00 INDEX

Vulnerability is a weakness in the security system that might be exploited to cause loss or harm. For ex, weakness in procedures, design or implementation.
Threat to a computing system is a set of circumstances that has potential to cause loss or harm. There are many threats to a computer system, including human-initiated and computer-initiated ones. A threat is blocked by control of a vulnerability. **Types of Threats:** **1) Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files. **2)Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or disabling of file management system.**3) Modification:** An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network. **4) Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.
Attacks: When a vulnerability is exploited, attack happens on the system. Any action that compromises the security of information owned by an organization.

Types of attacks on data security. Active attack attempts to alter system resources or affect their operations. Active attacks involve an attacker intentionally altering or destroying data, or disrupting the normal operation of a system. Examples of active attacks include denial of service (DoS), where an attacker floods a system with traffic in an attempt to make it unavailable to legitimate users, and malware, where an attacker installs malicious software on a system to steal or destroy data.**Types: 1)Masquerade** attack takes place when one entity pretends to be a different entity. this attack involves one of the other forms of active attacks. If an authorization procedure isn't always protected, it is able to grow to be extraordinarily liable to a masquerade assault.
2) Modification of messages: It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data.
3) Repudiation: This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author's information can be changed by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages.
4)Replay: It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.**5) Denial of Service:** It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination.
Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information. **Types of Passive attacks**: **The release of message content:** Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions**. Traffic analysis**: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Relation between security services and mechanisms: Security mechanisms are technical tools and techniques that are used to implement security services. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack.

Security Services: Confidentiality: This security service ensures that information is kept private and only accessible to authorized parties. Confidentiality can be achieved through encryption, access controls, and secure communication protocols. The main attack against confidentiality is eavesdropping or interception of data. **Integrity:** This security service ensures that information is not modified or tampered with during transmission or storage. Integrity can be achieved through data hashing, digital signatures, and access controls. The main attack against integrity is data modification or alteration. **Availability:** This security service ensures that information and systems are accessible to authorized parties when needed. Availability can be achieved through redundancy, backup systems, and fault-tolerant hardware. The main attack against availability is denial of service (DoS) attacks that overload the system with traffic. **Authentication:** This security service ensures that the identity of users and systems is verified before access is granted. Authentication can be achieved through passwords, smart cards, and biometric identification. The main attack against authentication is identity theft or impersonation. **Authorization:** This security service ensures that users have the necessary permissions to access information and resources. Authorization can be achieved through access controls, role-based access controls, and security policies. The main attack against authorization is unauthorized access or privilege escalation. **Non-repudiation:** This security service ensures that a user cannot deny their actions or transactions. Non-repudiation can be achieved through digital signatures, time-stamping, and audit trails. The main attack against non-repudiation is denial of service or tampering with audit logs.

Security Mechanisms A mechanism that is designed to detect, prevent or recover from a security attack. One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. **Mech: 1) Encipherment:** Encipherment is hiding or covering data and can provide confidentiality. It makes use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.Cryptography and Steganography techniques are used for enciphering. **2) Data integrity:** The data integrity mechanism appends a short check value to the data which is created by a specific process from the data itself. The receiver receives the data and the check value. The receiver then creates a new check value from the received data and compares the newly created check value with the one received. If the two check values match, the integrity of data is being preserved. **3) Digital Signature:** A digital signature is a way by which the sender can electronically sign the data and the receiver can electronically verify it. The sender uses a process in which the sender owns a private key related to the public key that he or she has announced publicly. The receiver uses the sender's public key to prove the message is indeed signed by the sender who claims to have sent the message.
4) Authentication exchange: A mechanism intended to ensure the identity of an entity by means of information exchange. The two entities exchange some messages to prove their identity to each other. For example the three-way handshake in TCP. Traffic padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts**. 5) Routing** control: Enables selection of particular physically secure routes for certain data and allows routing changes which means selecting and continuously changing different available routes between the sender and the receiver to prevent the attacker from traffic analysis on a particular route. **6) Notarization:** The use of a trusted third party to control the communication between the two parties. It prevents repudiation. The receiver involves a trusted third party to store the request to prevent the sender from later denying that he or she has made such a request. **7) Access Control:** A variety of mechanisms are used to enforce access rights to resources data owned by a system, eg. PINS and passwords.

Security Goals: are specific objectives that aim to protect sensitive information, systems, and assets from unauthorized access, disclosure, modification, destruction, or disruption.
1.**Confidentiality:** is the security goal that ensures that sensitive data or information is only accessible by authorized individuals or systems. **ii.**Confidentiality is essential in protecting private, personal, and sensitive data, such as financial information, medical records, or trade secrets.**iii.**Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.**iv.**Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
2.Integrity: is the security goal that ensures that data or information is accurate, reliable, and trustworthy.**ii**.Integrity means making sure that the data or information you have is correct and can be trusted. To do this, you need to make sure that nobody changes the information without permission, and if any changes are made, they are recorded properly**. iii.** Data integrity means that information and programs can only be changed in an authorized way, to ensure that they are accurate and trustworthy**.iv.** System integrity: means that a computer system can perform its intended functions without unauthorized changes or manipulations, intentional or unintentional, which could cause it to malfunction.
3.Availability: i. It is the security goal that ensures that systems, applications, and data are accessible to authorized users whenever they need them.**ii**.Availability ensures that systems and applications are functioning correctly and that users can access them without delay or interruption.

Disadvantages of Substitution ciphers: easy to break using frequency analysis.It is not secure enough for modern encryption needs.The key is easy to discover, since there are only 25 possible keys in the Caesar Cipher.
Disadvantages of Transposition Cipher: The encryption process is easy to understand, and once the pattern is recognized, the cipher is relatively easy to break. The length of the plaintext determines the number of rows, which means the pattern is predictable. The key can be discovered by finding the pattern in the ciphertext.

Stream Ciphers vs Block ciphers**: 1) Processing or encoding of PT is done bit by bit. The block size here is simply one bit.** Processing or encoding of PT is done as a fixed length block one by one. The block could be 64 or 128 bits in size. **2) A different key bit can be used to encrypt each of bits.** The same key is used to encrypt each of the blocks. **3) Uses both symmetric and asymmetric encryption.** Uses symmetric encryption and is not used in asymmetric encryption **4) Low Diffusion : each symbol is separately enciphered therefore all information of that symbol is contained in one symbol of CT.** High Diffusion: Information from PT is diffused into several CT symbols. One CT blocks may depend on several PT letters **5) Sensible to malicious insertion & modification: Bcoz each symbol is separately enciphered, an active interceptor who has broken code can splice together pieces of previous messages and transmit a new message that may look authentic.** Immunity for insertion of symbols and modification is high : Bcoz blocks of symbols are enciphered, it is impossible to insert a single symbol into a block. Then the length of block would then be incorrect and reveal the insertion. **6) Error Propagation: Bcoz each symbol is separately encoded, an error in encryption process affects only that character.** Error Propagation: An error will affect the transformation of all other characters in the same block. **7) Examples of stream cipher: RC4, A5/1, SEAL, SNOW, ISAAC etc.** Examples of block cipher : DES, AES, IDEA, RC5, Blowfish

Symmetric Encryption: 1) This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.**2)** It uses a secret key that can either be a number, a word or a string of random letters. **3)** The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. **4)** Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.**5)** Disadvantage of the symmetric key encryption is that all parties involved must exchange the key used to encrypt the data before they can decrypt it.
Asymmetric Encryption:1) Asymmetric encryption uses two keys to encrypt a plain text. **2)**Secret keys are exchanged over the Internet or a large network. **3)** It ensures that malicious persons do not misuse the keys.**4)** It is important to note that anyone with a secret key can decrypt the message and this is why asymmetric encryption uses two related keys to boosting security.**5)** A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

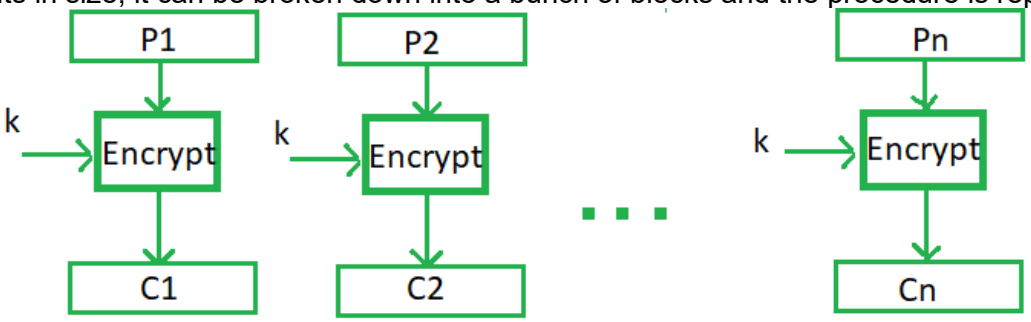
Cryptographic Techniques: Symmetric-key cryptography: This technique uses the same key for both encryption and decryption. Examples include DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Blowfish.
Asymmetric-key cryptography: This technique uses different keys for encryption and decryption. Examples include RSA, DSA, and Elliptic Curve Cryptography.
Hash functions: These are one-way functions that take input data and generate a fixed-length string of bits that represents the data. Examples include MD5, SHA-1 & SHA-256.
Digital signatures: These are used to provide authentication and integrity of digital documents. Examples include RSA and DSA. **Public key infrastructure (PKI):** This is a set of protocols and procedures for managing public key encryption. It includes the creation, distribution, and revocation of digital certificates. Examples: X.509 and PGP.
Quantum cryptography: This is a new and emerging technology that uses the principles of quantum mechanics to create cryptographic systems that are resistant to attack. Examples include quantum key distribution (QKD) and quantum coin flipping. **Steganography:** This technique involves hiding a message within another message or file. It can be used to hide the fact that a message is being sent at all.
Homomorphic encryption: This is a technique that allows computation to be performed on encrypted data without decrypting it first. It can be used to perform secure computations on sensitive data without revealing the data itself.
Obfuscation: This technique involves making code or data difficult to understand or reverse-engineer. It can be used to protect intellectual property or to prevent reverse engineering of software.

Attacks on encrypted messages. 1.Ciphertext Only Attack: An attacker has access to only the encrypted ciphertext and attempts to decipher it without any knowledge of the plaintext or the encryption key. Encryption algorithm to alter the data. **2.Known Plaintext Attack:A**n attacker has access to both the plaintext and the corresponding encrypted ciphertext.By analyzing the known pairs, the attacker attempts to deduce the encryption key. **3.Chosen Plaintext Attack:** An attacker can choose the plaintext message and see its corresponding encrypted ciphertext. By analyzing the encrypted messages, the attacker attempts to deduce the encryption key. **4.Chosen Ciphertext Attack:** An attacker can choose the encrypted ciphertext and see its corresponding decrypted plaintext. By analyzing the known pairs, the attacker attempts to deduce the encryption key.**5. Chosen text:** Algorithm processed for the encryption of data. Cipher text together with subsequent plain text and key chosen by the cryptanalysts.

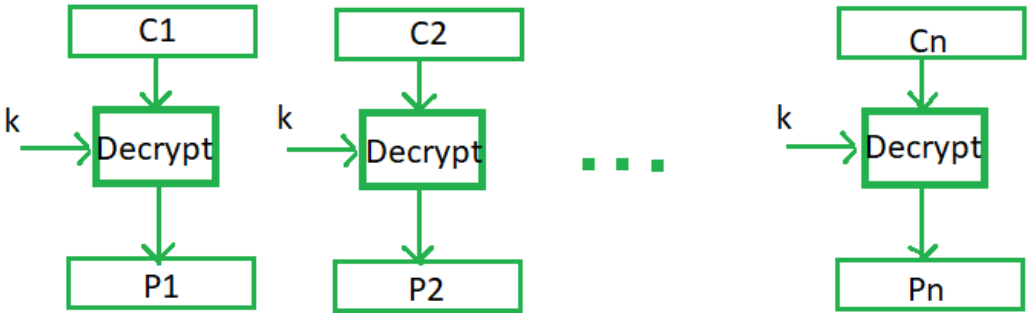
Diff b/w Advanced Encryption Standard (AES) & Data Encryption Standard (DES):
1) Byte-Oriented. Bit-Oriented. **2) Key length can be 128-bits, 192-bits, and 256-bits.** The key length is 56 bits in DES. **3) No. of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits).** DES involves 16 rounds of identical operations. **4) The structure is based on a substitution-permutation network.** The structure is based on a Feistel network. **5) 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. **6) AES can encrypt 128 bits of plaintext. It can generate Ciphertext of 128, 192, 256 bits.** DES can encrypt 64 bits of plaintext. It generates Ciphertext of 64 bits. **7) 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.

