CNS IMPORTANT QUESTIONS

Module 1:

1. Cia triad

- The **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.
- It stands for:
- **Confidentiality:** This term covers two related concepts:
    a. Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
    b. 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.
- **Integrity**: This term covers two related concepts:
    a. Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
    b. System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
    c. In simple words SENT = RECEIVED
- **Availability:** Assures that systems work promptly and service is not denied to authorized users
- Additional elements of CIA Triad:
    a. **Authenticity:** It is the property of being genuine & verifying the parties involved.
    b. **Accountability:** Every individual user working with an information system should have specific responsibilities for Information assurance.
- Examples:
    a. Confidentiality: Banking Account Information
    b. Integrity: Patients Information
    c. Availability: Authentication Services

2. Explain OSI security architecture

- Security Architecture for OSI defines a systematic way of defining and providing security requirements for us it provides a useful, if abstract, overview of concepts we will study in the due course.
- OSI Security Architecture Encompasses three main concepts:
    - Security Attacks
    - Security Services
    - Security Mechanisms
- **Security attacks**:
    - A THREAT is a potential for violation of security,which exits when there is a circumstance, capability,action or event that could breach security and

cause harm.

- ATTACK is any action that compromises the security of information owned by an organization.
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.
- Passive Attacks:
  - Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.
  - Two types of passive attacks are the **release of message contents** and **traffic analysis.**
  - Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
  - The emphasis in dealing with passive attacks is on prevention rather than detection

- Active Attacks: Active attack involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.
  - **A Masquerade** takes place when one entity pretends to be a different entity.Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.
  - **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.In this attack, the attacker can 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.
  - **Modification** of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
  - **Denial of Service (DoS)** is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests. An attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.

- **Security Services**:
  - Authentication - assurance that the communicating entity is the one

claimed
    - Access Control - prevention of the unauthorized use of a resource
    - Data Confidentiality –protection of data from unauthorized disclosure
    - Data Integrity - assurance that data received is as sent by an authorized entity
    - Non-Repudiation - protection against denial by one of the parties in a communication

Table 1.2 Security Services (X.800)

AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-Origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block. **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-Flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

- **Security Mechanisms:**
    - The mechanisms are divided into those that are implemented in a specific

protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.

- Specific security mechanisms: encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms: trusted functionality, security labels, event detection, security audit trails, security recovery

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	PERVASIVE SECURITY MECHANISMS Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The 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.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** *Data collected and potentially used to facilitate a* security audit, which is an independent review and examination of system records and activities.
	Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

SPECIFIC SECURITY MECHANISMS	
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

3. Classical encryption techniques

The two basic building blocks of all encryption techniques are Substitution and Transposition.

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.
- A different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

CAESAR CIPHER

- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.
- So that the general Caesar algorithm is
    - $C = E(k, p) = (p + k) \bmod 26$
    - $p = D(k, C) = (C - k) \bmod 26$
- For example,
  plain: meet me after the toga party
  cipher: PHHW PH DIWHU WKH WRJD SDUWB
- Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:
  1. The encryption and decryption algorithms are known.
  2. There are only 25 keys to try.
  3. The language of the plaintext is known and easily recognizable

MONOALPHABETIC SUBSTITUTION CIPHER

- A permutation of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once.
- For example, if S = {a, b, c}, there are six permutations of S
  abc, acb, bac, bca, cab, cba
- In general, there are n! permutations of a set of n elements, because the first element can be chosen in one of n ways, the second in n - 1 ways, the third in n - 2 ways, and so on.
- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 * 1026 possible keys.
- Such an approach is referred to as a Monoalphabetic Substitution Cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

MONOALPHABETIC SUBSTITUTION CIPHER

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

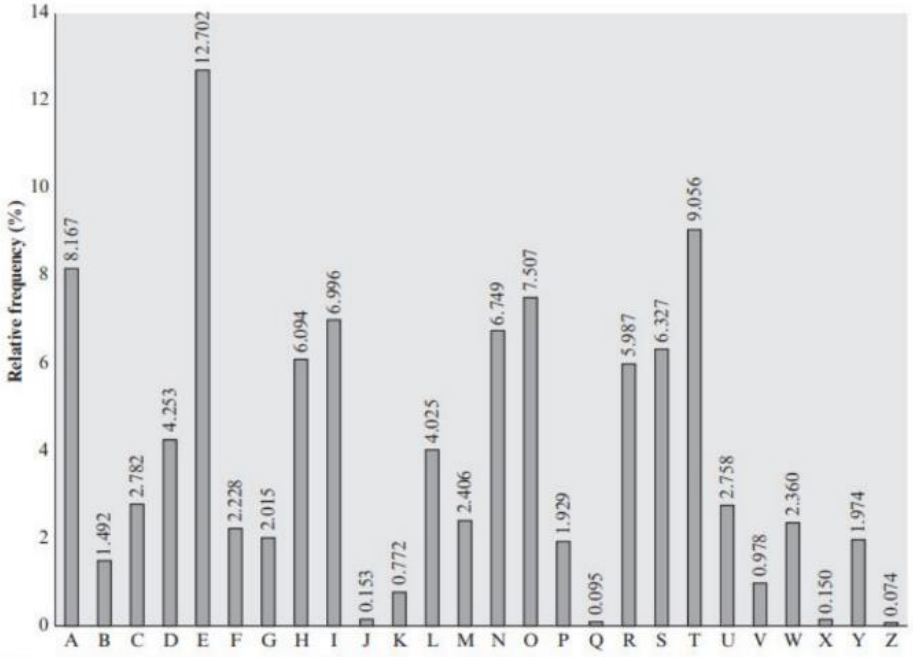


Figure 3.5 Relative Frequency of Letters in English Text

DRAWBACKS

● A table similar to Figure 3.5 could be drawn up showing the relative frequency of diagrams.

