{0} forms an abelian group under multiplication.
   * Closure, associativity, identity (multiplicative identity: 1), and inverses (a−1*a*−1 for a≠0*a*=0) are satisfied.
3. **Distributive Property:** Multiplication distributes over addition: a×(b+c)=a×b+a×c*a*×(*b*+*c*)=*a*×*b*+*a*×*c* for all a,b,c∈F*a*,*b*,*c*∈*F*.

Example: The set of rational numbers QQ under standard addition and multiplication forms a field.

**Finite Field of the Form GF(p)**

A **finite field** is a field with a finite number of elements. Fields of the form GF(p)GF(*p*), also known as **Galois Fields**, are special finite fields where:

1. p*p* is a prime number.
2. The field GF(p)GF(*p*) consists of p*p* elements: {0,1,2,…,p−1}{0,1,2,…,*p*−1}.
3. Addition and multiplication are performed modulo p*p*.

**Applications of GF(p)**

1. **Cryptography:**
   * Used in **RSA**, **Elliptic Curve Cryptography (ECC)**, and **Diffie-Hellman Key Exchange**.
2. **Error-Correcting Codes:**
   * GF(p) is fundamental in **Reed-Solomon codes** and **BCH codes**.

**Qus.2 State the Advanced Encryption Standard (AES).  
Ans.** The Advanced Encryption Standard (AES) is a symmetric key block cipher established as a federal standard by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is widely used in cryptography for securing sensitive data due to its robustness, efficiency, and adaptability to various hardware and software platforms.

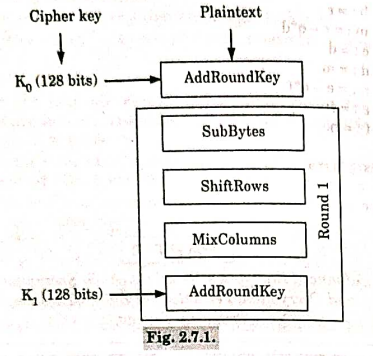
**Key Features of AES**

1. Symmetric Key Encryption:
   * The same key is used for encryption and decryption.
2. Block Cipher:
   * Operates on fixed-size blocks of data (128 bits per block).
3. Key Sizes:
   * AES supports key lengths of 128, 192, or 256 bits, offering different levels of security:
     + AES-128: 10 rounds
     + AES-192: 12 rounds
     + AES-256: 14 rounds
4. Standards and Applications:
   * AES is the de facto encryption standard for secure communications, used in Wi-Fi encryption (WPA2/WPA3), VPNs, TLS/SSL, and more.

**Working of AES**

AES consists of the following steps, repeated over a number of rounds depending on the key size:

1. Input Block:
   * The plaintext (128-bit block) is arranged in a 4×44×4 matrix called the state.
2. Key Expansion:
   * The key is expanded into multiple round keys using the Key Schedule algorithm.
3. Rounds:
   * Each round (except the last) involves four transformations:
     1. SubBytes:
        + A non-linear substitution step where each byte is replaced using an S-box (Substitution box).
     2. ShiftRows:
        + A transposition step where rows of the state matrix are cyclically shifted.
     3. MixColumns:
        + A mixing step where columns of the state matrix are transformed using matrix multiplication.
     4. AddRoundKey:
        + A step where the state matrix is XORed with the corresponding round key.
   * In the final round, the MixColumns step is omitted.
4. Output Block:
   * After the final round, the state matrix is converted back into a 128-bit ciphertext.



**Applications of AES**

1. **Data Encryption:**
   * Used in file encryption tools and secure messaging platforms.
2. **Secure Communication:**
   * Employed in protocols like TLS, IPsec, and WPA2 for encrypted communication.
3. **Storage Security:**
   * Protects data in SSDs, USB drives, and databases.
4. **Government and Industry Standards:**
   * Mandated for securing classified information by the U.S. government.

Qus.3 What are the advantages and disadvantages of AES.

Ans. **Advantages of AES (Advanced Encryption Standard)**

**1. High Security**

* AES is resistant to most cryptographic attacks, including brute force, differential, and linear cryptanalysis.
* With key sizes of 128, 192, and 256 bits, it offers varying levels of security suitable for different applications.

**2. Efficiency**

* AES is fast in both hardware and software implementations, making it suitable for a wide range of devices, including constrained environments like IoT devices.

**3. Flexibility**

* It supports multiple key lengths (128, 192, and 256 bits), allowing users to choose based on their security requirements.

**4. Standardized Algorithm**

* AES is widely adopted and standardized by NIST, ensuring compatibility across systems and applications globally.

**5. Scalability**

* AES works effectively across small and large datasets, making it suitable for various applications, from personal file encryption to securing enterprise systems.

**6. Lightweight**

* AES requires relatively low computational resources, making it suitable for devices with limited processing power, like smartphones and embedded systems.

**7. Open Algorithm**

* AES is an open standard, allowing for peer review and transparency, which increases trust in its security.

**Disadvantages of AES**

**1. Key Management**

* Symmetric encryption requires secure key distribution and management, which can be complex and prone to compromise if not handled correctly.

**2. Vulnerability to Side-Channel Attacks**

* While AES is mathematically secure, it can be vulnerable to **side-channel attacks**, such as:
  + Power analysis
  + Timing attacks
  + Cache attacks These attacks exploit implementation weaknesses rather than the algorithm itself.

**3. Block Size Limitation**

* AES operates on fixed-size blocks of 128 bits. If data does not fit exactly into a multiple of this block size, padding schemes are required, which can add complexity.

**4. Computational Overhead for Very Large Data**

* While efficient, the computational demands of AES can increase for extremely large datasets or in cases requiring real-time encryption of high-throughput streams.