Triple DES: 1.3DES is based on the original Data Encryption Standard (DES) algorithm, which uses a 56-bit key. **2.** 3DES is much more secure than DES because it uses three keys (each 56 bits in length) and encrypts the data three times. **3.**There are two modes of operation for 3DES: **a.EDE (Encrypt-Decrypt-Encrypt), where** the data is encrypted with one key, decrypted with another, and encrypted again with a third key. **b.CBC (Cipher Block Chaining),** where each block of data is encrypted using the previous block's cipher text as part of the encryption process**. 4.**3DES can be used for both symmetric key encryption (where the same key is used for encryption and decryption) and hybrid encryption (where a public key algorithm is used to securely exchange a symmetric key, which is then used for encryption**). 5.**While 3DES is still considered a secure encryption algorithm, it is slowly being phased out in favor of more modern algorithms such as AES (Advanced Encryption Standard). **6.**3DES is widely used in applications such as financial transactions, VPNs (Virtual Private Networks), and secure email communications.

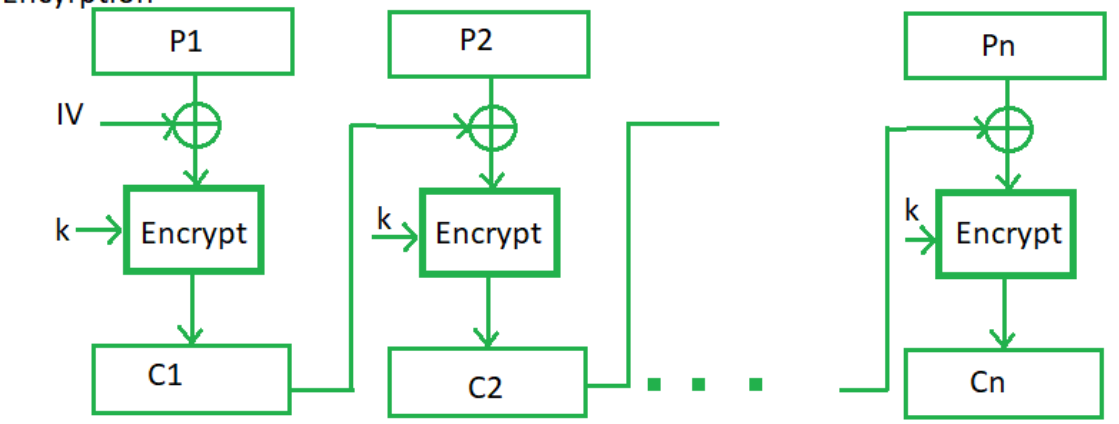
Block cipher modes of operation. 1) Electronic Code Book (ECB): ECB is the easiest block cipher mode of functioning because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext. Generally, if a message is larger than b bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.



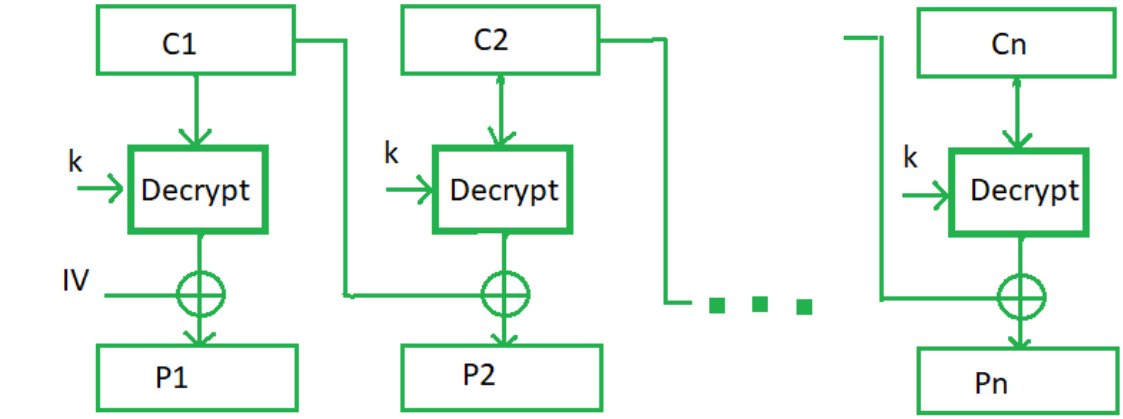
Decryption



2) Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block. In a nutshell here, a cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block.

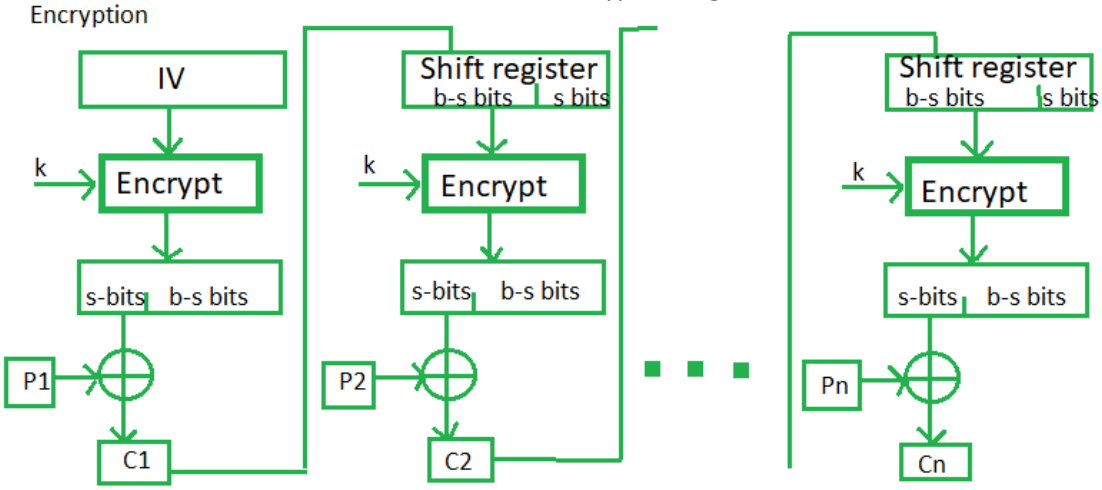


Decryption

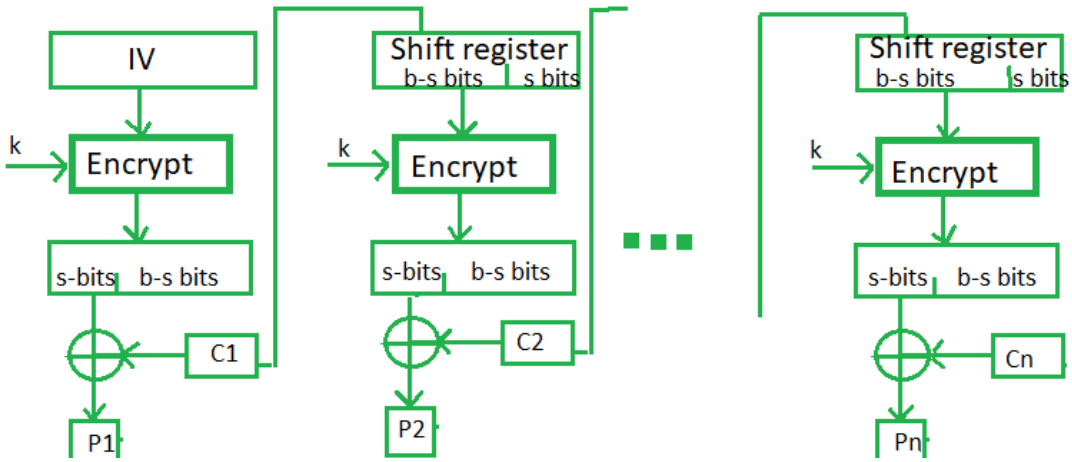


3) Cipher Feedback Mode (CFB): In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of s and b-s bits.The left-hand side s bits are selected along with plaintext bits to which an XOR operation is applied. The result is given as input to a shift register having b-s bits to lhs,s bits to rhs and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithms.

Encryption

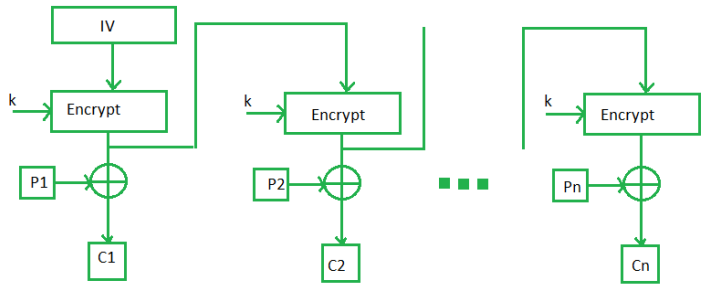


Decryption

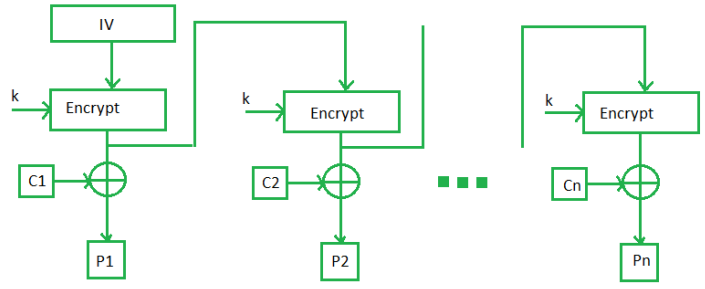


4) Output Feedback Mode: The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected s bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.

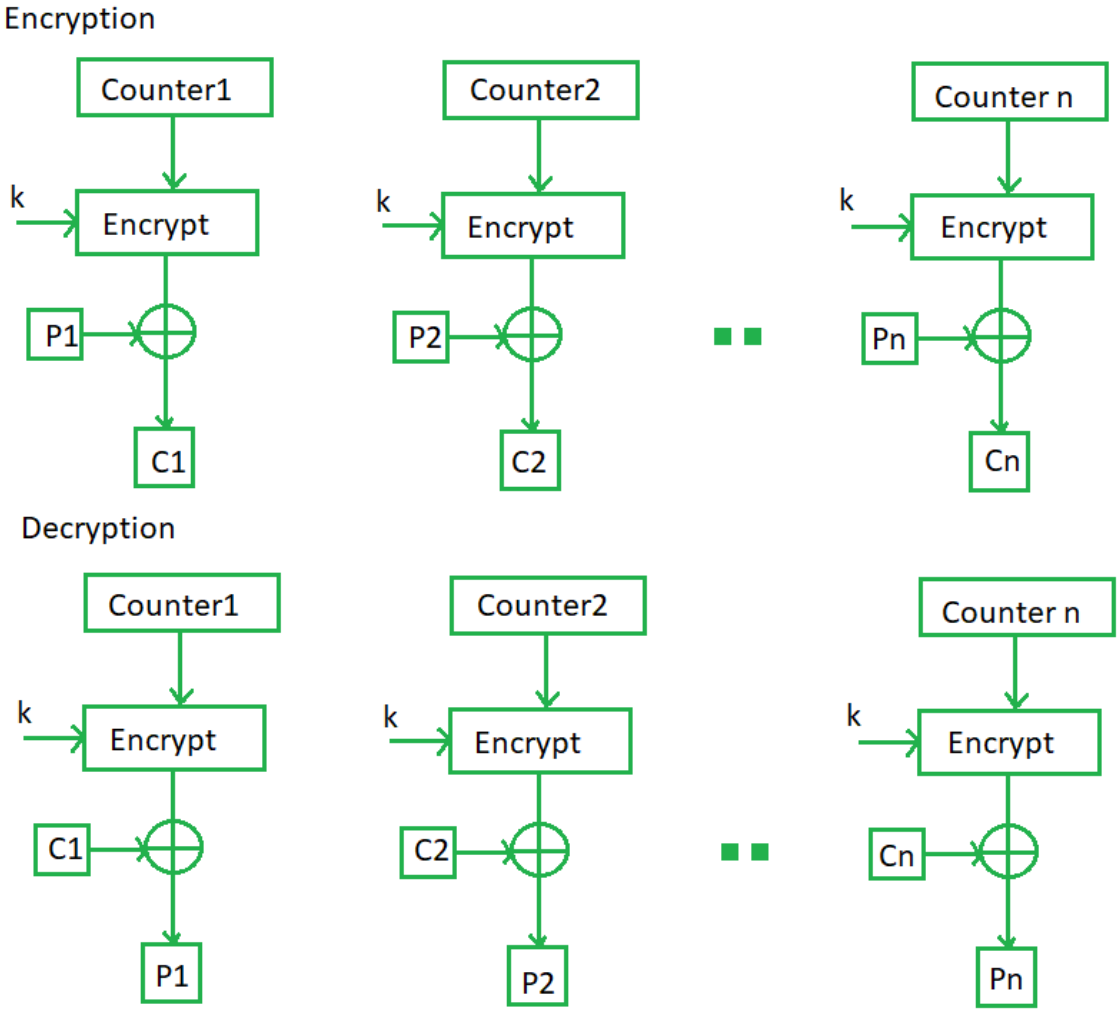
Encryption



Decryption



5) Counter Mode: The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.



Applications of Block Ciphers

Data Encryption: Block Ciphers are widely used for the encryption of private and sensitive data such as passwords, credit card details and other information that is transmitted or stored for a communication. This encryption process converts a plain data into non-readable and complex form. Encrypted data can be decrypted only by the authorised person with the private keys.