● The most common such diagram is “th”

● In our ciphertext, the most common diagram is ZW, which appears three times.

● So we make the correspondence of Z with t and W with h. Then, by our earlier hypothesis, we can equate P with e. Now notice that the sequence ZWP appears in the ciphertext, and we can translate that sequence as “the.”

PLAYFAIR CIPHER

- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letters I and J count as one letter.
- Plaintext is encrypted two letters at a time, according to the following rules:
    a. Repeating plaintext letters that are in the same pair are separated with a filler letter.
    b. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
    c. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
    d. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.
- PLAINTEXT: greet = gr ee t = gr ex et
  KEYWORD: moon mission = m,o,n,i,s

M	O	N	I/J	S
A	B	C	D	E
F	G	H	K	L
P	Q	R	T	U
V	W	X	Y	Z

Cipher Text: HQ CZ DU

VIGENERE CIPHER

- Simplest polyalphabetic ciphers
- In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Thus, the first letter of the key is added to the first letter of the plaintext, mod 26, the second letters are added, and so on through the first m letters of the plaintext.

- For the next m letters of the plaintext, the key letters are repeated. This process continues until all of the plaintext sequence is encrypted.
- A general equation of the encryption process is
  $C_i = (p_i + k_{i \bmod m}) \bmod 26$
- Similarly, decryption is a generalization of above Equation
  $p_i = (C_i - k_{i \bmod m}) \bmod 26$

VERNAM CIPHER

The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

His system works on binary data (bits) rather than letters.

ci = pi ⊕ki

where pi = ith binary digit of plaintext

ki = ith binary digit of key ci = ith binary digit of ciphertext

⊕= exclusive@or (XOR) operation

pi = ci ⊕ki

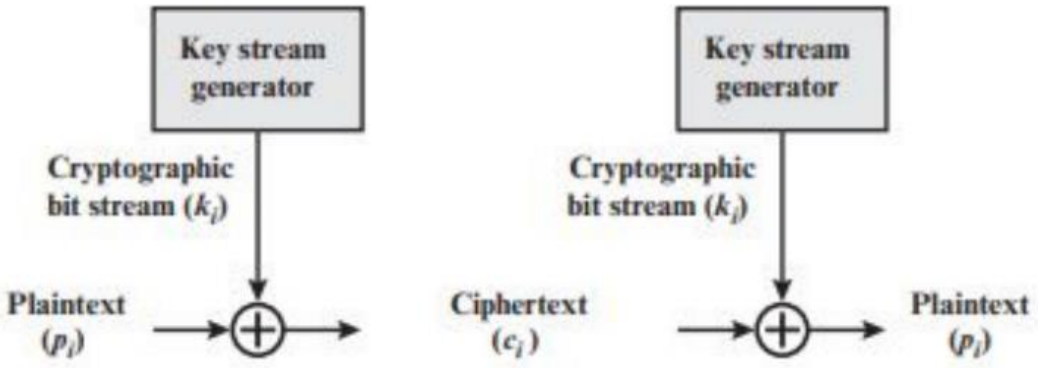


Figure 3.7 Vernam Cipher

ONE TIME PAD

● An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement

to the Vernam cipher that yields the ultimate in security.

● Mauborgne suggested using a random key that is as long as the message, so

that the key need not be repeated.

● In addition, the key is to be used to encrypt and decrypt a single message,

and then is discarded.

● Each new message requires a new key of the same length as the new

message.

● Such a scheme, known as a one-time pad, is unbreakable. It

● It produces random output that bears no statistical relationship to the

plaintext.

● Because the ciphertext contains no information whatsoever about the

plaintext, there is simply no way to break the code.

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pftgpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

● There is the practical problem of making large quantities of random keys. Any heavily used

system might require millions of random characters on a regular basis. Supplying truly

random characters in this volume is a significant task.

● Even more daunting is the problem of key distribution and protection. For every message to

be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth

key distribution problem exists.

TRANSPOSITION CIPHER

● So far, all the ciphers we've discussed are substitution ciphers, in which

plaintext letters are replaced by ciphertext letters.

● Changing the positions of plaintext letters is another enciphering technique.

It's called transposition, as in transferring position.