**5. Lack of Forward Secrecy**

* Since AES is a symmetric key algorithm, if the key is compromised, all past and future communications encrypted with the same key are also compromised.

**6. Complexity in Software Implementations**

* While efficient in hardware, software implementations require careful optimization to prevent inefficiencies and side-channel vulnerabilities.

Qus.4 Illustrate the concept of Chinese Remainder Theorem.

Ans. The **Chinese Remainder Theorem** is a mathematical principle that provides a solution to a system of simultaneous congruences with pairwise coprime moduli. It states that if the moduli are coprime, a unique solution exists modulo the product of the moduli.

**Statement**

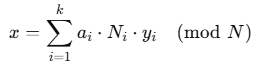
Let n1,n2,…,nk*n*1​,*n*2​,…,*nk*​ be pairwise coprime integers (gcd(ni,nj)=1gcd(*ni*​,*nj*​)=1 for i≠j*i*=*j*). Consider the system of congruences:

x≡a1(modn1)*x*≡*a*1​(mod*n*1​)x≡a2(modn2)*x*≡*a*2​(mod*n*2​)⋮⋮x≡ak(modnk)*x*≡*ak*​(mod*nk*​)

Then, there exists a unique solution x*x* modulo N=n1⋅n2⋅⋯⋅nk*N*=*n*1​⋅*n*2​⋅⋯⋅*nk*​.

**Steps to Solve Using CRT**

1. **Compute N*N*:**  
   Find the product of all moduli: N=n1⋅n2⋅⋯⋅nk*N*=*n*1​⋅*n*2​⋅⋯⋅*nk*​.
2. **Compute Nifor Each Modulus:**  
   For each ni*ni*​, compute Ni=Nni*Ni*​=*ni*​*N*​.
3. **Find the Modular Inverse of Ni​:**  
   Determine y*i*​such that Ni⋅yi≡1(mod ni)*Ni*​⋅*yi*​≡1(mod*ni*​) (this can be done using the Extended Euclidean Algorithm).
4. **Calculate the Solution:**  
   The solution x*x* is given by:



**Applications of CRT**

1. **Cryptography:**  
   Used in RSA encryption and decryption to optimize modular exponentiation.
2. **Distributed Computing:**  
   Helps in solving problems where computations are distributed across systems with different constraints.
3. **Error Correction:**  
   Used in error-detection systems and coding theory.

<https://youtu.be/e8DtzQkjOMQ?si=XFpElKAbX6LRGhIg>

Qus.5 Explain RSA algorithm and its Advantages and disadvantages.

Ans. <https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>

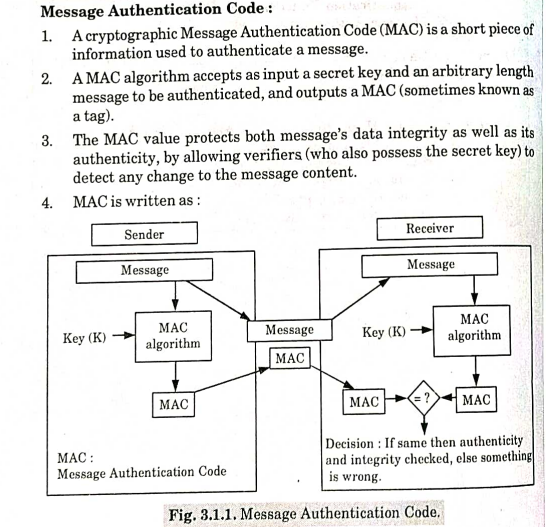
Qus.6 Difference between DES and AES.

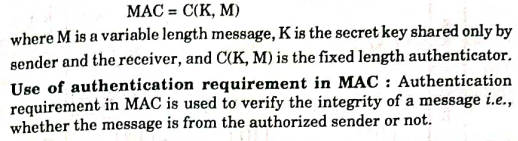
Ans.

| **S.No** | **AES** | **DES** |
| --- | --- | --- |
| **1.** | AES stands for [Advanced Encryption Standard](https://www.geeksforgeeks.org/advanced-encryption-standard-aes/) | DES stands for [Data Encryption Standard](https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/) |
| **2.** | The date of creation is 2001. | The date of creation is 1977. |
| **3.** | Byte-Oriented. | Bit-Oriented. |
| **4.** | Key length can be 128-bits, 192-bits, and 256-bits. | The key length is 56 bits in DES. |
| **5.** | Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits) | DES involves 16 rounds of identical operations |
| **6.** | The structure is based on a substitution-permutation network. | The structure is based on a [Feistel](https://www.geeksforgeeks.org/feistel-cipher/) network. |
| **7.** | The design rationale for AES is open. | The design rationale for DES is closed. |
| **8.** | The selection process for this is secret but accepted for open public comment. | The selection process for this is secret. |
| **9.** | AES is more secure than the DES cipher and is the de facto world standard. | DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES. |
| **10.** | The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition | The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation |
| **11.** | AES can encrypt 128 bits of plaintext. | DES can encrypt 64 bits of plaintext. |
| **12.** | It can generate Ciphertext of 128, 192, 256 bits. | It generates Ciphertext of 64 bits. |
| **13.** | AES cipher is derived from an aside-channel square cipher. | DES cipher is derived from Lucifer cipher. |
| **14.** | AES was designed by Vincent Rijmen and Joan Daemen. | DES was designed by IBM. |
| **16.** | It is faster than DES. | It is slower than AES. |
| **17.** | It is flexible. | It is not flexible. |
| **18.** | It is efficient with both hardware and software. | It is efficient only with hardware |

UNIT-3

Qus.1 Discuss the message authentication codes. Also give the use of authentication requirement in MAC.





Qus.2 What is hash function? Discuss SHA-512.