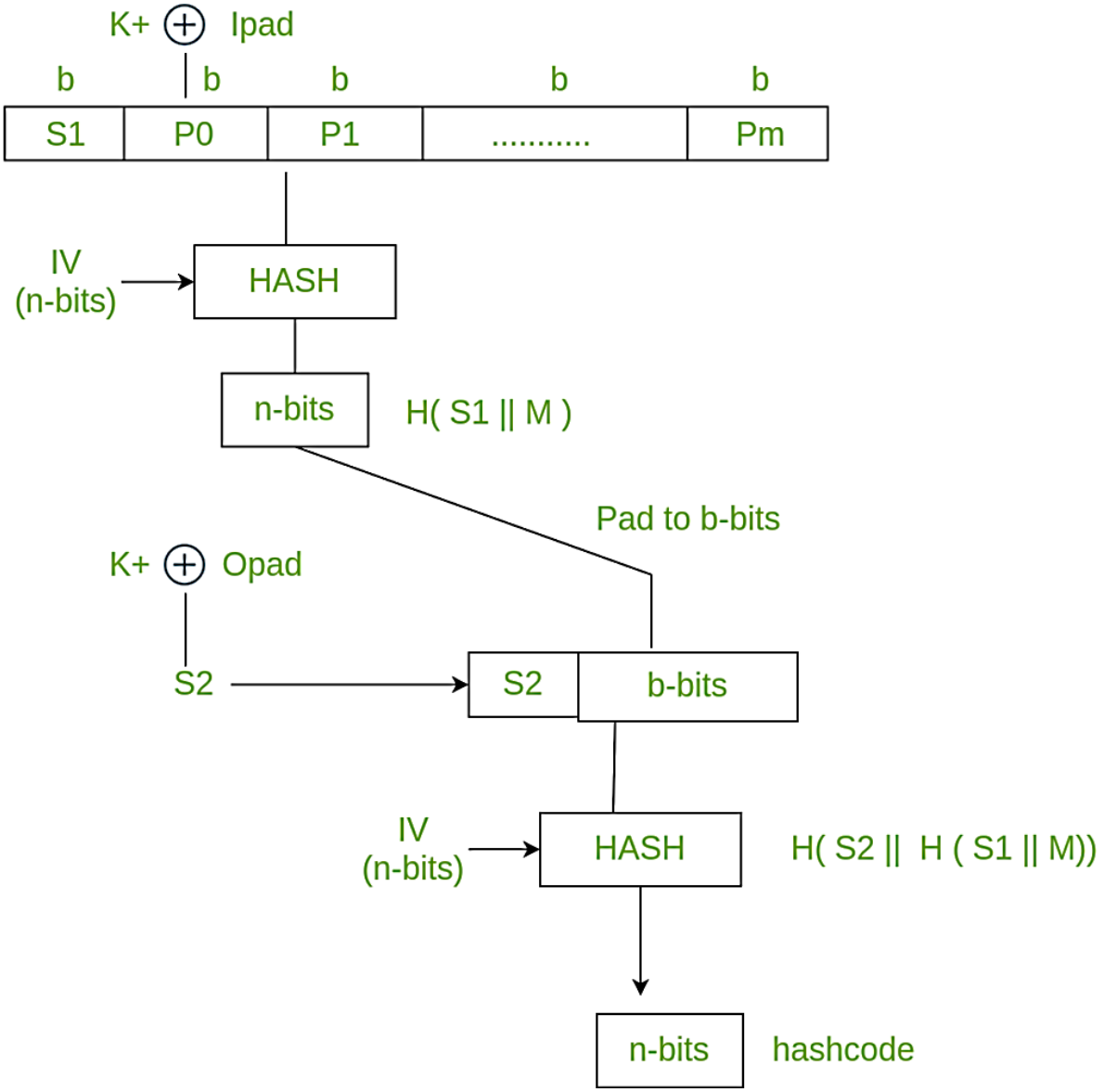
File and Disk Encryption: Block Ciphers are used for encryption of entire files and disks in order to protect their contents and restrict from unauthorised users. The disk encryption softwares such as BitLocker, TrueCrypt aslo uses block cipher to encrypt data and make it secure.

Virtual Private Networks (VPN): Virtual Private Networks (VPN) use block cipher for the encryption of data that is being transmitted between the two communicating devices over the internet. This process makes sure that data is not accessed by unauthorised person when it is being transmitted to another user.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS): SSL and TLS protocols use block ciphers for encryption of data that is transmitted between web browsers and servers over the internet. This encryption process provides security to confidential data such as login credentials, card information etc.

Digital Signatures: Block ciphers are used in the digital signature algorithms, to provide authenticity and integrity to the digital documents. This encryption process generates the unique signature for each document that is used for verifying the authenticity and detecting if any malicious activity is detected.

HMAC

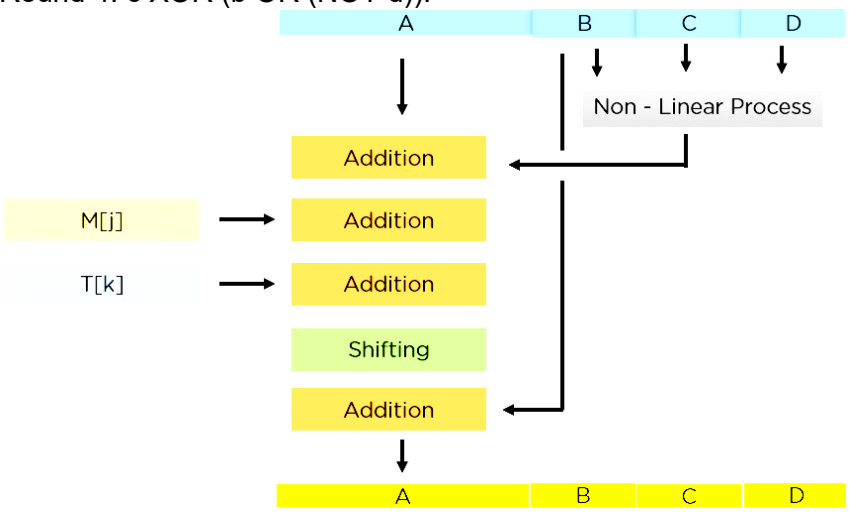


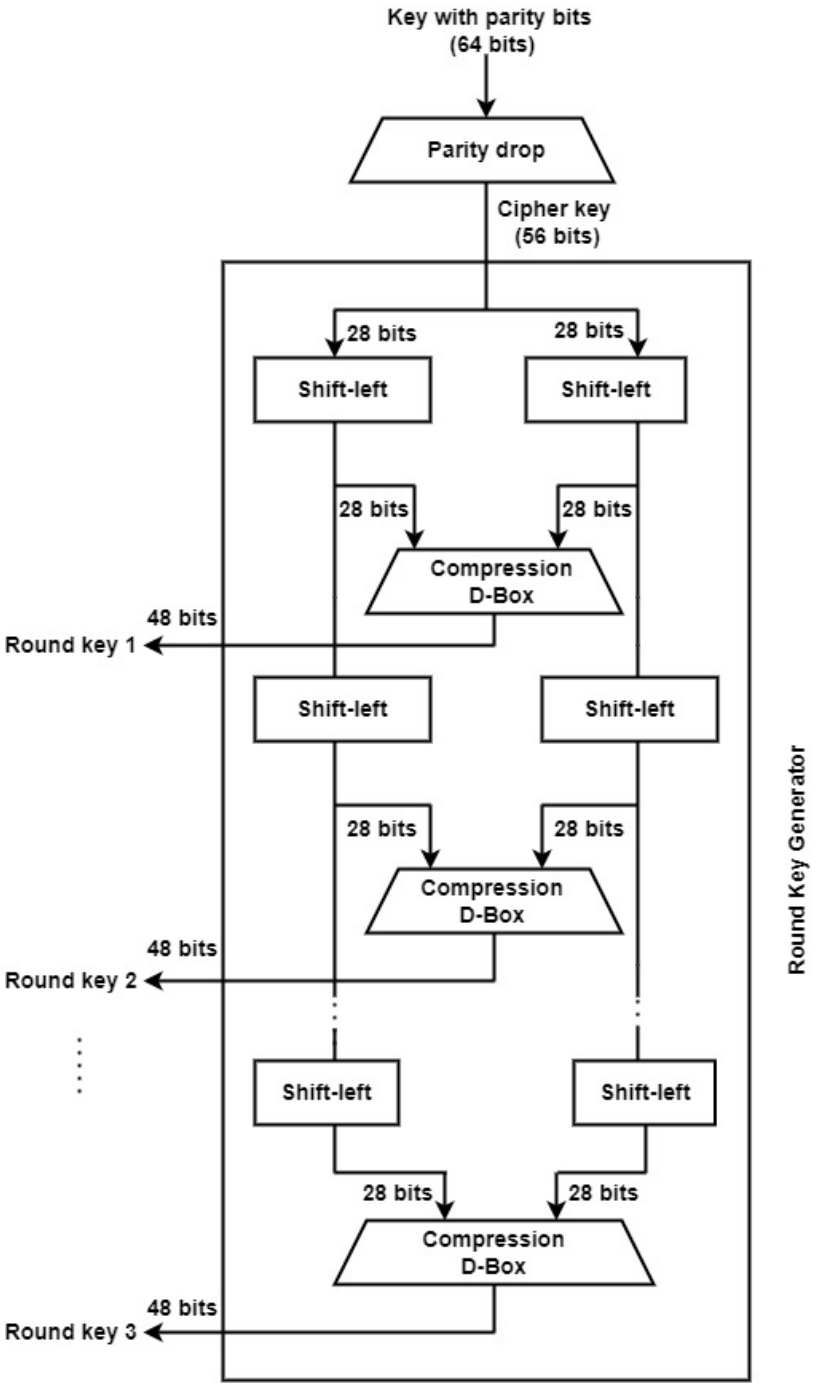
The Hash-based Message Authentication Code (HMAC) algorithm is a widely-used cryptographic algorithm that provides message authentication and integrity. Its primary objectives are:
Message Integrity: The HMAC algorithm ensures that the message has not been tampered with during transmission, by checking the integrity of the message using a cryptographic hash function.
Message Authentication: The HMAC algorithm provides authentication by verifying the sender's identity and confirming that the message has not been modified.

The HMAC algorithm works by using a cryptographic hash function (e.g., SHA-256) in combination with a secret key. Steps:
-The sender generates a secret key known only to the sender and recipient.
-The sender calculates the HMAC by applying the secret key to a cryptographic hash function along with the message being sent.
-The recipient receives the message and calculates the HMAC using the same cryptographic hash function and the shared secret key.
-The recipient compares the calculated HMAC with the HMAC received with the message. If they match, the message is authenticated and has not been modified during transmission.
-The HMAC algorithm is commonly used in various applications, including network security protocols (e.g., SSL/TLS), software authentication, and message authentication in distributed systems. Its use of a shared secret key makes it a secure way to authenticate messages and verify the integrity of the data transmitted between two parties

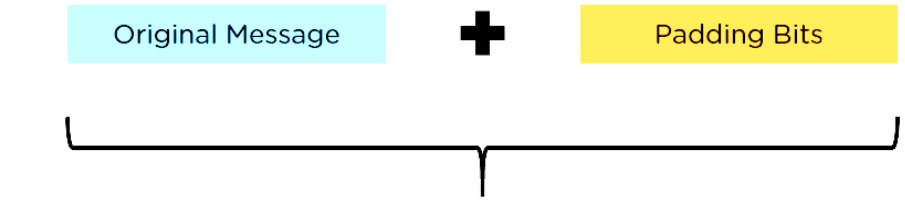
MD5: is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. **Key generation: Data Encryption Standard (DES)** is a block cipher algorithm that creates plain text in blocks of 64 bits and transform them to ciphertext using keys of 48 bits. It is a symmetric key algorithm, which defines that the similar key is used for encrypting and decrypting info. DES takes a 64-bit plaintext and produce a 64-bit ciphertext; at the decryption site, DES takes a 64-bit ciphertext and produce a 64-bit block of plaintext. The same 56-bit cipher key can be used for encryption and decryption.
The algorithm implement 16 rounds of encryption and for each round, a unique key is produced. Before transforming to the steps, it is essential to understand that in plaintext the bits are labeled from 1 to 64 where 1 is the most significant bit & 64 is least significant bit.
1)The round key generator produce sixteen 48-bit keys out of a 56-bit cipher key. The cipher key is provided as 64 bit key in which 8 extra bits are parity bits, which are discarded before the actual key generation process begins.
2)The parity bit drop process drops the parity bits (bit 8, 16, 24, 32…64) from the 64-bit key and permutes the remaining bit according to the pre-defined rules as display in the parity bit drop table below.
3)These remaining 56 bits are generally used for key generation.
4)After the permutation, the keys are divided into two 28 bits parts. Each part is changed left one or two bits is depend on the rounds.
5)In round 1, 2, 9, and 16 shifting is one bit and in the other rounds it is two bits. The two parts are integrate to build a 56 bit part.
6)Thus the compression D-box transform it into 48 bit. These 48 bits are being utilized as a key for a round.