RAIL FENCE CIPHER

● The simplest such cipher is the Rail Fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

● It is also known as Keyless Transposition Cipher

● For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following:

m		e		m		a		t		r		h		t		g		p		r		y
	e		t		e		f		e		t		e		o		a		a		t	

● The encrypted message is MEMATRHTGPRYETEFETEOAAT

COLUMNAR TRANSPOSITION CIPHER

● A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

● This is called Keyed Transposition Cipher. The order of the columns then becomes the key to the algorithm. For example,

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

4. Compare classical and modern encryption

Aspect	Classical Encryption Techniques	Modern Encryption Techniques
Key Length	Typically shorter key lengths	Utilizes longer key lengths for added security
Algorithms	Simple substitution and transposition ciphers, e.g., Caesar cipher, Vigenère cipher	Complex mathematical algorithms, e.g., AES, RSA, ECC
Security	Generally less secure and easier to break with modern computing power and techniques	Designed to be highly secure against modern attacks
Cryptanalysis	Vulnerable to frequency analysis, brute force attacks, and known-plaintext attacks	Resistant to most known attacks, requiring advanced techniques like quantum computing for potential vulnerabilities
Key Management	Often lacks robust key management systems	Incorporates secure key management protocols and practices
Block vs Stream Ciphers	Primarily used stream ciphers like the one-time pad	Utilizes block ciphers, making them more secure and practical
Speed	Often faster due to simplicity, but less secure	Slower due to complex mathematical operations, but more secure
Application	Historical and not suitable for securing modern data and communications	Widely used in modern data protection, secure communication, and e-commerce
Use of Computers	Originally designed for manual encryption/decryption	Designed for use with computers and digital systems
Public Key Cryptography	Lacks public key cryptography, limiting secure communication over open networks	Utilizes public key infrastructure for secure communication over the internet
Resilience Against Attacks	Prone to various attacks, including known-plaintext attacks	Resistant to many known attacks and requires more sophisticated methods for breaking encryption
Key Exchange	Lacks efficient and secure methods for key exchange	Provides secure key exchange mechanisms, e.g., Diffie-Hellman, ECDH
Quantum Resistance	Not designed with quantum resistance in mind	Some modern encryption techniques are designed to be quantum-resistant
Regulatory Compliance	May not meet regulatory compliance requirements	Designed to meet regulatory standards for data protection and privacy

5. Short note on steganography

- A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

- A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message.
- Various other techniques have been used historically; some examples are the following:
    - Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
    - Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
    - Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- Steganography has a number of drawbacks when compared to encryption:
    - It requires a lot of overhead to hide a relatively few bits of information.
    - Also, once the system is discovered, it becomes virtually worthless.
- Alternatively, a message can be first encrypted and then hidden using steganography.

Module 2:

1. Explain different block cipher modes of operation

- Block cipher is an encryption algorithm that takes a fixed size of input, say b bits and produces a ciphertext of b bits again.
- If the input is larger than b bits it can be divided further.
- For different applications and uses, there are several modes of operations for a block cipher.

Electronic Codebook Mode:

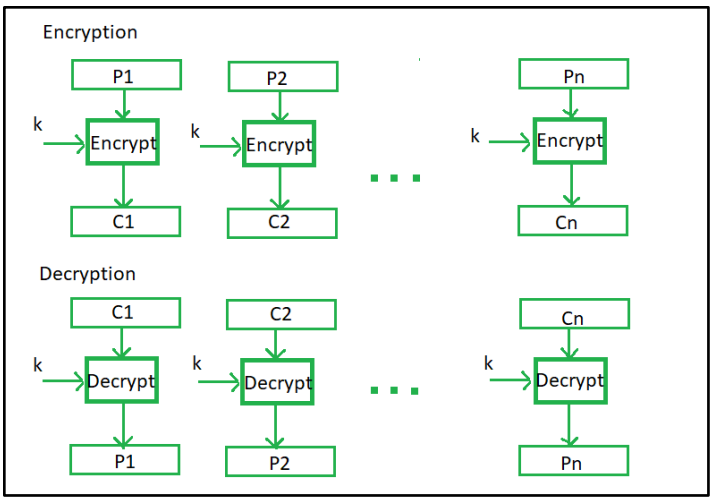
- Electronic code book is the easiest block cipher mode of functioning.
- It is easier because of direct encryption of each block of input plaintext and output is in the form of blocks of encrypted ciphertext.
- Generally, if a message is larger than b bits in size, it can be broken down into a bunch of blocks and the procedure is repeated

Advantages of using ECB –

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of using ECB –

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.



Cipher Block Chaining Mode:

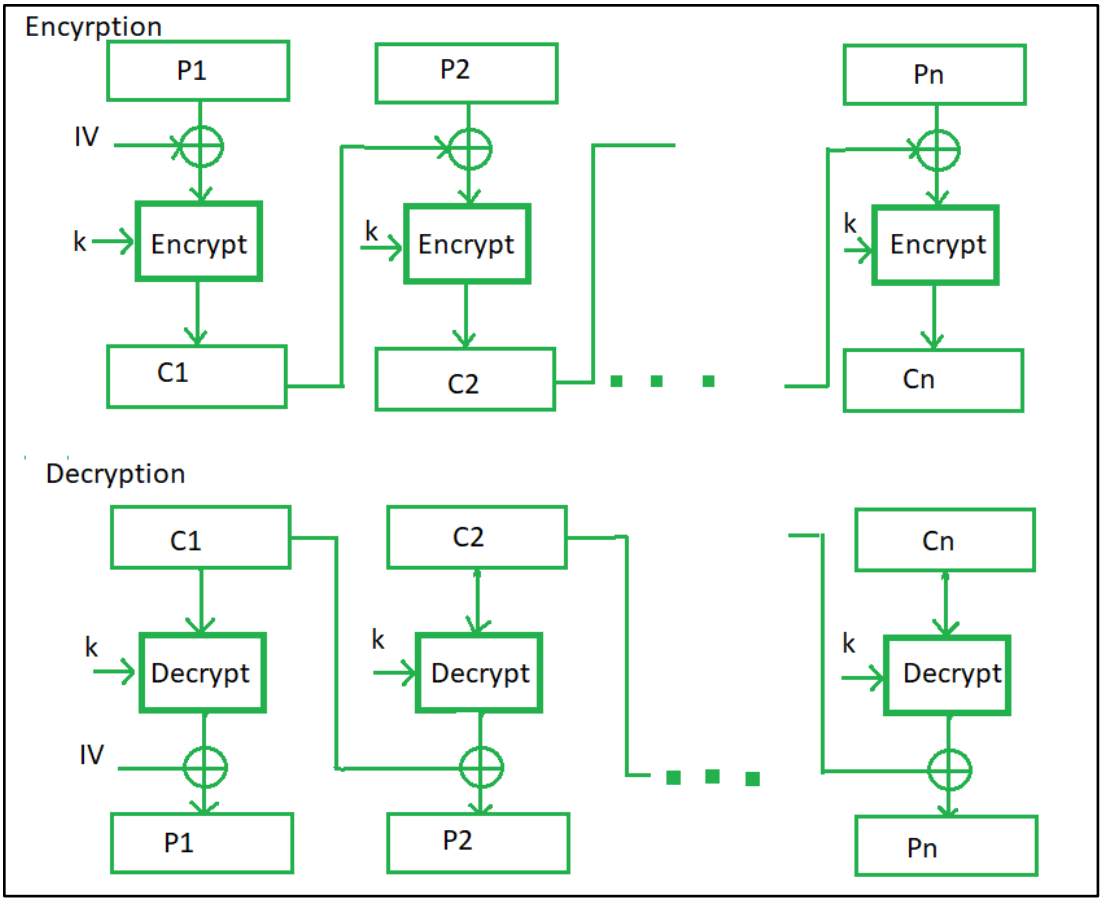
- Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements.
- In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block.
- In a nutshell here, a cipher block is produced by encrypting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

Advantages of CBC –

- CBC works well for input greater than b bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.

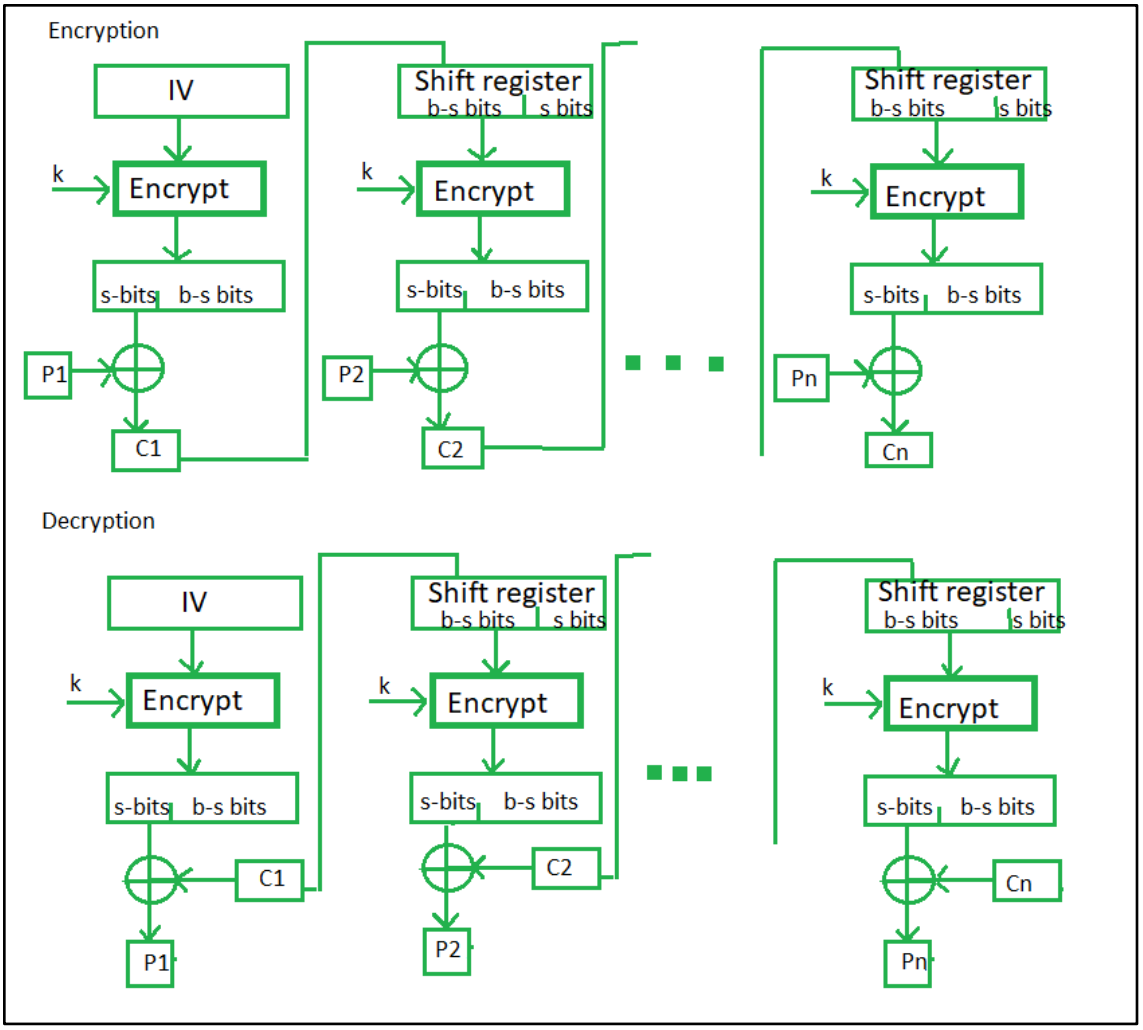
Disadvantages of CBC –

- Parallel encryption is not possible since every encryption requires a previous cipher.