Ans. A **hash function** is a cryptographic algorithm that takes an input (or message) of arbitrary length and produces a fixed-length output, called a **hash value** or **digest**. Hash functions are widely used in cryptography for data integrity verification, digital signatures, and password storage.

**Characteristics of Hash Functions**

1. **Fixed-Length Output:**
   * Regardless of input size, the output hash has a fixed size (e.g., 256 bits, 512 bits).
2. **Deterministic:**
   * The same input always produces the same hash.
3. **Fast Computation:**
   * The hash value is computed quickly, even for large inputs.
4. **Pre-Image Resistance:**
   * It should be computationally infeasible to reverse-engineer the input from its hash value.
5. **Collision Resistance:**
   * It should be extremely unlikely for two different inputs to produce the same hash.
6. **Avalanche Effect:**
   * A small change in input significantly changes the output hash.

**SHA-512 (Secure Hash Algorithm - 512)**

SHA-512 is part of the SHA-2 family of cryptographic hash functions, designed by the National Security Agency (NSA) and standardized by NIST. It generates a **512-bit (64-byte)** hash value, making it highly secure.

**How SHA-512 Works**

**1. Input Preprocessing**

* The input message is preprocessed to fit the algorithm's requirements:
  1. **Padding:** The message is padded to ensure its length is a multiple of 1024 bits (128 bytes).
  2. **Length Encoding:** The length of the original message (in bits) is appended to the padded message.

**2. Initialization**

* SHA-512 uses **eight 64-bit words** as initial hash values (denoted H0*H*0​ to H7*H*7​).

**3. Message Parsing**

* The preprocessed message is divided into **1024-bit blocks**.

**4. Compression Function**

* Each 1024-bit block is processed in **80 rounds**:
  1. **Message Schedule:** A schedule of 80 64-bit words is created from the current block.
  2. **Round Operations:** The hash values are updated using bitwise operations, modular additions, and logical functions with predefined constants.

**5. Output**

* After processing all blocks, the concatenated hash values H0*H*0​ to H7*H*7​ form the final 512-bit hash.

Qus.3 Write the DSA of Digital Signature Standard.

Ans. The **Digital Signature Algorithm (DSA)** is a federal standard for digital signatures used in various cryptographic applications, including authentication, integrity verification, and non-repudiation. It is defined by the **Digital Signature Standard (DSS)**, which was established by the **National Institute of Standards and Technology (NIST)**.

**Steps Involved in DSA**

The DSA process involves three main steps: **Key Generation**, **Signature Generation**, and **Signature Verification**.

**1. Key Generation**

**Key Generation** is the first step where the signer generates a public-private key pair:

* **Prime number generation:**
  1. Select a **large prime number** p*p* and a **generator** g*g*, which is a number less than p*p*.
  2. The prime number p*p* and g*g* are publicly known.
* **Private Key x*x*:**
  1. Select a **random integer** x*x* such that 0<x<q0<*x*<*q*, where q*q* is a 160-bit prime divisor of p−1*p*−1 (used to define the group structure).
  2. The private key x*x* is kept secret by the signer.
* **Public Key y*y*:**
  1. Compute y=gxmod  p*y*=*gx*mod*p*.
  2. The public key y*y* is made publicly available and is used by others to verify signatures.

**2. Signature Generation**

Once the keys are generated, the **signer** creates a signature for a given message using the private key:

* **Hash the message:**
  + Compute a **hash** of the message m*m* using a cryptographic hash function (e.g., SHA-1 or SHA-256).
  + This hash value H(m)*H*(*m*) is used to create the signature.
* **Signature components:**
  + Generate a **random number** k*k* (between 1 and q−1*q*−1) that is used only once for the signature.
  + Compute r=(gkmod  p)mod  q*r*=(*gk*mod*p*)mod*q*.
  + Compute s=(k−1⋅(H(m)+x⋅r))mod  q*s*=(*k*−1⋅(*H*(*m*)+*x*⋅*r*))mod*q*, where k−1*k*−1 is the modular inverse of k*k* modulo q*q*.
* **Digital signature:**
  + The **signature** consists of the two values (r,s)(*r*,*s*), which are sent along with the message to the recipient.

**3. Signature Verification**

The recipient verifies the digital signature using the **public key** of the signer:

* **Hash the message:**
  + Compute the hash H(m)*H*(*m*) of the received message.
* **Signature components:**
  + The recipient receives the signature (r,s)(*r*,*s*) along with the message.
  + Ensure that r*r* and s*s* are within the valid range: 0<r<q0<*r*<*q* and 0<s<q0<*s*<*q*.
* **Verify the signature:**
  + Compute w=s−1mod  q*w*=*s*−1mod*q* (modular inverse of s*s*).
  + Compute u1=(H(m)⋅w)mod  q*u*1​=(*H*(*m*)⋅*w*)mod*q* and u2=(r⋅w)mod  q*u*2​=(*r*⋅*w*)mod*q*.
  + Compute v=((gu1⋅yu2)mod  p)mod  q*v*=((*gu*1​⋅*yu*2​)mod*p*)mod*q*.
* **Decision:**
  + If v=r*v*=*r*, the signature is valid (the message is authentic and unaltered).
  + If v≠r*v*=*r*, the signature is invalid.

Qus.4 What are the properties and requirements for a digital signature?

Ans. **Properties of a Digital Signature**

1. **Authentication:**
   * The digital signature proves the origin of the message. Only the sender (who possesses the private key) could have generated the signature.
   * It confirms that the message was indeed created by the entity claiming to have sent it.
2. **Integrity:**
   * The digital signature ensures that the message has not been altered during transmission. If the message is changed, the signature will no longer match, indicating tampering.
3. **Non-repudiation:**
   * The signer cannot deny the authenticity of the signature. Since the private key is kept secret and only the sender has access to it, once the signature is made, the sender cannot claim they did not sign the message.
4. **Uniqueness:**
   * A valid digital signature is unique to both the message and the signer. If either the message or the signer changes, a new digital signature must be generated.