Padding Bits: When you receive the input string, you have to make sure the size is 64 bits short of a multiple of 512. When it comes to padding the bits, you must add one(1) first, followed by zeroes to round out the extra characters.
Padding Length: You need to add a few more characters to make your final string a multiple of 512. To do so, take the length of the initial input and express it in the form of 64 bits. On combining the two, the final string is ready to be hashed.
Initialize MD Buffer: The entire string is converted into multiple blocks of 512 bits each. You also need to initialize four different buffers, namely A, B, C, and D. These buffers are 32 bits each and are initialized as follows: A = 01 23 45 67; B = 89 ab cd ef;
C = fe dc ba 98; D = 76 54 32 10.
Process Each Block: Each 512-bit block gets broken down further into 16 sub-blocks of 32 bits each. There are four rounds of operations, with each round utilizing all the sub-blocks, the buffers, and a constant array value. This constant array can be denoted as T[1] -> T[64]. Each of the sub-blocks are denoted as M[0] -> M[15]. It passes B, C, and D onto a non-linear process. The result is added with the value present at A. It adds the sub-block value to the result above. Then, it adds the constant value for that particular iteration. There is a circular shift applied to the string. As a final step, it adds the value of B to the string and is stored in buffer A. The steps mentioned above are run for every buffer and every sub-block. When the last block's final buffer is complete, you will receive the MD5 digest. The non-linear process above is different for each round of the sub-block. Round 1: (b AND c) OR ((NOT b) AND (d)); Round 2: (b AND d) OR (c AND (NOT d)); Round 3: b XOR c XOR d; Round 4: c XOR (b OR (NOT d)).

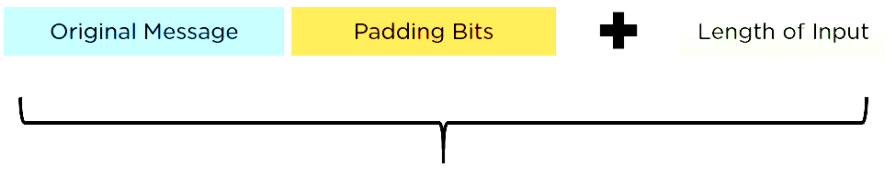




Block diagram of shift key Generation

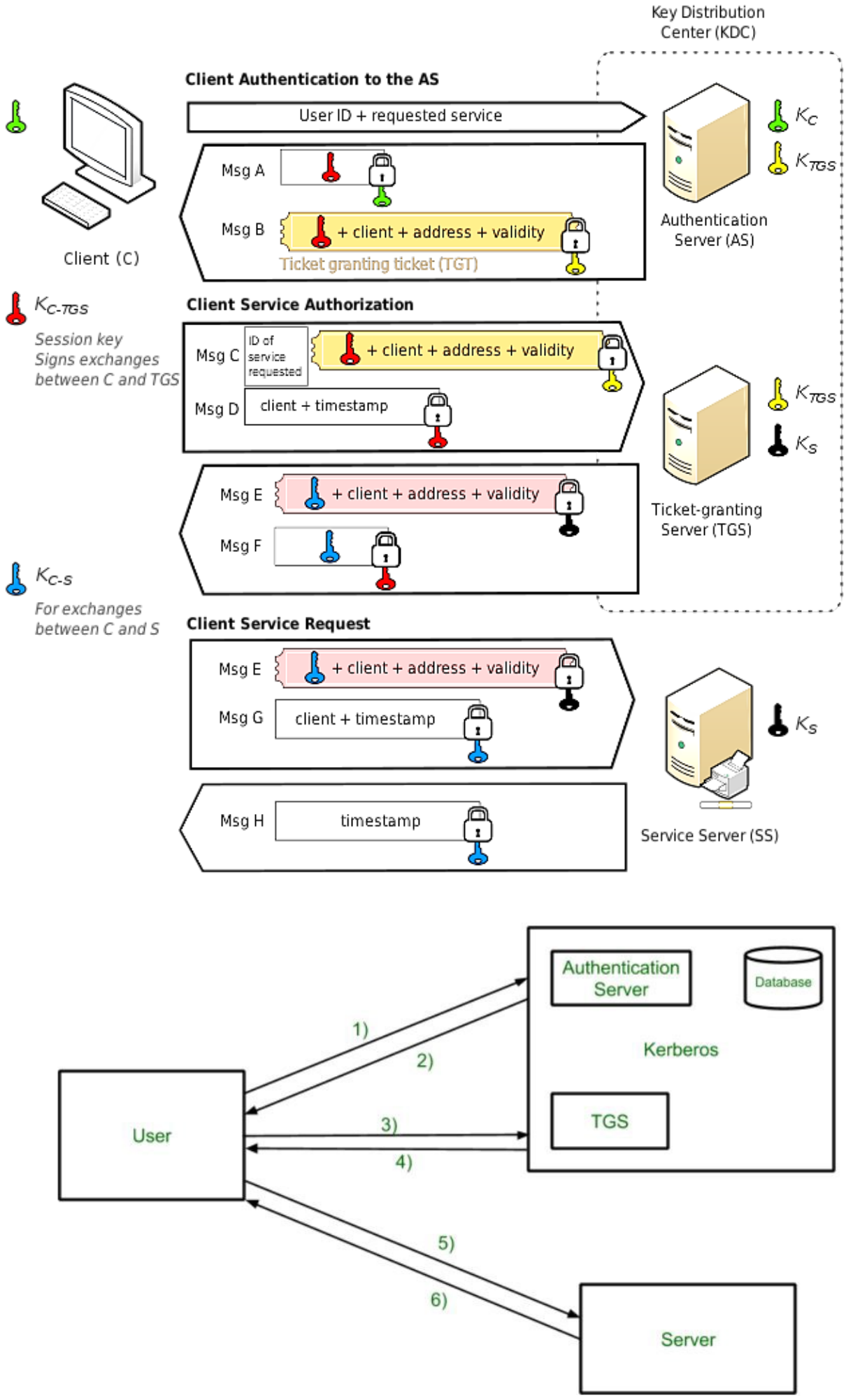


Total length to be 64 bits less than multiple of 512



Final Data to be Hashed as a multiple of 512

Kerberos


Key Distribution Center (KDC)
Client Authentication to the AS
User ID + requested service
Msg A
Msg B
+ client + address + validity
Ticket granting ticket (TGT)
Client (C)
Authentication Server (AS)
K_C
K_{TGS}
$K_{C\text{-}TGS}$
Session key
Signs exchanges between C and TGS
Client Service Authorization
Msg C
ID of service requested
+ client + address + validity
Msg D
client + timestamp
Msg E
+ client + address + validity
Msg F
Ticket-granting Server (TGS)
K_{TGS}
K_S
$K_{C\text{-}S}$
For exchanges between C and S
Client Service Request
Msg E
+ client + address + validity
Msg G
client + timestamp
Msg H
timestamp
Service Server (SS)
K_S

Authentication Server
Database
Kerberos
TGS
User
1)
2)
3)
4)
5)
6)
Server

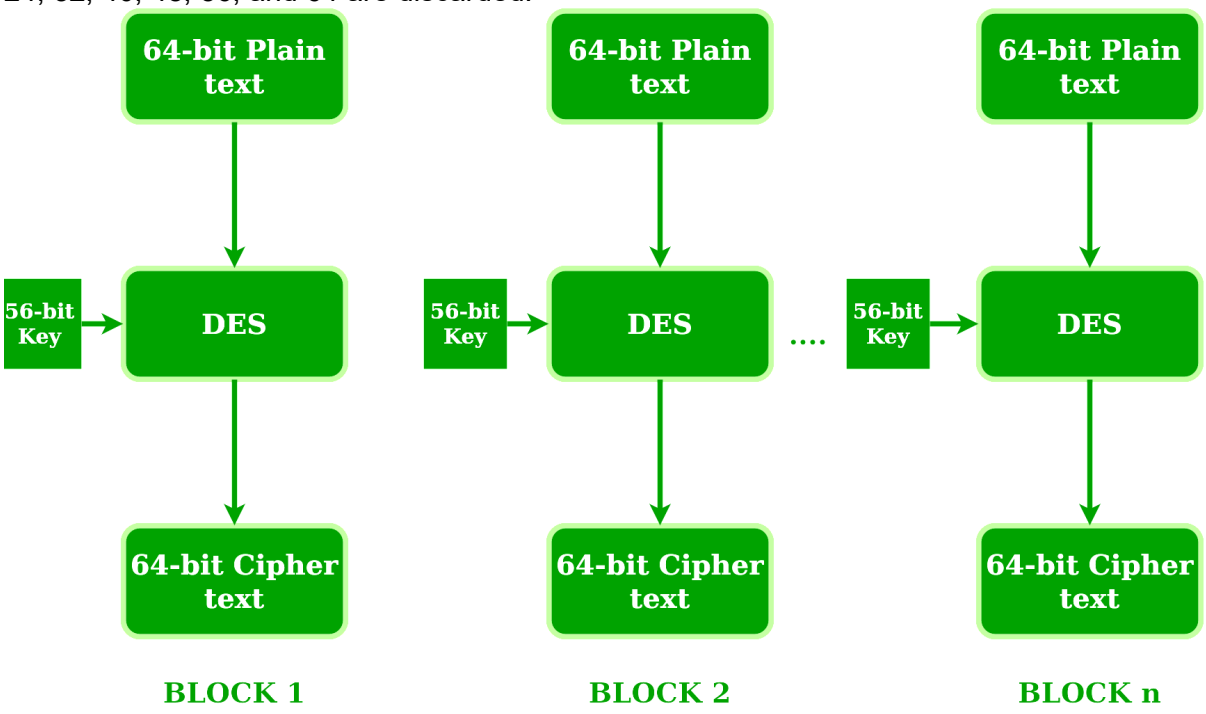
Step-1: User login and request services on the host. Thus user requests for ticket-granting service.
Step-2: Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.
Step-3: The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.
Step-4: Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.
Step-5: The user sends the Ticket and Authenticator to the Server.
Step-6: The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

MD5 Message Digest & SHA1 Secure Hash Algorithm: **1) MD5 can have 128 bits length of message digest.** SHA1 can have 160 bits length of message digest. **2) Faster than SHA**. Slower. **3) To make out the initial message the aggressor would want 2^128 operations whereas exploitation the MD5 algorithmic program**. In SHA1 it'll be 2^160 that makes it quite troublesome to seek out. **4) MD5 provides indigent or poor security.** SHA provides balanced or tolerable security. **5) In MD5, if the assailant needs to seek out the 2 messages having identical message digest then assailant would need to perform 2^64 operations.** In SHA1, assailant would need to perform 2^80 operations which is greater than MD5.

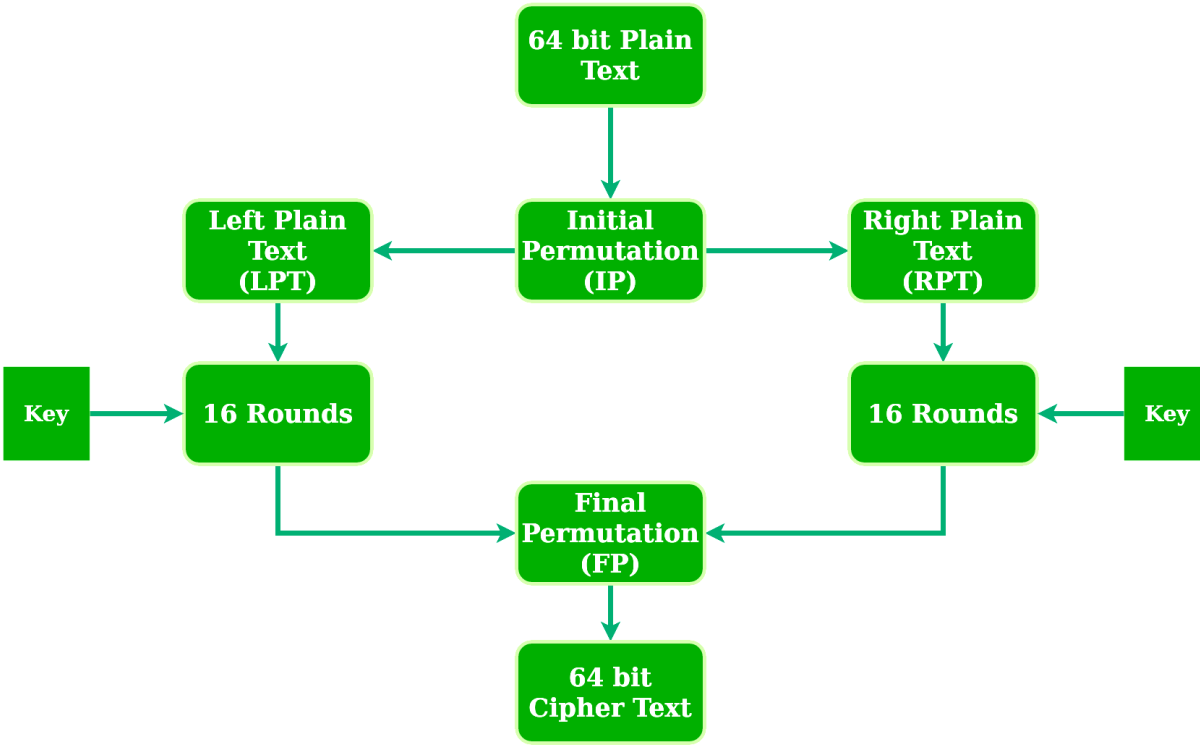
Need for Message Authentication: 1. Verify the origin of the message**.2.**Ensure the message has not been tampered with in transit.**3.**Ensure the message has not been altered or modified by an unauthorized party.**4.**Ensure the integrity and confidentiality of the message. **Techniques:1)Message Authentication Codes (MAC):** A symmetric-key technique used to authenticate messages between two parties. It uses a secret key shared between the sender and receiver to generate a MAC, which is appended to the message. The receiver can then generate their own MAC using the same key and verify the message by comparing the two MACs..**Explanation: a)** A secret key is shared between the sender and receiver.**b)**The sender generates a MAC using the key and appends it to the message.**c)**The receiver generates their own MAC using the same key and compares it to the received MAC. **D)** If the two MACs match, the message is authenticated and has not been tampered with in transit. **E)** If the MACs do not match, the message has been tampered with and should be discarded or further investigated. **F)**The strength of the MAC depends on the length of the key and the cryptographic algorithm used.
2.Digital Signatures: A public-key technique used to authenticate messages between two parties. It uses the sender's private key to sign the message, which can be verified by the recipient using the sender's public key. **3.Hash Functions:** A technique used to ensure the integrity of a message. A hash function generates a fixed-length value that represents the original message. Any change in the message will result in a different hash value.