Cipher Feedback Mode:

- 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.
- **Advantages of CFB –**
  - Since, there is some data loss due to the use of shift register, thus it is difficult for applying cryptanalysis.
- **Disadvantages of using CFB –**
  - The drawbacks of CFB are the same as those of CBC mode. Both block losses and concurrent encryption of several blocks are not supported by the encryption. Decryption, however, is parallelizable and loss-tolerant.



Output Feedback Mode:

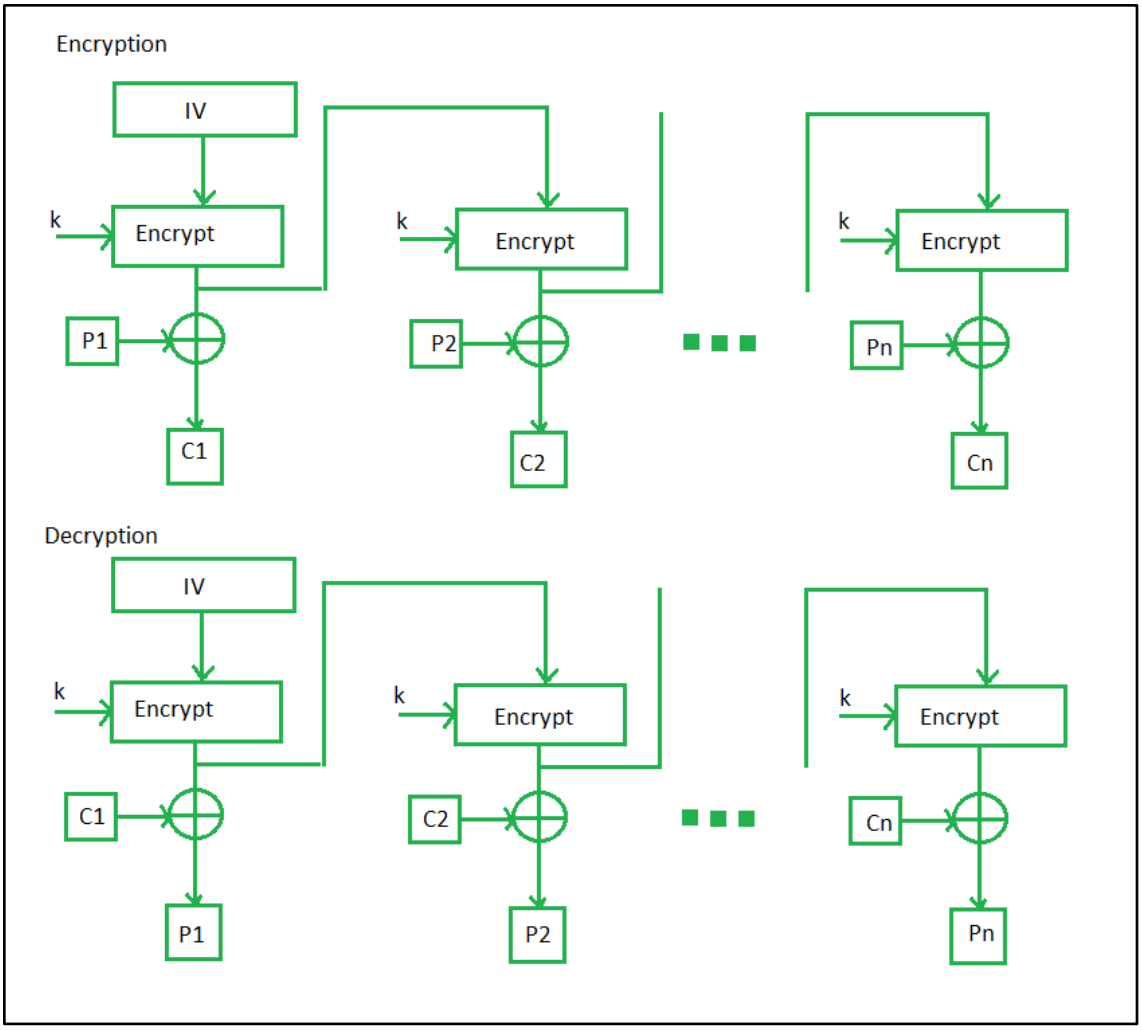
- The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output.
- In this output feedback mode, all bits of the block are sent instead of sending selected s bits.
- The Output 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.

Advantages of OFB –

- In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.

Disadvantages of OFB-

- The drawback of OFB is that, because to its operational modes, it is more susceptible to a message stream modification attack than CFB.