**Requirements for a Digital Signature**

1. **Private Key for Signing:**
   * The sender must have a **private key** to create the digital signature. The private key must be kept secure and not shared with others.
2. **Public Key for Verification:**
   * The recipient must have access to the **public key** of the sender to verify the digital signature. The public key can be shared openly and is used to confirm that the signature was created by the holder of the private key.
3. **Hash Function:**
   * A **cryptographic hash function** (e.g., SHA-256) is required to generate a fixed-length hash of the message before it is signed. The hash ensures that the signature is applied to a digest of the message rather than the entire message, improving efficiency.
4. **Message Digest Integrity:**
   * The digital signature is created by applying the private key to the hash (digest) of the message. This ensures the integrity of the message, as any modification in the message will result in a different hash, invalidating the signature.
5. **Security of Key Management:**
   * The private key must be stored securely to prevent unauthorized access, and the public key must be made available to all recipients in a trustworthy manner.
6. **Randomness for Signature Creation (in some algorithms):**
   * Some digital signature algorithms (like DSA) require the generation of a **random number** k*k* during the signing process. The randomness of k*k* is essential for the security of the signature.
7. **Revocation Mechanism (Optional):**
   * In case the private key is compromised, there must be a way to revoke the corresponding public key. This is typically managed through **certificate revocation lists (CRLs)** or online status protocols.

**Security Requirements**

1. **Unforgeability:**
   * It should be computationally infeasible for anyone (other than the signer) to generate a valid signature for a given message. This ensures the authenticity of the signature.
2. **Collision Resistance:**
   * The hash function used in the digital signature must be collision-resistant, meaning that it is difficult to find two different messages that produce the same hash.
3. **Strong Private Key Protection:**
   * The security of the digital signature depends on the secrecy of the private key. If the private key is exposed, anyone could sign messages on behalf of the owner.
4. **Secure Transmission of Public Key:**
   * The public key used for verification must be transmitted securely, typically through digital certificates, to ensure it truly belongs to the signer.

**Performance Requirements**

1. **Efficiency:**
   * The signing process must be efficient, typically involving the hashing of the message and then signing the digest. Verification should also be fast for practical use in communication.
2. **Scalability:**
   * The digital signature algorithm should support large-scale systems, with the ability to manage and verify signatures in systems that involve many users or devices.

UNIT-4

Qus.1 What is key management? Also explain the functions of key management?

Ans. Key management is the process of managing cryptographic keys to ensure they are used securely and only by authorized users. It is a critical part of data security and encryption.

This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Key management involves:

* Creating keys
* Storing keys
* Distributing keys
* Deleting keys
* Backing up keys
* Assigning names to keys
* Marking keys as "in use" or "not yet used"
* Deactivating keys

Key management is important because it protects sensitive information from attacks like forward secrecy and lack of historical secrecy.

Key management systems can include key servers, user procedures, and protocols. A public-key infrastructure (PKI) is a type of key management system that uses digital certificates and public keys for authentication and encryption. PKIs are commonly used in World Wide Web traffic.

Organizations can use Key Management as a Service (KMaaS) to outsource key management to a third-party provider. KMaaS can reduce the burden on IT teams and offer benefits like convenience, flexibility, and scalability.

Qus.2 Difference between symmetric and asymmetric key cryptography?

Ans. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

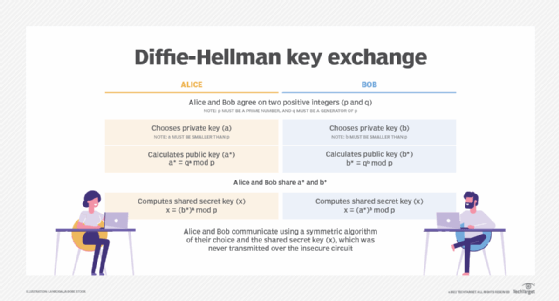
Asymmetric key encryption is one of the most common cryptographic methods that involve using a single key and its pendent, where one key is used to encrypt data and the second one is used to decrypt an encrypted text. The second key is kept highly secret, while the first one which is called a public key can be freely distributed among the service’s users.

| **Symmetric Key Encryption** | **Asymmetric Key Encryption** |
| --- | --- |
| It only requires a single key for both encryption and decryption. | It requires two keys, a public key and a private key, one to encrypt and the other to decrypt. |
| The size of ciphertext is the same or smaller than the original plaintext. | The size of ciphertext is the same or larger than the original plaintext. |
| The encryption process is very fast. | The encryption process is slow. |
| It is used when a large amount of data needs to be transferred. | It is used to transfer small amount of data. |
| It only provides confidentiality. | It provides confidentiality, authenticity, and non-repudiation. |
| The length of key used is 128 or 256 bits | The  length of key used is 2048 or higher |
| In symmetric key encryption, resource utilization is low compared to asymmetric key encryption. | In asymmetric key encryption, resource utilization is high. |
| It is efficient as it is used for handling large amount of data. | It is comparatively less efficient as it can handle a small amount of data. |
| Security is lower as only one key is used for both encryption and decryption purposes. | Security is higher as two keys are used, one for encryption and the other for decryption. |
| The Mathematical Representation is as follows- P = D (K, E(K, P))  where K –> encryption and decryption key P –> plain text D –> Decryption  E(K, P) –> Encryption of plain text using K | The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke –> encryption key  Kd –> decryption key D –> Decryption E(Ke, P) –> Encryption of plain text using encryption key Ke. P –> plain text |
| **Examples:** 3DES, AES, DES and RC4 | **Examples:**Diffie-Hellman, ECC, El Gamal, DSA and RSA |

Qus.3 Explain Diffie-Hellman key exchange.