Role & Properties of hash function: Hash functions play a crucial role in cryptography, as they are used to create digital signatures and verify the authenticity of messages. Hash Function is a function that has a huge role in making a System Secure as it converts normal data given to it as an irregular value of fixed length. A secure hash function is essential in various applications, including digital signatures, password storage, and data verification.
1.Pre-image resistance (one-way-ness): Given a hash value, it should be computationally infeasible to find the input that produced that hash value.
2.Second pre-image resistance (weak collision-resistance): Given an input, it should be computationally infeasible to find another input that produces the same hash value.
3.Collision resistance (strong collision-resistance): It should be computationally infeasible to find two different inputs that produce the same hash value.
4.Fixed output: The hash function should always produce the same size output, regardless of the size of the input.
5.Arbitrary-length input: The hash function should be able to handle inputs of any size.
6.Efficiency: The hash function should be computationally efficient and require a reasonable amount of time to compute.
7.Uniform distribution: The hash function should produce a uniformly distributed output, which means that each possible output should be equally likely.
8.Fast computation: The hash function should be computationally efficient and require a reasonable amount of time to compute.

Data encryption standard (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, with minor differences. The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.



Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key. DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. **steps in DES**. 1) In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function. **2)** The initial permutation is performed on plain text. **3)** Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT). **4)** Each LPT and RPT go through 16 rounds of the encryption process. **5)** In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block **6)** The result of this process produces 64-bit ciphertext.



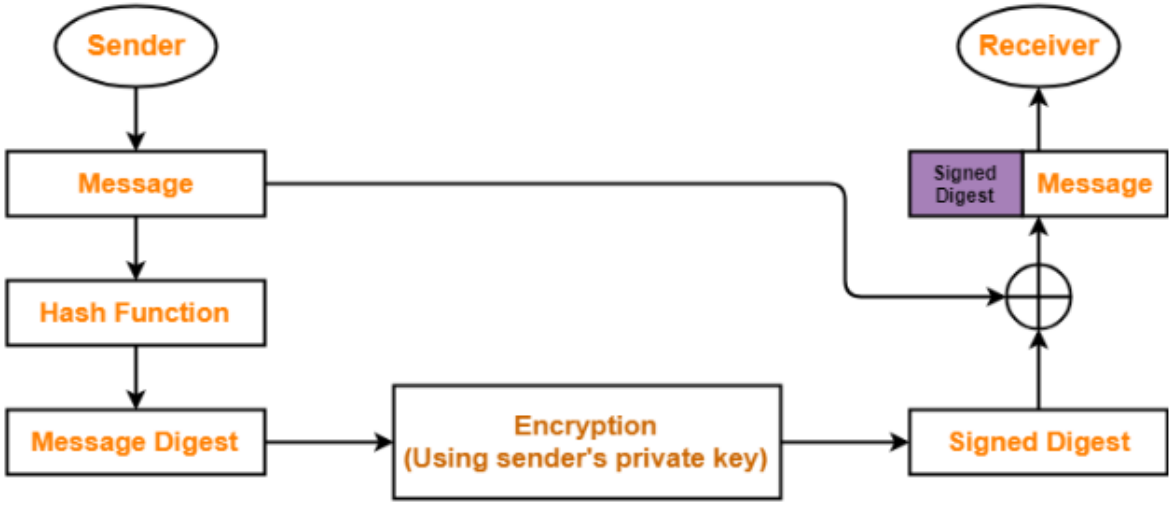
Broad Level Steps in DES

Discuss DES with reference to: i. Fiestel structure and its significance ii. Block Size & key Size iii. Key Expansion iv. Significance of extra swap between left and right half blocks v. Need of expansion permutation vi. Significance of S-box vii. DES function viii.Weak Keys and semi weak keys ix. Possible attacks on DES x. Avalanche effect

i)Fiestel structure and its significance: The Fiestel structure is a design principle for constructing a symmetric-key block cipher that divides the plaintext into two halves and applies a series of rounds on them, with each round using a subkey derived from the main key. In DES, the Fiestel structure is used to perform 16 rounds of encryption and decryption. The significance of the Fiestel structure is that it makes DES highly secure and it makes very difficult for an attacker to decrypt the ciphertext without the key. **ii) Block Size & key Size:** The block size of DES is 64 bits, which means that it can encrypt data in 64-bit blocks at a time. The key size of DES is 56 bits, which means that it uses a 56-bit key to encrypt and decrypt data. **iii) Key Expansion:** To generate subkeys for each round of encryption and decryption, DES uses a key expansion algorithm that generates 16 subkeys from the 56-bit key. The key expansion algorithm uses a combination of permutation and substitution techniques to generate subkeys that are used in each round**.iv) Significance of extra swap between left and right half blocks:** In DES, after each round of encryption or decryption, the left and right halves of the block are swapped. This extra swap ensures that the bits in the left half of the block are mixed with the bits in the right half of the block, making it difficult for an attacker to decrypt the ciphertext without the key.**v) Need of expansion permutation:** In DES, before the main encryption algorithm is applied, the 64-bit plaintext block is first expanded to 72 bits using an expansion permutation. This is done to ensure that each bit of the plaintext is affected by every bit of the key, making it difficult for an attacker to decrypt the ciphertext without the key.**vi) Significance of S-box:** In DES, S-boxes (Substitution boxes) are used to perform substitution on the 48-bit blocks generated by the key expansion algorithm. The S-boxes are designed to ensure that even small changes in the input to the s-box result in significant changes in the output, making it difficult for an attacker to predict the output of the S-box without the key. **vii) DES function:** The DES function is the main encryption and decryption algorithm used in DES. It performs a series of operations on the plaintext block and the subkey generated by the key expansion algorithm to generate the ciphertext block. **viii) Weak Keys and semi-weak keys:** In DES, certain keys are considered weak or semi-weak because they result in a reduced level of security. A weak key is a key that, when used for encryption or decryption, produces the same ciphertext for every plaintext block. A semi-weak key is a key that, when used for encryption or decryption, produces a limited number of possible ciphertexts. **ix) Possible attacks on DES:** One of the main attacks is a brute-force attack, where an attacker tries all possible keys until the correct key is found. Another attack that DES is vulnerable to is differential cryptanalysis. This attack involves observing the differences between plaintexts and their corresponding ciphertexts and using this information to deduce the key. **x) Avalanche effect:** The avalanche effect is the property of encryption algorithms where a small change in the plaintext or the key results in a significant change in the ciphertext. DES has a strong avalanche effect, which means that any small change in the input results in a significant change in the output. This property ensures that any tampering or manipulation of the ciphertext will result in a significant change in the plaintext, making it difficult for an attacker to modify the ciphertext without being detected.

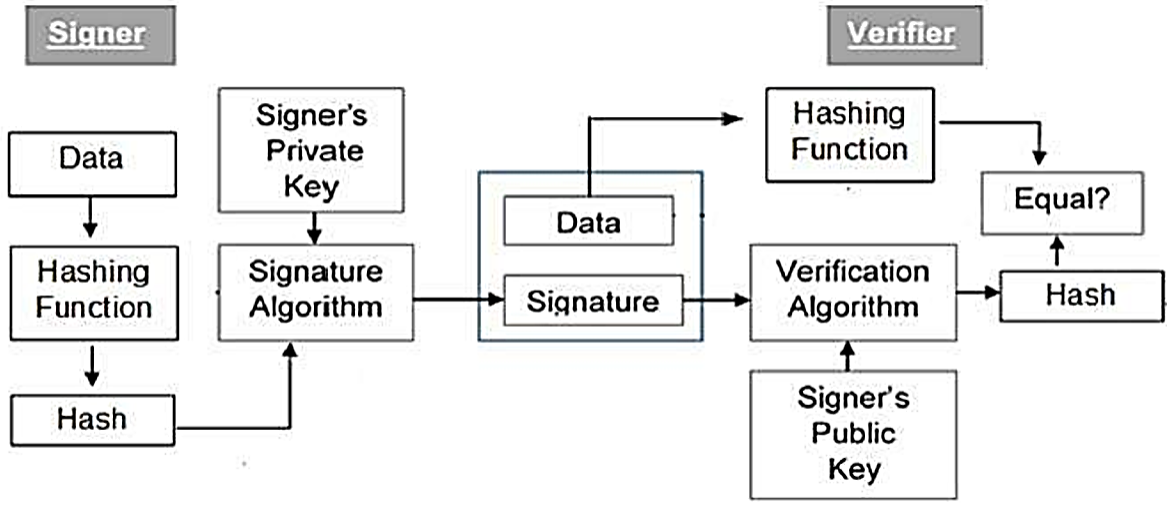
Significance of s and p block in DES:S-boxes substitute the 6-bit input from the previous stage with a 4-bit output. The substitution is based on a fixed table defined in the algorithm that maps each 6-bit input to a corresponding 4-bit output. This substitution provides non-linearity to the algorithm, which makes it difficult for attackers to determine the relationship between the input and the output. There are eight S-boxes used in the DES algorithm, each having a different substitution table. **P-boxes** perform a permutation operation on the output of the S-boxes, rearranging the bits of the output in a predefined pattern. This permutation provides the diffusion property to the algorithm by ensuring that a small change in the input produces a significant change in the output. The permutation provided by the P-box ensures that every output bit depends on every input bit. Together, S-boxes and P-boxes make it extremely difficult for attackers to break the encryption. The S-boxes provide confusion by substituting bits, while the P-boxes provide diffusion by permuting the bits. The combination of these two operations makes the DES algorithm secure and resistant to attacks.

Digital signatures and certificates: are required for secure communication over the internet. In the digital world, people need to exchange information securely over a public network like the internet. This information can be personal information, financial information, or any other confidential information. Digital certificates and signatures help to ensure the authenticity, confidentiality, and integrity of this information.
Digital certificates are issued by Certificate Authorities (CA) to validate the identity of a person, organization or device. The certificate contains the public key of the owner and is digitally signed by the CA. A digital signature is a mathematical algorithm that verifies the authenticity of the digital certificate. It is generated by hashing the certificate and then encrypting the hash with the owner's private key.
Digital signature is a cryptographic technique used to ensure the authenticity, integrity, and non-repudiation of digital messages or documents. It is created using the sender's private key and can be verified using their public key.The process involves creating a hash of the message/document, encrypting the hash using the private key, and appending the resulting digital signature to the message/document.The recipient can verify the digital signature and the message digest using the sender's public key.A digital signature provides assurance that the message/document has not been tampered with during transmission and was indeed sent by the claimed sender.It also provides non-repudiation, meaning that the sender cannot deny having sent the message/document.