Counter Feedback Mode:

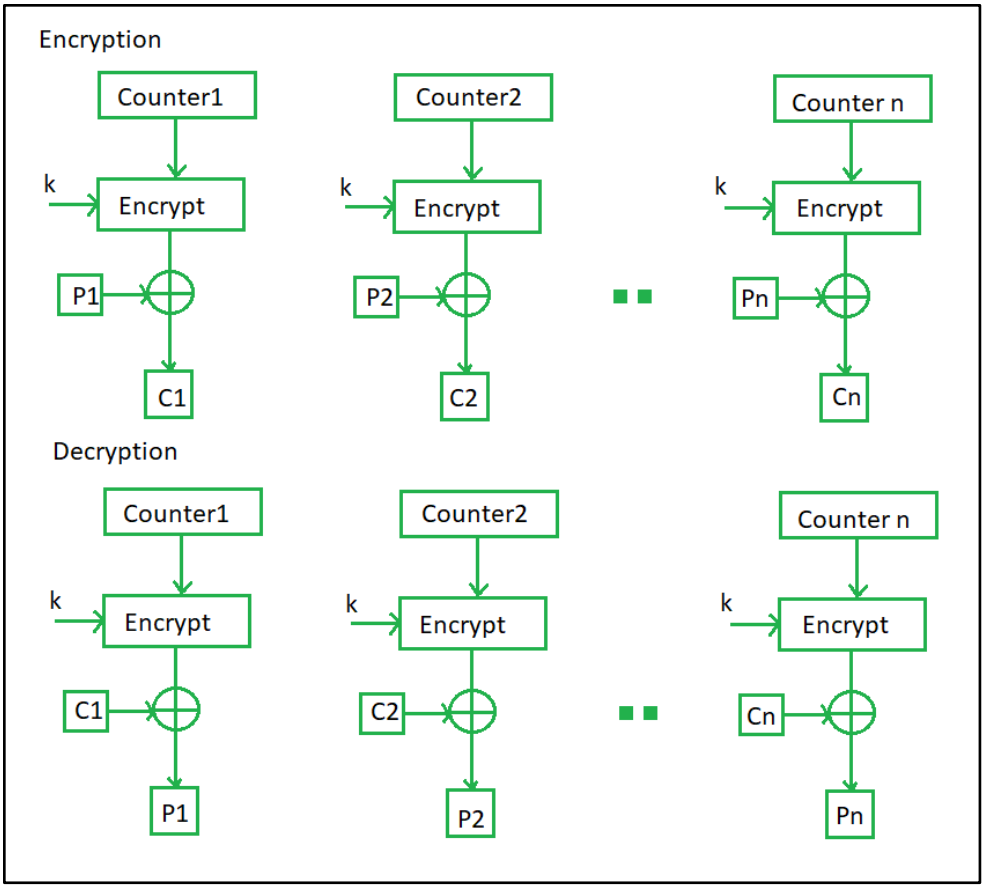
- The Counter Mode or CTR is a simple counter-based block cipher implementation.
- Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in a ciphertext block.
- The CTR mode is independent of feedback use and thus can be implemented in parallel.

Advantages of Counter –

- Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plain text can map to different ciphertext.
- Parallel execution of encryption is possible as outputs from previous stages are not chained as in the case of CBC.

Disadvantages of Counter-

- The fact that CTR mode requires a synchronous counter at both the transmitter and the receiver is a severe drawback. The recovery of plaintext is erroneous when synchronization is lost.



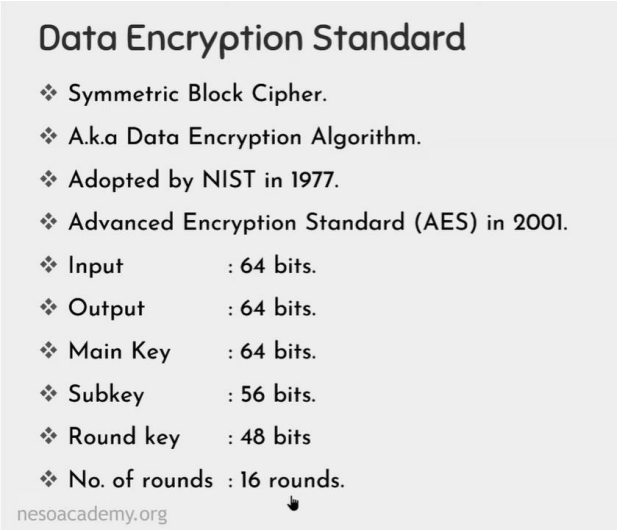
For Applications refer this table:

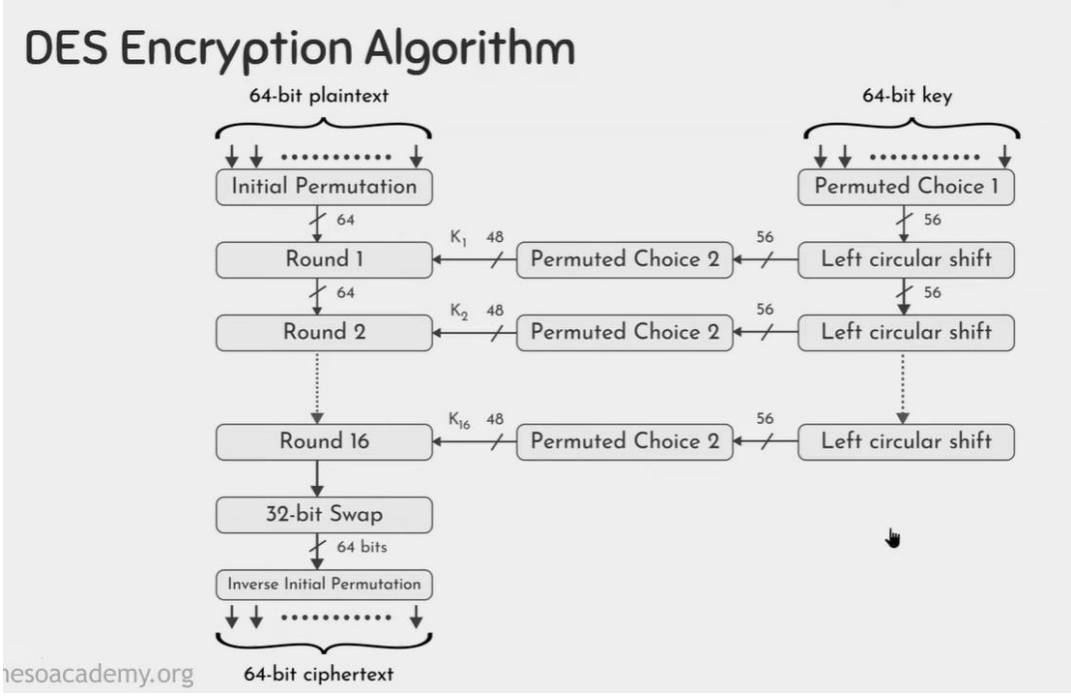
Table 7.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

2. Explain des

- The Data Encryption Standard (DES) was the most widely used encryption scheme.
- DES was issued in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard.
- It is a Symmetric Block Cipher.
- The algorithm is also referred to as the Data Encryption Algorithm (DEA).
- It was redundant after the invasion of Advanced Encryption Standard (AES) in 2001.
- For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.



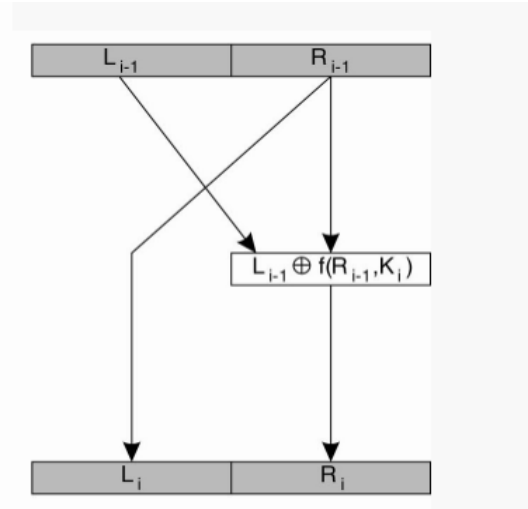


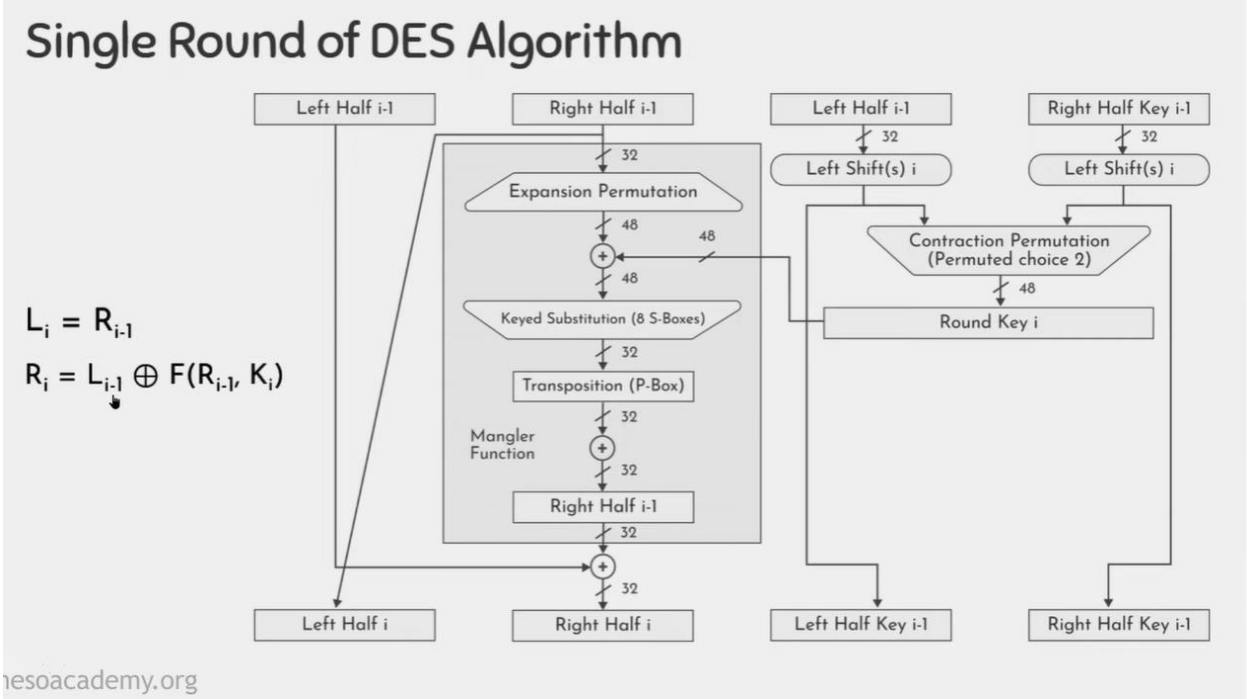
- The overall scheme for DES encryption is illustrated in Figure 4.5. As with any encryption scheme, there are two inputs to the encryption function: the plaintext