Ans. Diffie-Hellman key exchange is a cryptographic protocol that allows two parties to securely exchange keys over a public channel to establish a shared secret key for encrypted communication.

The two parties use symmetric cryptography to encrypt and decrypt their messages.



Qus.4 Describe various schemes used for public key distribution.

Ans. Here are some schemes for distributing public keys:

* **Public-key authority**

A central authority maintains a directory of public keys for all participants. The authority knows the private keys for the public keys in the directory, but the participants know the public keys for the authority.

* **Public-key certificates**

Participants can use certificates to exchange keys without contacting a public-key authority. A certificate includes a public key, an identifier for the key owner, and a signature from a trusted third party.

* **Publicly available directory**

A trusted entity or organization maintains a dynamic directory of public keys. Participants register their public keys with the directory authority, and can replace their public key at any time.

* **Hybrid scheme**

A key distribution center (KDC) shares a secret master key with each user. The KDC distributes secret session keys encrypted with the master key, which are distributed using a public key scheme.

Qus.5 Discuss X.509 digital certificate format. What is its significance in cryptography?

Ans. In cryptography, the X.509 certificate securely associates cryptographic key pairs of public and private keys with websites, individuals or organizations. The certificate is typically used to manage identity and security in computer networking and over the internet. For the internet, it is used in numerous protocols to ensure a malicious website doesn't fool a web browser. The X.509 certificate is also used to secure email, device communications and digital signatures.

Standard information in an X.509 certificate includes the following:

* **Version.** Which X.509 version applies to the certificate, indicating what data the certificate must include.
* **Serial number.** The CA creating the certificate must assign it a serial number that distinguishes the CA certificate from other certificates.
* **Algorithm information.** The signature algorithm the issuer uses to sign the certificate.
* **Issuer distinguished name.** The name of the entity issuing the certificate -- usually, the CA.
* **Validity period of the certificate.** The start and end date, as well as the time the certificate is valid and can be trusted.
* **Subject distinguished name.** The name to which the certificate is issued.
* **Subject public key information.** The public key associated with the identity.
* **Extensions (optional).** Extensions have their own unique IDs, expressed as a set of values called an *object identifier*. An extension can be rejected if it is not recognized or if the extension has information that can't be processed.

Qus.6 Discuss Public key infrastructure.

Ans. Public key infrastructure or PKI is the governing body behind issuing digital certificates. It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications.

The public key infrastructure uses a pair of keys: the public key and the private key to achieve security. The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them.

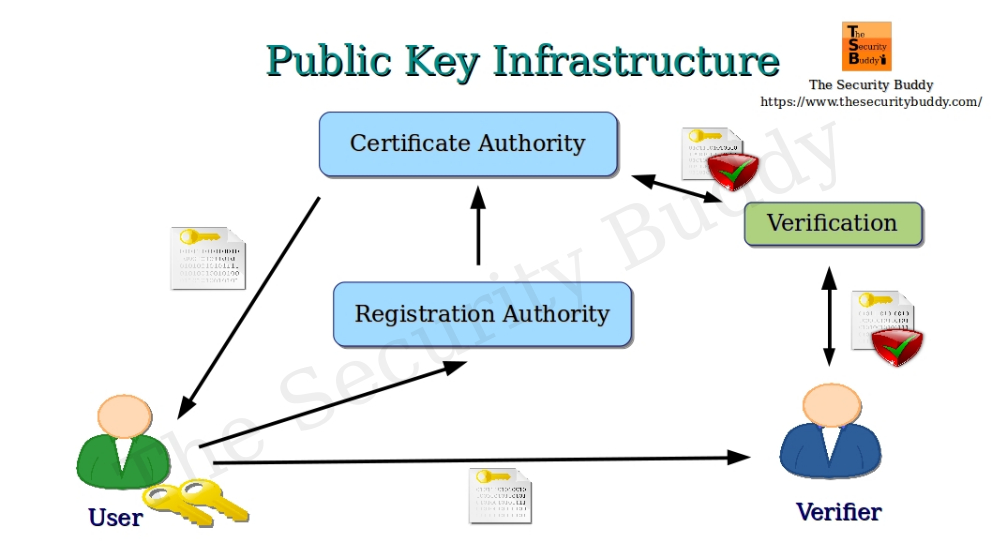
Public key infrastructure affirms the usage of a public key. PKI identifies a public key along with its purpose. It usually consists of the following components:

* A digital certificate also called a public key certificate
* Private Key tokens
* Registration authority
* Certification authority
* CMS or Certification management system

**Use of PKI in Today’s Digital Age:**

Today, there are an enormous number of applications that need require authentication. Certifications are needed at millions of places. This can not be done without a Public key infrastructure. The importance of PKI, depending on the use case and needs, has evolved over time. Here is a part of that track.

* For the very first time during the period of 1995 to 2002, the use of PKI was limited to the most important and high-value certificates. This included the certificates of eCommerce websites that enabled them to display the lock icon in the search bar. The goal was to make consumers confident about the security and authenticity of various websites.