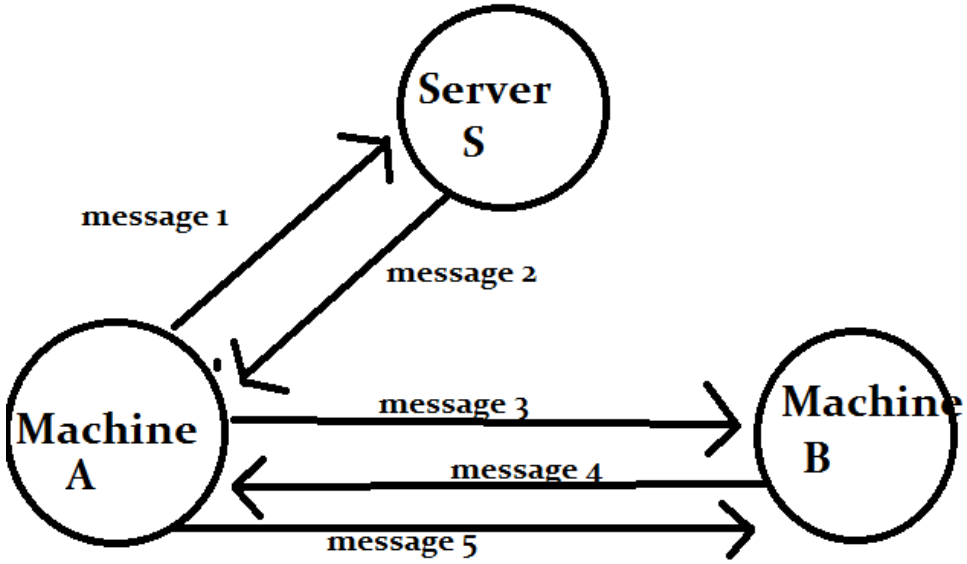


Role of digital signatures in digital certificates: Digital signatures are used for authentication or verification. They are used to verify the authenticity and integrity of a digital document or message. The prominent role of a digital signature is to ensure the integrity and authenticity of a digital document or message. A digital signature is essentially a type of electronic signature which provides non-repudiation and authentication between two parties. It serves as proof that the two parties have agreed to specific terms and conditions and have mutually verified the contents of a document or message.Digital signatures can also protect confidential information, ensuring that only authorized persons can access the data. Digital signatures can also be used to track a digital transaction's source and ensure that it has not been modified.

DSA Algorithm (Digital Signatures Algorithm): Benefits: Message Authentication: You can verify the origin of the sender using the right key combination. **Integrity Verification:** You cannot tamper with the message since it will prevent the bundle from being decrypted altogether. **Non-repudiation:** The sender cannot claim they never sent the message if verifies the signature. **Steps in DSA Algorithm: 1. Key Generation:** Select a prime number p of length l bits. Select a prime number q of length 160 bits. Select an integer g such that g is a primitive root modulo p. Choose a random number x, such that 0 < x < q. Calculate y = g^x mod p. The public key is (p, q, g, y) and the private key is x.
2. Signature generation: Choose a random number k such that 0 < k < q. Calculate r = (g^k mod p) mod q. Calculate s = [(H(m) + x * r)/k] mod q. The signature is (r, s)
3. Signature verification: Verify that 0 < r < q and 0 < s < q. Calculate w = s^-1 mod q. Calculate u1 = [H(m) * w] mod q. Calculate u2 = [r * w] mod q. Calculate v = [(g^u1 * y^u2) mod p] mod q. If v = r, then the signature is valid. Otherwise, it is invalid. where:
p and q are large prime numbers used to generate the keys and are public
g is a generator of a subgroup of order q of Zp* and is public
x is the private key; y is the public key; k is a random number, different for each signature
H(m) is the hash value of the message m, usually computed using a secure hash function.

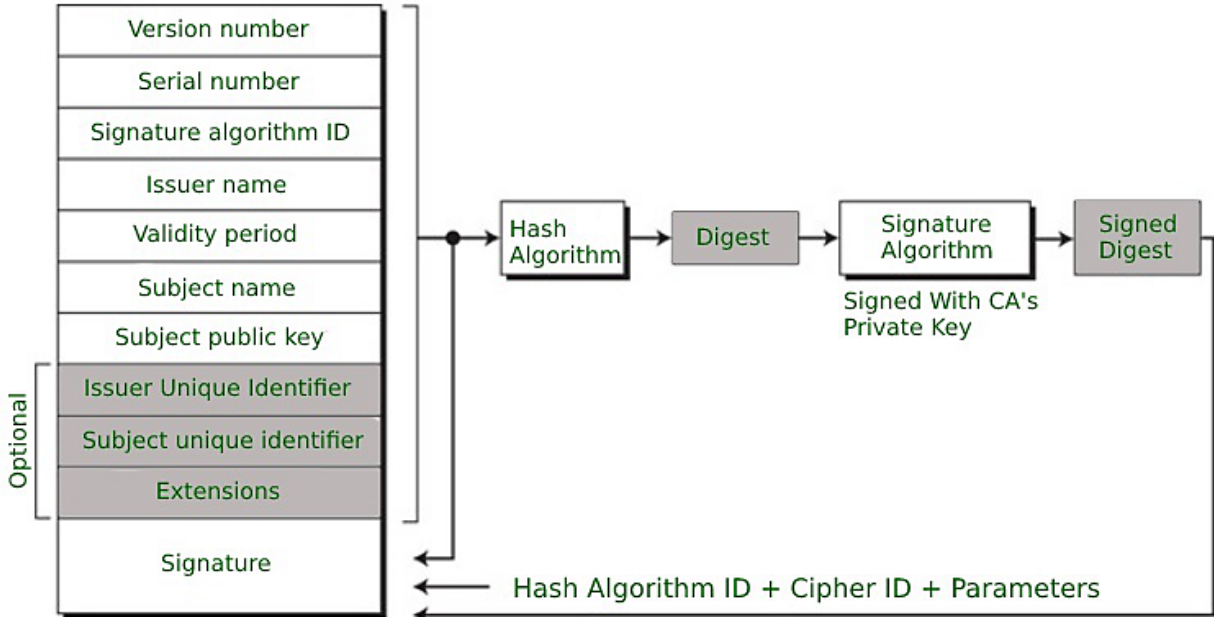


needham-schroeder-protocol: secure authentication and key exchange



A = Machine A; B = Machine B
SK(AS) = this is the symmetric key known to Machine A and middle man Server named “S”
SK(BS) = this is the symmetric key known to Machine B and middle man Server named “S”
NON(A) = Nonce generated by Machine A; NON(B) = Nonce generated by Machine B
SK(S) = this is the symmetric key/session key generated by the server for both machine A and Machine B.
Message 1: Machine 1 sends a message to Server S saying that i want to communicate with Machine B. A -> S: (this message contains A and B and NON(A))
Message 2: Server S sends message 2 back to Machine A containing SK(S), and one more copy of SK(S) encrypted with SK(BS), this copy will be send to Machine B by Machine A.
Message 3: Machine A forwards the copy of SK(S), to Machine B, who can decrypt it with the key it has because it was encrypted by the Middle man server with the Machine B's symmetric Key SK(BS).
Message 4: Machine B sends back Machine A a nonce value encrypted by SK(S). to confirm that he has the symmetric key or session key provided by the middle man server.
Message 5: Machine A performs a simple operation on the nonce provided by the Machine B and resends that back to machine B just to verify Machine A has the key.
After this exchange, both users A and B have the session key to communicate securely. The Needham-Schroeder protocol ensures that both users are authenticated and that the session key is secure by encrypting it with the public key of user B, which only they can decrypt with their private key.

X.509 Authentication Service:

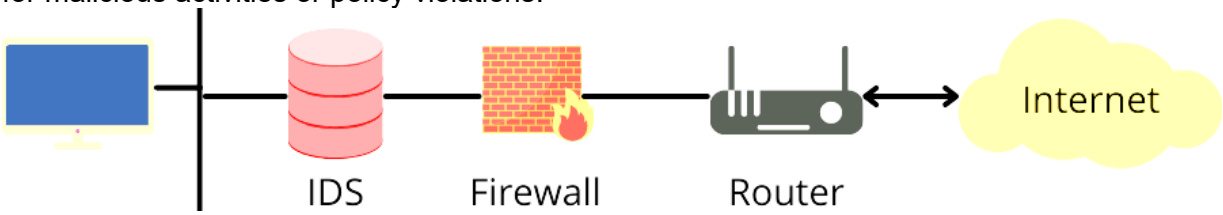


Steps: The core of the X.509 authentication service is the public key certificate connected to each user. These user certificates are assumed to be produced by some trusted certification authority and positioned in the directory by the user or the certified authority. These directory servers are only used for providing an effortless reachable location for all users so that they can acquire certificates. X.509 standard is built on an IDL known as ASN.1. With the help of Abstract Syntax Notation, the X.509 certificate format uses an associated public and private key pair for encrypting and decrypting a message. Once an X.509 certificate is provided to a user by the certified authority, that certificate is attached to it like an identity card.
Version number: It defines the X.509 version that concerns the certificate.
Serial number: It is the unique number that the certified authority issues.
Signature Algorithm Identifier: This is the algorithm that is used for signing the certificate.
Issuer name: Tells about the X.500 name of the certified authority which signed and created the certificate.
Period of Validity: It defines the period for which the certificate is valid.
Subject Name: Tells about the name of the user to whom this certificate has been issued.
Subject's public key information: It defines the subject's public key along with an identifier of the algorithm for which this key is supposed to be used.
Extension block: This field contains additional standard information.
Signature: This field contains the hash code of all other fields which is encrypted by the certified authority private key.
Applications: Document signing and Digital signature, Web server security with the help of Transport Layer Security (TLS)/Secure Sockets Layer (SSL) certificates, Email certificates, Code signing, Secure Shell Protocol (SSH) keys and Digital Identities.

Difference between Firewall & IDS: **1) A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.** An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network. **2) A firewall can block an unauthorized access to network (E.g. A watchman standing at gate can block a thief)**. An IDS can only report an intrusion; it cannot block it (E.g. A CCTV camera which can alert about a thief but cannot stop it). **3) A firewall cannot detect security breaches for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers).** IDS is fully capable of internal security by collecting information from a variety of system and network resources and analyzing the symptoms of security problems **4) Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company).** IDS keeps a check of overall network. **5) No man-power is required to manage a firewall.** An administrator (man-power) is required to respond to threats issued by IDS**. 6) Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)**. IDS are very difficult to be spotted in a network (especially stealth mode of IDS).

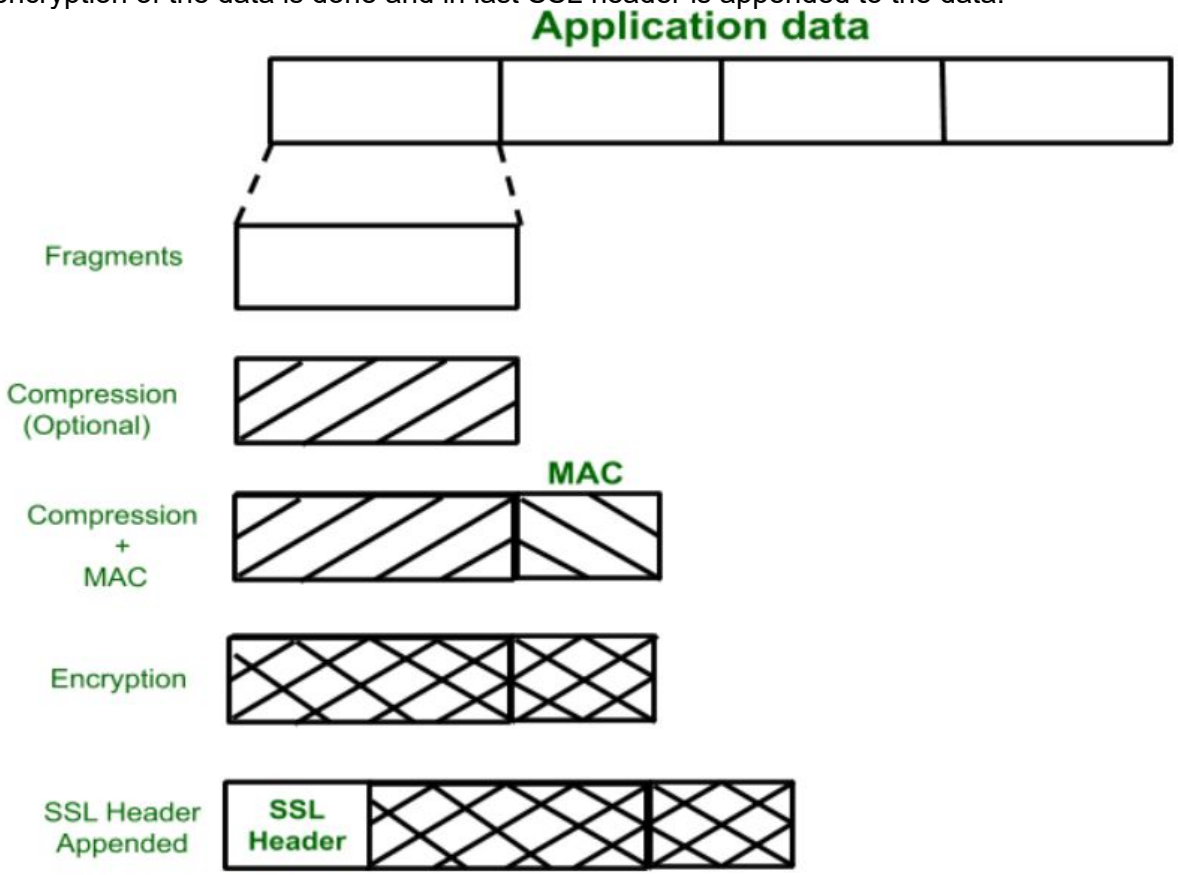
Types of firewalls: 1) Packet Filters : It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports. This firewall is also known as a static firewall. --Simplest Type of firewall—sees only address and service protocol type—auditing is difficult--screens based on connection rules -complex addressing can make configuration tricky. **2) Stateful Inspection Firewalls :** It is also a type of packet filtering which is used to control how data packets move through a firewall. It is also called dynamic packet filtering. These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if, the session is perfectly established between two endpoints else it will block the communication. --a bit more complex than packet filtering—can see either address or data—Auditing is possible—screeens based on information across packets—it is usually preconfigured. **3) Application Layer Firewalls:** These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away. --Even more complex—sees full data portion of packet—can audit activity—screens on the basis of behaviour of proxy—simple proxies can be can be substituted for complex addressing. **4) Guards:** It is a type of firewall that is designed to protect critical network resources like servers, databases, and applications.--most complex—sees full text of communicaton—can audit activity—screens on the basis on interpretation of message content—its functionality can limit assurance**. 5) Personal Firewall:** It is a type of software firewall that runs on individual computers and provides protection against attacks from the internet and other computers on the network. --similar to packet filtering—can see full data portion of packet—can audit activity—screens based on the info of a single packet—usually starts in “deny all inbound” **6) Next-Generation Firewall:** It is a type of firewall that combines the features of packet filtering, stateful inspection, and application layer filtering with advanced security features like intrusion prevention, antivirus, and web filtering.

Intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations.



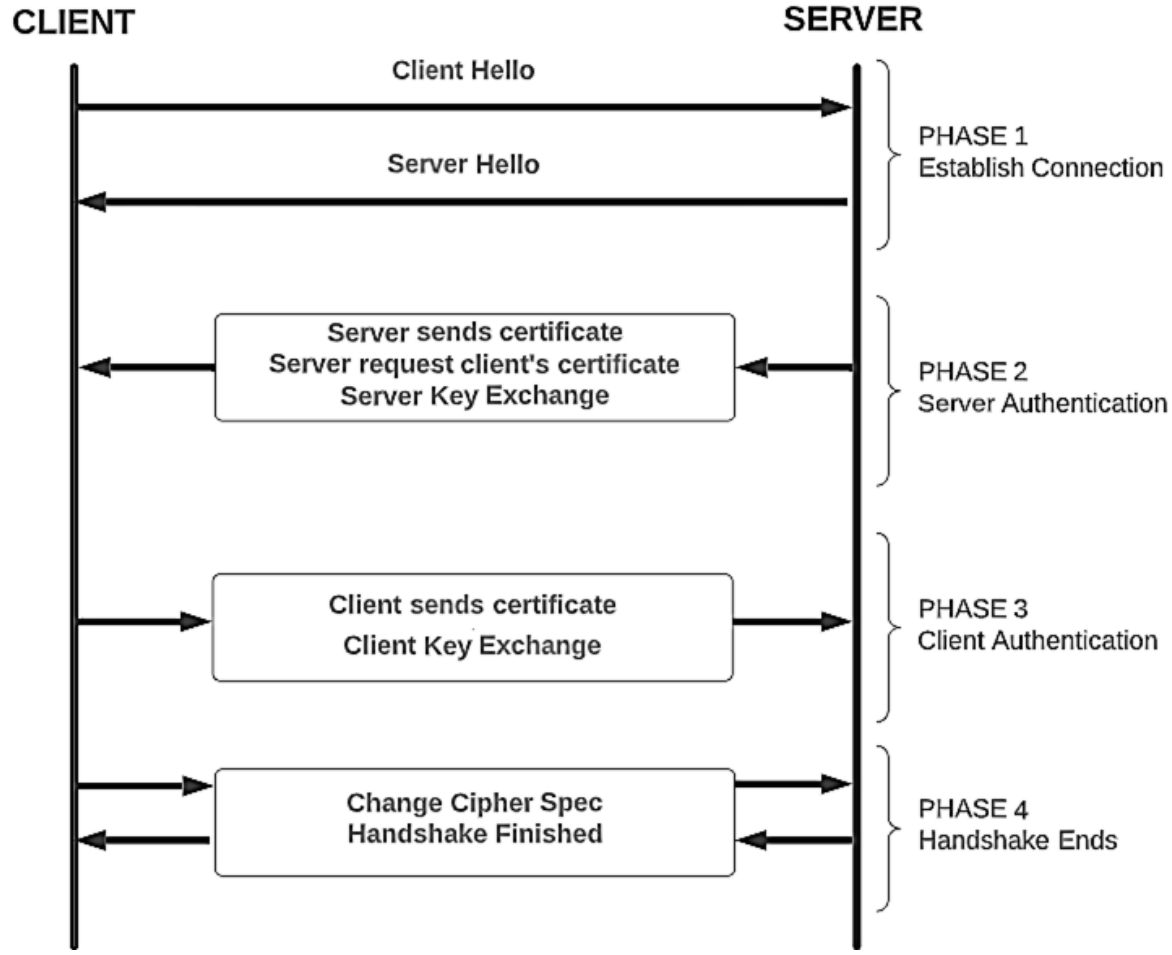
An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity. It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior. The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion. If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator. The system administrator can then investigate the alert and take action to prevent any damage or further intrusion. IDS can be classified into two types: Network-Based IDS (NIDS) and Host-Based IDS (HIDS). Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment. A host Intrusion detection system (HIDS) can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network. Host based IDS systems are used to monitor any intrusion attempts on critical servers. Active IDS is a type of IDS that takes an active role in preventing attacks. It can block suspicious traffic or terminate malicious processes to prevent further damage. Active IDS is useful for quickly responding to and stopping attacks in real-time. Passive IDS, on the other hand, only monitors network traffic or system activity and generates alerts for system administrators or security personnel. It does not take any direct action to prevent or stop attacks. Passive IDS is useful for collecting information about network traffic and analyzing it to identify potential attacks.

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. 1**. In 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) and MD5 is appended. After that encryption of the data is done and in last SSL header is appended to the data.



2. Change-cipher Protocol: This protocol uses the SSL record protocol. Unless Handshake 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.
3. Alert Protocol: This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.
Warning (level = 1): This Alert has no impact on the connection between sender and receiver. Some of them are: **Bad certificate:** When the received certificate is corrupt. **No certificate:** When an appropriate certificate is not available. **Certificate expired:** When a certificate has expired. **Certificate unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable. **Close notify:** It notifies that the sender will no longer send any messages in the connection. **Unsupported certificate:** The type of certificate received is not supported. **Certificate revoked:** The certificate received is in revocation list.
Fatal Error (level = 2): This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are : **Handshake failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available. D**ecompression failure:** When the decompression function receives improper input. **Illegal parameters:** When a field is out of range or inconsistent with other fields. **Bad record MAC:** When an incorrect MAC was received. **Unexpected message:** When an inappropriate message is received.
The second byte in the Alert protocol describes the error.

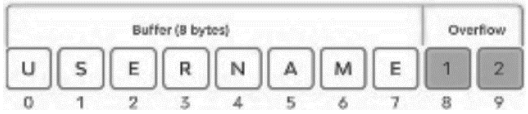
4. Handshake Protocol: is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.
Phase-1: In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
Phase-2: Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
Phase-3: In this phase, Client replies to the server by sending his certificate and Client-exchange-key. **Phase-4:** In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.



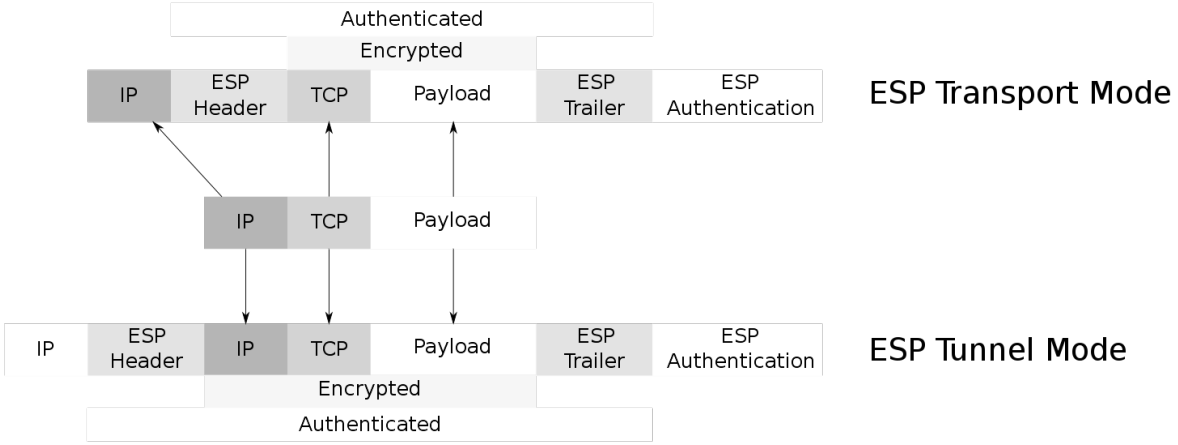
Need for SSL: 1) Encryption: The SSL certificate uses encryption algorithms to secure the communication between the website or service and its users. This ensures that the sensitive information, such as login credentials and credit card information, is protected from being intercepted and read by unauthorized parties. **2)Authentication:** The SSL certificate verifies the identity of the website or service, ensuring that users are communicating with the intended party and not with an impostor. This provides assurance to users that their information is being transmitted to a trusted entity.**3) Integrity:** The SSL certificate uses message authentication codes (MACs) to detect any tampering with the data during transmission. This ensures that the data being transmitted is not modified in any way, preserving its integrity. **4)Non-repudiation:** SSL certificates provide non-repudiation of data, meaning that the recipient of the data cannot deny having received it. This is important in situations where the authenticity of the information needs to be established, such as in e-commerce transactions. **5) Public-key cryptography:** SSL certificates use public-key cryptography for secure key exchange between the client and server. This allows the client and server to securely exchange encryption keys, ensuring that the encrypted information can only be decrypted by the intended recipient. **6) Session management:** SSL certificates allow for the management of secure sessions, allowing for the resumption of secure sessions after interruption. This helps to reduce the overhead of establishing a new secure connection each time a user accesses a website or service.

Dos Attk: A denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. The basic purpose of a DOS attack is simply to flood a network so as to deny the authentic users services of the network.
Types of DoS attacks: 1.Application Layer Flood: This is a type of DoS attack that targets the application layer of a system, such as a web server. The attacker floods the system with a large number of requests, overwhelming the server & causing it to become unresponsive. This type of attack is difficult to detect and mitigate because it appears to be legitimate traffic. **2.Distributed Denial of Service (DDoS):** This is a type of DoS attack that involves multiple systems, often compromised by malware and controlled by the attacker, to flood the target system with traffic. The goal is to overwhelm the system's resources and make it unavailable to legitimate users. DDoS attacks can be difficult to prevent and mitigate because they come from multiple sources and can be distributed across multiple networks.
3. Unintended Denial of Service Attacks: These are DoS attacks that occur unintentionally, often as a result of software bugs or misconfigurations. For example, a software update may cause a server to crash or a misconfigured network device may cause a network outage. These types of attacks are unintentional but can still cause significant disruptions to services.
Ways to mount DOS attack on the system: 1) SYN Flood Attack: 1. The attacker takes control of multiple hosts over the internet instructing them to contact the target Web server. **2.** Each SYN packet is a request to open a TCP connection. For each such packet, the web server responds with a SYNACK packet trying to establish a TCP connection. **3.**SYN request waiting for a response back and becomes bogged down as more traffic floods in due to which users are denied access. **2) Distributed DOS Attack : 1.** An attacker begins a DDoS attack by exploiting vulnerability in one computer system and making it the DDoS master. **2.** The attacker infects multiple systems and controls machines to launch DDoS attacks using commands. **3) Exhaustion of Bandwidth: 1**.The attacker takes control of multiple hosts over the internet instructing them to send ICMP ECHO packets with the targets spoofed IP address to a group of hosts. **2.** Nodes at the bounce site receive multiple spoofed requests and respond by sending echo reply packets to the target site. **3.**The targets router is flooded with packets from the bounce site leaving no data transmission capacity for legitimate traffic. **4) Slowloris 1.** Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. **2.** Slowloris does this by holding as many connections to the target web server open for as long as possible. **5) Ping of Death: 1.** A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. **2.** This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets. **6) UDP Flood:** This type of attack floods random ports on a remote host with numerous UDP packets, causing the host to repeatedly check for the application listening at that port, and reply with an ICMP Destination Unreachable packet. **7) Teardrop Attack:** The Teardrop attack involves sending corrupted IP packages, the purpose of this is to confuse and potentially crash the receiving system. **8) Smurf Attack: 1.** In this the attacker knows the broadcast servers in a network and sends a ping request. **2.**When the broadcast server receives the ping request, the ping request is sent to the entire network and all the machines in the network return a response. These responses are further redirected by the broadcast server to the target machine.