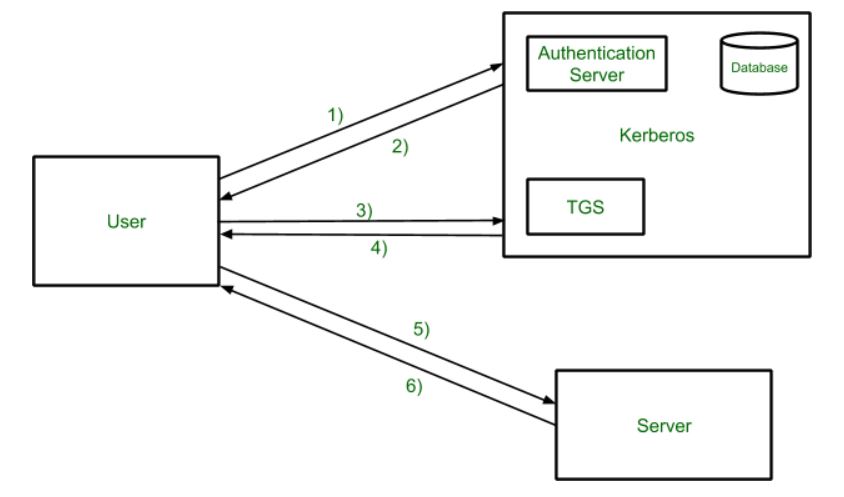


Qus.7 What is Kerberos? Discuss Kerberos version 4 in detail.  
Ans. Kerberos is a network authentication protocol that uses a trusted third party to verify the identity of clients and servers. It's used to secure communication and prevent unauthorized access to a network. Here's some more information about Kerberos, including version 4.

* **How it works**

Kerberos uses a trusted third party, called the Key Distribution Center (KDC), to issue tickets that prove the identity of clients and servers. When a user logs in, they enter the kinit command to acquire a ticket from the KDC. The ticket is valid for the session time, or eight hours by default.

The main components of Kerberos are:

* **Authentication Server (AS):**  
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
* **Database:**   
  The Authentication Server verifies the access rights of users in the database.
* **Ticket Granting Server (TGS):**   
  The Ticket Granting Server issues the ticket for the Server   
   

**Kerberos Limitations**

* Each network service must be modified individually  for use with Kerberos
* It doesn’t work well in a timeshare environment
* Secured Kerberos Server
* Requires an always-on Kerberos server
* Stores all passwords are encrypted with a single key
* Assumes workstations are secure
* May result in cascading loss of trust.
* Scalability

**Kerberos Version 4**

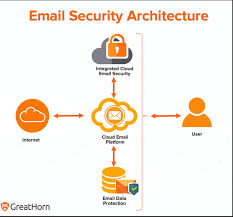
Kerberos version 4 is an update of the Kerberos software which is a computer-network authentication system. Kerberos version 4 is a web-based authentication software that is used for the authentication of users’ information while logging into the system by the DES technique for encryption. It was launched in the late 1980s.

**Features of Kerberos V4**

* **Authentication**: Kerberos V4 provides authentication and encryption services to network clients and servers.
* **Encryption**: Kerberos V4 uses a simple encryption algorithm that is less secure than the encryption used in Kerberos V5.
* **Ticket-Granting Service (TGS):** Kerberos V4 uses a single TGS for all network services, which means that the TGS has to handle a large number of requests.
* **No Support for Timestamps**: Kerberos V4 does not support timestamps, which makes it vulnerable to replay attacks.

Qus.8 What is electronic mail security? Provide the application of pretty good privacy (PGP) in transaction authentication.  
Ans. Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise. It's important because email is a critical component of organizational communication that contains sensitive information.

Email security can help protect against a variety of threats, including:

* Phishing and spoofing attacks
* Data breaches
* Malware and viruses
* Ransomware
* Social engineering
* Account takeover
* 

Qus.9 Explain S/MIME. Discuss the functionality of S/MIME.

Ans. S/MIME stands for Secure/Multipurpose Internet Mail Extensions. Through encryption, S/MIME offers protection for business emails. S/MIME comes under the concept of Cryptography. S/MIME is a protocol used for encrypting or decrypting digitally signed E-mails. This means that users can digitally sign their emails as the owner(sender) of the e-mail.

S/MIME uses public key cryptography to create certificates and encrypt messages. When an email is digitally signed with S/MIME, the sender's email client creates a hash of the message and encrypts it with their private key. The digital signature and the corresponding public key are then attached to the message when it is sent. The recipient can use the public key to verify the sender's identity and the hash to ensure that the message has not been altered.

S/MIME provides the following functions:

·  **Enveloped data:**This consists of encrypted content of any type and encrypted-contentencryption keys for one or more recipients.

·  **Signed data**: A digital signature is formed by taking the message digest of the content tobe signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.

· **Clear-signed data:**As with signed data, a digital signature of the content is formed.However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.

· **Signed and enveloped data:**Signed-only and encrypted-only entities may be nested, sothat encrypted data may be signed and signed data or clear-signed data may be encrypted.

UNIT-5

Qus.1 Explain Internet protocol security in detail. Aplication of IPS.

Ans. <https://www.geeksforgeeks.org/ip-security-ipsec/>

Internet Protocol Security (IPsec) is a network protocol suite that has many applications, including:

* **Secured data transmission**: IPsec can be used to send data securely over public connections.
* **Encrypted data applications**: IPsec can be used to create applications that encrypt data.
* **Data authentication**: IPsec can be used to quickly authenticate data.
* **Data source identification**: IPsec can be used to identify the source of data senders.
* **Network protection**: IPsec can be used to encrypt tunnels to protect networks.
* **VPN**: IPsec is one of the most widely used VPNs, providing end-to-end security features.

Qus.2 Difference between transport mode and tunnel mode.

Ans. **IPsec Tunnel Mode**

* **Full Header and Payload Encryption:** In Tunnel Mode, the complete original IP packet (header and payload) is encrypted after which it is encapsulated inside a new IP packet. This new packet has a different IP header, normally with exclusive source and destination spotted on its IP addresses.
* **Used for Site-to-Site VPNs**: Tunnel Mode is normally utilized in site-to-web page VPNs (Virtual Private Networks) in which entire networks or subnets need to talk securely over an untrusted network, including the Internet.
* **Protects Network-to-Network Communication:**Network to network Communication secures communication between all the networks, for encryption and protection from attacks.

**IPsec Transport Mode**

* **Payload encryption simplest:**In shipping mode, preferably the payload (information) of a valid IP packet is encrypted, while the valid IP header stays intact. This mode is usually used to pause communication between hosts or gadgets.
* **Used for host-to-host communication**: The host-to-host communication mode is generally used to guard communication among hosts or devices in preference to the whole network.
* **Less overhead**: Since the original IP header no longer trades, new headers may have less overhead in keeping with the sentence compared to Tunnel Mode.

Qus.3 Explain the Authentication Header (AH) protocol.

Ans. The Authentication Header (AH) protocol is a security protocol that ensures the integrity of data and packet headers, and provides user authentication. It is a component of the Internet Protocol security (IPsec) suite.

Here are some of the features of the AH protocol:

* **Data integrity**

AH uses a checksum generated by a message authentication code, like MD5, to ensure data integrity.

* **Data origin authentication**

AH uses a secret shared key in the authentication algorithm to ensure data origin authentication.

* **Replay protection**

AH uses a sequence number field in the AH header to ensure replay protection.

* **Doesn't encrypt data**

AH doesn't encrypt any part of the packets.

* **Works in both transport and tunneling mode**

AH can be inserted between the IP header and the transport header, which can be TCP, UDP, SCTP, or ICMP.

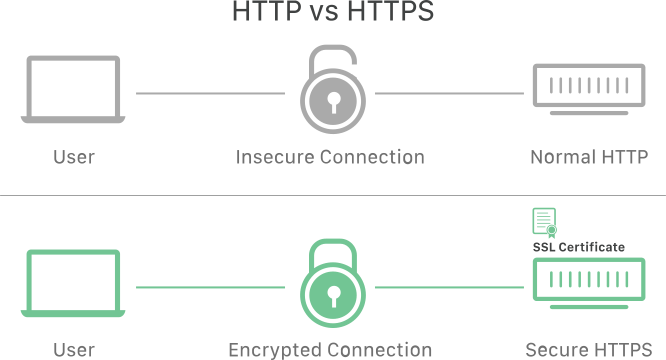
* **Protects most of the IP packet**

AH protects the majority of the IP packet, but it doesn't protect certain fields in the IP header, known as mutable fields.

Qus.4 Explain SSL with its architecture.

Ans. SSL, or Secure Sockets Layer, is an [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/)-based Internet security [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/). It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern [TLS](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/) encryption used today.

A website that implements SSL/TLS has "[HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/)" in its URL instead of "[HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/)."

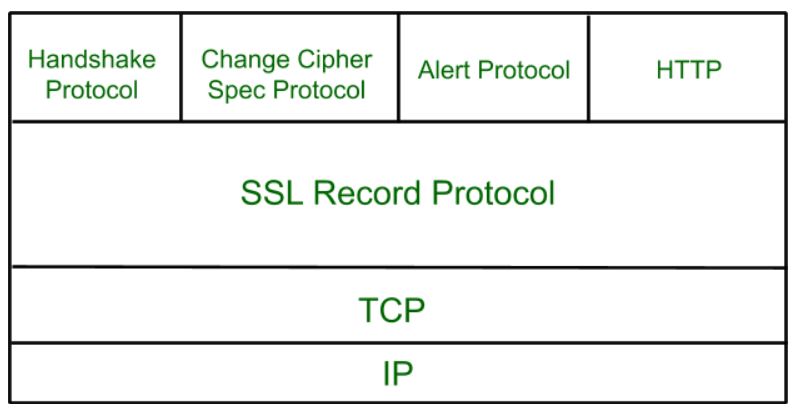


**How does SSL/TLS work?**

* In order to provide a high degree of [privacy](https://www.cloudflare.com/learning/privacy/what-is-data-privacy/), SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
* SSL initiates an **authentication** process called a [handshake](https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/) between two communicating devices to ensure that both devices are really who they claim to be.
* SSL also digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

**Secure Socket Layer Protocols**

* SSL Record Protocol
* Handshake Protocol
* Change-Cipher Spec Protocol
* Alert Protocol



**SSL Record Protocol**

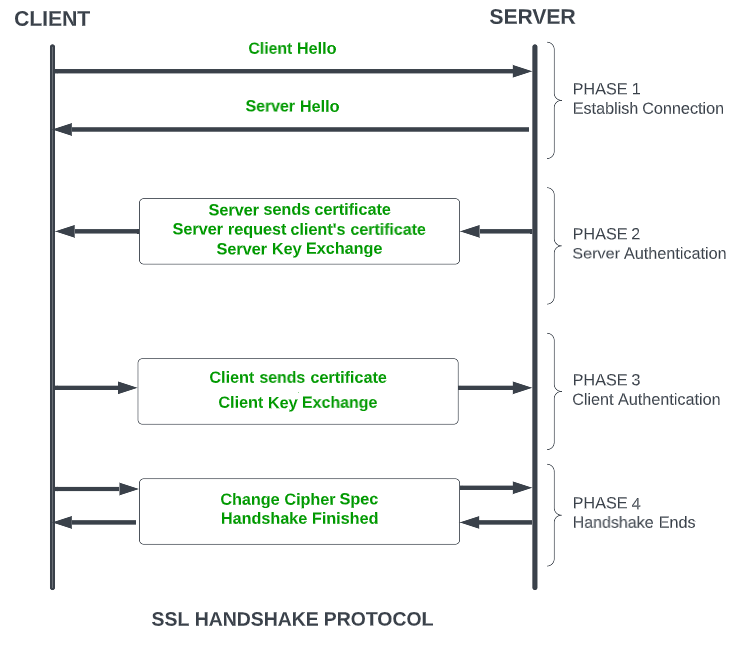
SSL Record provides two services to SSL connection.