1. Buffer overflow is a type of software vulnerability that occurs when a program or process tries to store more data in a buffer (temporary storage area) than it can hold. **2.**This can happen when the size of the input data exceeds the capacity of the buffer, or when the input data is not properly checked or validated before being stored in the buffer. **3.** Buffer overflow attacks can allow an attacker to overwrite or modify the contents of the buffer, which can lead to a variety of security issues, such as crashing the program, executing malicious code, or gaining unauthorized access to a system.**4.**To prevent buffer overflow attacks, developers can use techniques such as bounds checking, input validation & buffer size limits. **5. S**ecurity measures such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) can make it more difficult for attackers to exploit buffer overflow vulnerabilities. **6.** Regular software updates and security patches can also help to mitigate the risk of buffer overflow attacks. **7.** Overall, buffer overflow attacks are a serious threat to software security and can have significant consequences if not properly addressed.



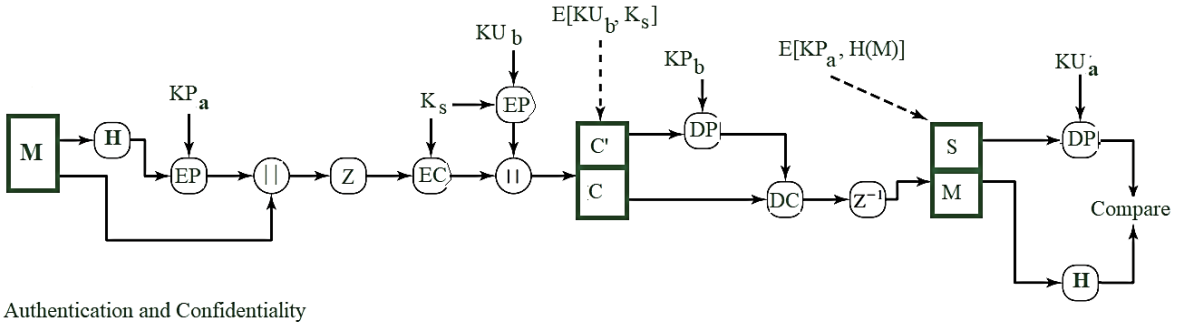
IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. **Components of IP Security: 1. Encapsulating Security Payload (ESP):** is an IPSec protocol that provides confidentiality, integrity, and authentication of the IP packet payload. It encrypts the payload using a shared secret key, and also adds a message digest to provide integrity and authenticity of the payload. The recipient of the packet can then verify the digest and decrypt the payload using the shared secret key. **2. AH (Authentication Header)** is an IPSec protocol that provides authentication and integrity of the IP packet header. It ensures that the packet has not been tampered with during transmission. AH calculates a message digest using a shared secret key and adds it to the packet header. The recipient of the packet can then verify the digest to ensure the packet has not been modified. **3. Internet Key Exchange (IKE):** It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not.



Transport mode: Provides end-to-end security between two hosts. Protects only the payload of the IP packet, leaving the header unencrypted. Uses IP protocol number 50 to encapsulate the payload. Provides encryption and authentication of the payload. AH and ESP protocols can be used to provide authentication and encryption, respectively.
Tunnel mode: Provides security between two networks. Protects both the payload and the header of the IP packet by encapsulating the original packet within a new packet. Uses IP protocol number 51 to encapsulate the new packet. Provides encryption and authentication of the entire packet. AH and ESP protocols can be used to provide authentication and encryption, respectively.

Public Key Infrastructure (PKI): It is a set of protocols and technologies used to manage the creation, use, storage, and revocation of digital certificates and public-private key pairs. **1)** PKI provides a framework for secure communication over the internet by using public-key cryptography. It allows entities to securely exchange data without having to share their private keys. **2)** PKI consists of several components, including a certificate authority (CA), a registration authority (RA), a certificate repository & certificate revocation list (CRL). **3)** The CA is responsible for issuing digital certificates to entities and verifying their identity. The RA is responsible for verifying the identity of entities before the CA issues the certificate. The certificate repository is a central location where certificates are stored, and the CRL is a list of revoked certificates. **4)** PKI is used to secure various types of communication, including email, web browsing & file transfer. It is also used for secure remote access & virtual private networks(VPNs). **5)** Transport Layer Security (TLS) is a protocol that uses PKI to secure communication between web browsers and servers. It is commonly used to secure online transactions, such as online banking and shopping. **6)** PKI can be used for digital signatures, which provide a way to verify the authenticity of digital documents. Digital signatures are used in many applications, such as contracts, legal documents & software updates. **7)** PKI has some drawbacks, such as the complexity of managing certificates & the potential for key compromise or loss. However, it remains an important technology for secure communication and is widely used in many industries, including finance, healthcare & government.

Pretty Good Privacy (PGP) is a secure email program that provides a confidentiality and authentication service that can be used for electronic email and file storage applications. PGP achieves confidentiality and authentication by the following steps: **1 Authentication: M**eans something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure. In the email world, checking the authenticity of an email is nothing but to check whether it actually came from the person it says. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience.
2. Confidentiality: Sometimes we see some packages labelled as 'Confidential', which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two. The message is first compressed and a 128 bit session key (Ks), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key (Ks) itself gets encrypted through public key encryption (EP) using receiver's public key(KUb) . Both the encrypted entities are now concatenated and sent to the receiver. At the receiver's end, the encrypted session key is decrypted using receiver's private key (KPb) and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the original message (M). RSA algorithm is used for the public-key encryption and for the symmetric key encryption, CAST-128(or IDEA or 3DES) is used.



Authentication and Confidentiality

Software Vulnerabilities: 1. Buffer Overflow: This occurs when a program tries to write more data to a buffer than it can hold, allowing an attacker to overwrite adjacent memory and execute malicious code. **Example:** An attacker can craft a specific input to a program, such as a long string of characters, that will overflow the buffer and overwrite memory with their own code, which can be executed by the program.**2. SQL Injection:** This occurs when an attacker uses malicious input to manipulate a SQL query and access unauthorized data or perform unauthorized actions. **Example:** An attacker can input SQL code into a web form that is not properly sanitized, causing the SQL query to execute malicious code that can access or modify data in the database.**3. Cross-Site Scripting (XSS):** This occurs when an attacker injects malicious code into a website that is then executed by a user's browser. **Eg:** An attacker can input JavaScript code into a web form that is not properly sanitized, causing the code to execute when a user visits the website, potentially allowing the attacker to steal sensitive data or perform unauthorized actions. **4. Cross-Site Request Forgery (CSRF):** This occurs when an attacker tricks a user into unknowingly performing an action on a website, such as submitting a form or making a payment. **Eg:** An attacker can craft a webpage that includes a hidden form that submits a request to a vulnerable website when the user visits the page, causing the user to unknowingly perform an action on the website without their knowledge. **5. Remote Code Execution:** This occurs when an attacker is able to execute arbitrary code on a system, potentially allowing them to take control of the system or access sensitive data. **Eg:** An attacker can exploit a vulnerability in a web application or server software to execute their own code on the system, potentially allowing them to access sensitive data or take control of the system.

SQL injection involves inputing the SQL queries into an application to perform an unexpected action. Often, existing queries are simply edited to achieve the same results. SQL is easily manipulated by the placement of even a single character in a chosen spot, causing the entire query to behave in quite malicious ways. The characters that are most commonly used for such input validation attacks include the meaning in SQL backtick , the double dash (-), and the semicolon (. all of which have special meaning in SQL. SQL injection is a type of web security vulnerability that allows an attacker to execute malicious SQL statements in a web application's backend database, potentially gaining access to sensitive data or compromising the application's functionality. **SQL injection attacks occur when an application does not properly validate user inputs or improperly constructs SQL queries based on user-supplied inputs. Example:** Suppose a web application has a search field that allows users to search for products by name, and the SQL query for the search function is constructed as follows:
SELECT * FROM products WHERE name = '<user-supplied input>'
An attacker could enter the following input into the search field: **' OR '1'='1**
The resulting SQL query: **SELECT * FROM products WHERE name = '' OR '1'='1'**

Types of viruses: 1. Parasitic virus: A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect. **2. Memory-resident virus:** Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes. **3. Boot sector virus:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.**4. Stealth virus**: A form of virus explicitly designed to hide itself from detection by antivirus software.**5. Polymorphic virus:** A virus that mutates with every infection, making detection by the signature of the virus impossible.
Propagation of virus: 1) Dormant phase: The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. 2) **Propagation phase:** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase. **3)Triggering phase:** The virus is activated to perform the function for which it was intended.**4) Execution phase:** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Propogation of worms: A network worm exhibits the same characteristics as a computer virus a dormant phase a propagation phase, a triggering phase and an execution phase. **1.** Search for other systems to infect by examining host tables or siml repositories of remote system addresses. **2.** Establish a connection with a remote system. **3.** Copy itself to the remote system and cause the copy to be run.
Types of worms: 1) Worm is a program that replicates itself by installing copies of itself on other machines across a network. **2)** An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system**. 3)** Network worm programs use network connections to spread from system to system. To replicate itself, a network worm uses some sort of network vehicle.

Diff b/w Worm and Virus: **1)Worm is a form of malware that replicates itself and can spread to different computers via Network.** A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. **2) The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.** The main objective of viruses is to modify the information. **3) It doesn't need a host to replicate from one computer to another.** It requires a host is needed for spreading. **4) less harmful.** More harmful **5) Worms generally comes from the downloaded files or through a network connection.** Viruses generally comes from the shared or downloaded files. **6) Symptoms: Hampering computer performance by slowing down it. Automatic opening and running of programs. Sending of emails without your knowledge. Affected the performance of web browser. Error messages concerning to system & OS.** Symptoms: Pop-up windows linking to malicious websites. Hampering computer performance by slowing down it. After booting, starting of unknown programs. Passwords get changed without your knowledge. **7) Eg: Morris worm, storm worm, etc.** Eg: Creeper, Blaster, Slammer, etc.

Trojan Horses: 1) A Trojan horse is a single harmful programme that can give another PC complete control of an infected PC. **2)** This is a code segment that attempts to exploit its own environment. **3)** They have an appealing appearance, yet they are extremely dangerous and serve as virus vectors. **4)**It could manufacture duplicates of them, damage the host computer systems, or steal data. **5)** The Trojan horse will do damage if installed or executed on your computer, but it will look to be useful software at first glance. **6)** Trojans are designed to inflict substantial damage to your system by deleting files and destroying data. **7)** Trojans allow the system to compromise confidential or personal information, resulting in the creation of a backdoor on your computer that grants unauthorised persons access to your system. **8)** Because Trojans do not self-replicate or multiply by infecting other files, Trojan horse viruses differ from other computer viruses in that they do not disseminate themselves. **9)** Beast, Zeus, The Blackhole Exploit Kit, Flashback Trojan, Netbus, Subseven, Y3K Remote Administration Tool, and Back Orifice are the most common Trojan horses.

Trap door: 1) A trap door is a type of hidden entry point into a programme that allows anyone to obtain access to any system without having to go through the normal security access procedures. **2)** A trap door is also defined as a technique of circumventing standard authentication mechanisms. As a result, it is often known as a back door. **3)** Trap Doors are difficult to detect, and in order to identify them, programmers or developers must search through the system's components. **4)** Trap door is legitimately used by programmers to debug and test programmes. When dishonest programmers obtain unlawful access, trap doors become threats. **5)** The primary priority of security measures should be programme development and software update activities. It is tough to implement the operating system that controls the trap doors.

Logic Bomb: It is a type of malware that contains malicious code that is discreetly installed into software, a computer network, or an operating system with the goal of causing harm to a network when certain conditions are met. It is triggered at a specific event and used to devastate a system by clearing hard drives, deleting files, or corrupting data. An event can be a specific date or time leading up to the launch of an infected software application or the deletion of a specific record from a system. In order to maximize damage before being noticed, logic bombs are mainly used with trojan horses, worms, and viruses. The primary objective of logic bombs is to reformat a hard drive, modify or corrupt data, and remove important files from the system. The devastation caused by a logic bomb can be a huge level.

Attks on OSI Layers: 1) Physical: Wire-cuts; Disrupting the signal; Any other media transmission disturbance**. 2) Data Link:** ARP Flooding; ARP Spoofing; MAC flooding; DHCP Spoofing **3) Network:** IP Spoofing; Source Address Spoofing; ICMP Flood; Packet Sniffing; Teardrop attack; Other DoS attacks **4) Transport:** SYN Flood; UDP Flood; Port Scanning; Other DoS attacks **5) Session:** Session Hijacking; SSH downgrade; Session sniffing **6) Presentation:** Malicious SSL requests;Inspecang SSL encryption packets **7)Application:** Layer Dos attacks (HTTP flood); SQL tniecuon; Cross-site scriptitw; DNS Spoofing

Prime Numbers:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Hill cipher: Encryption: C= PxK mod26
(C1,C2,C3)=[(P1,P2,P3)x(K1,K2,K3;K4,K5,K6;K7,K8,K9)]mod26
Decryption: P= CxK^{-1} mod26 where K^{-1} = multiplicative inverse of det of K x Adjoint K

Diffie-Hellman (g,n): A=g^x modn; B=g^y modn;
Authentication K1= B^x modn; K2=A^y modn where **K1=K2**