* Confidentiality
* Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA ([Secure Hash Protocol](https://www.geeksforgeeks.org/sha-1-hash-in-java/)) and MD5 ([Message Digest](https://www.geeksforgeeks.org/what-is-the-md5-algorithm/)) is appended.

**Handshake Protocol**

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.



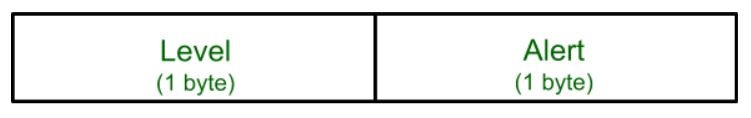
**Change-Cipher Protocol**

This protocol uses the SSL record protocol. Unless [Handshake](https://www.geeksforgeeks.org/tcp-3-way-handshake-process/)Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state.   
Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol’s purpose is to cause the pending state to be copied into the current state.



**Alert Protocol**

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



Qus.5 Discuss Secure Electronic Transaction(SET). Who are the participants in SET?

Ans. <https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/>

Qus.6 What do you mean by system security? Also discuss viruses and related threats to system security?

Ans. System security is the practice of protecting an organization's information systems and resources from unauthorized access, modification, or destruction. It also includes preventing cyber threats and downtime.

System security is closely related to data security, which is the protection of information from being accidentally or intentionally deleted, modified, or misused.

Computer viruses and other types of malware are a serious threat to system security. Malware is a general term for malicious software that can damage, disrupt, or gain unauthorized access to a computer system. Some types of malware include:

* **Viruses**

A malicious code that copies itself to other programs, systems, or host files. Viruses remain dormant until activated, then spread the infection without the user's knowledge.

* **Worms**

A self-replicating program that infects other computers without requiring human interaction. Worms can spread quickly using automatic parts of an operating system.

* **Spyware**

A type of malware that can monitor a user's online and offline activities, including web browsing and online shopping. Hackers can use spyware to view passwords and bank account information.

* **Keyloggers and infostealers**

Malware that collects and exfiltrates sensitive information from an infected computer.

* **Adware and cryptojackers**

Malware that uses infected machines to earn money for the attacker.

Qus.7 Write a short note on Firewall. Types of firewall? Limitations of firewalls.

Ans. A firewall is a network security device that monitors and controls incoming and outgoing network traffic.

A firewall's main purpose is to protect a network from unauthorized access, harmful activities, and potential threats. It does this by acting as a barrier between a trusted internal network and an untrusted external network, such as the internet.

Firewalls inspect data packets and decide whether to allow or block them based on a set of rules. These rules can be configured to permit or deny traffic based on various criteria, such as source and destination IP addresses, port numbers, and protocol type.

There are several types of firewalls, including:

* **Packet filtering firewall**

Analyzes and filters data packets based on parameters like IP addresses, ports, and protocols. While simple and cost-effective, they can't examine packet contents.

* **Stateful inspection firewall**

Also known as dynamic packet filtering firewalls, these firewalls track active sessions and determine if packets are part of an established connection.

* **Proxy firewall**

Acts as an intermediary between users and the services they want to access.

* **Web application firewall (WAF)**

Protects web applications by filtering and monitoring HTTP traffic between the web application and the internet.

* **Unified threat management (UTM) firewall**

Combines multiple security functions into a single device or service, including intrusion prevention, antivirus software, VPN support, and content filtering.

* **Next-generation firewall (NGFW)**

A network security device that provides capabilities beyond a traditional, stateful firewall.

* **Cloud-native firewall**

A security solution designed for cloud environments that protects cloud applications and workloads.

**Firewalls are a necessary part of cybersecurity, but they have some limitations**, including:

* **Reactive**: Firewalls are designed to counter known threats, which can leave gaps against more sophisticated cyber threats.
* **Cybercriminals are adaptable**: Cybercriminals can find loopholes in firewall defenses, exploit configuration errors, or use encrypted traffic to hide malicious activities.
* **Social engineering attacks**: Firewalls can't prevent the revealing of sensitive information through social engineering attacks, such as phishing.
* **Firewalls can't stop attacks if traffic doesn't pass through them**: Firewalls can't stop attacks if the traffic doesn't pass through them.
* **Firewalls can't protect against what has been authorized**: Firewalls permit normal communications of approved applications, but if those applications themselves have flaws, a firewall will not stop the attack.
* **Users can bypass the firewall**: Firewalls cannot prevent users or attackers from dialing in to or out of the internal network.
* **Password policy**: Firewalls cannot enforce password policies or prevent misuse of passwords.
* **Malicious code**: Firewalls cannot stop internal users from accessing websites with malicious code.
* **Internal threats**: Firewalls cannot defend a network from internal threats such as backdoors.
* **Compatibility issues**: Switching vendors can create compatibility issues.

Qus.8 Difference between SSL and SET.

Ans.

| **SSL** | **SET** |
| --- | --- |
| SSL secures communication between browsers and servers. Merchants manage both order and payment details. | SET secures credit card payments and hides customer payment details from merchants. |
| It developed by Netscape for secure online transactions. | It developed by MasterCard and Visa for safe card payments. |
| Developed by MasterCard and Visa for safe card payments. | Requires verification by both CAs and financial institutions. |
| It can secure emails, websites, and other applications. | It has limited to online financial transactions only. |
| Merchants can view the cardholder’s payment information. | Card details are hidden from merchants, ensuring privacy. |
| It is easy to implement and suitable for small businesses. | It is harder to implement and more expensive to set up. |
| Harder to implement and more expensive to set up. | Stronger encryption of 1024-bit for financial security. |