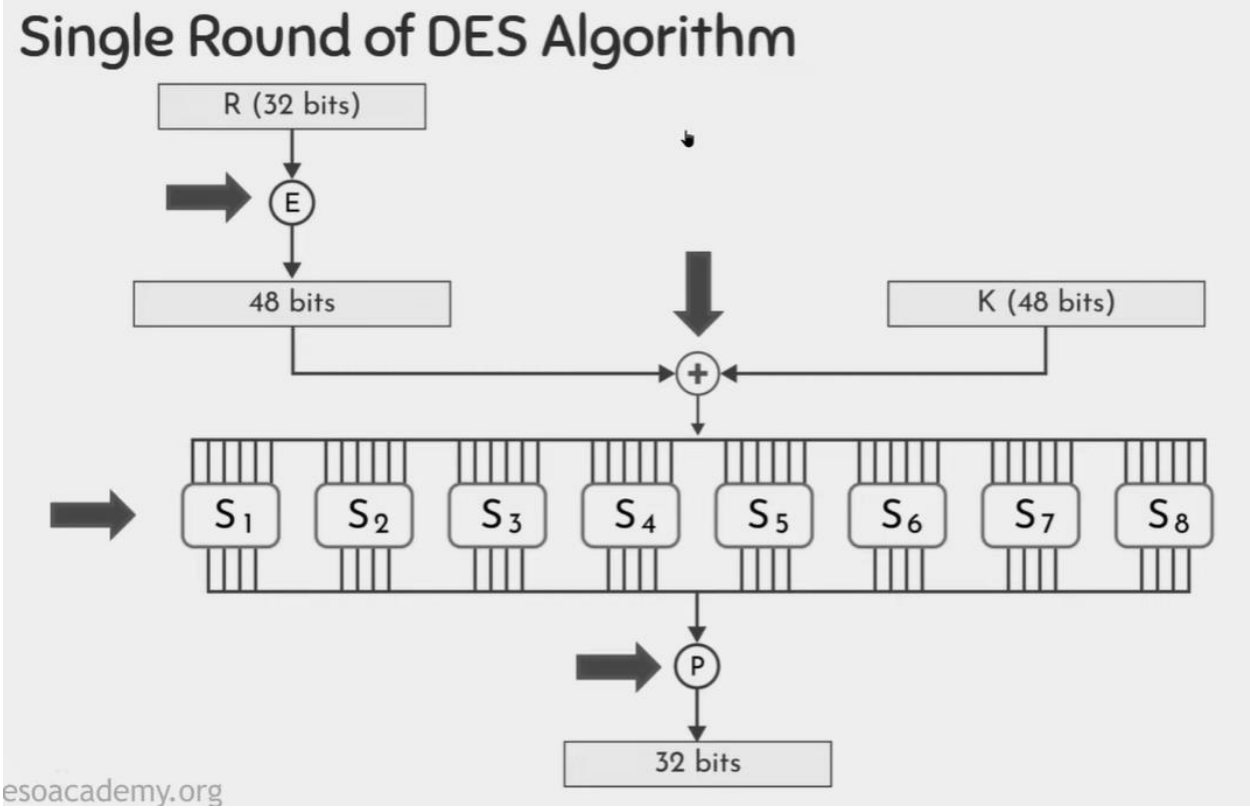
to be encrypted and the key.

- In this case, the plaintext must be 64 bits in length and the key is 56 bits in length. Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases.
- First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
- This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.
- The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the pre output.
- As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed. Additionally, the initial and final permutations are reversed
- Finally, the pre output is passed through a permutation [IP-1] that is the inverse of the initial permutation function, to produce the 64-bit ciphertext. With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher, as shown in Figure 4.3
- The right-hand portion of Figure 4.5 shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function.
- Then, for each of the sixteen rounds, a subkey (Ki) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

FOR EACH ROUND:





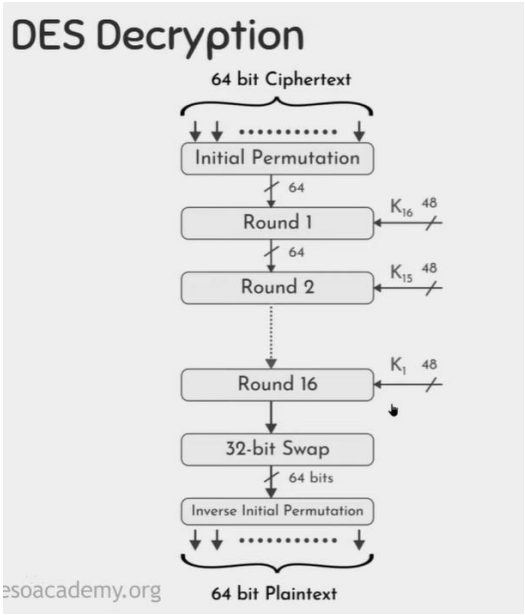


- Each encryption round i takes the 64-bit block produced by the previous round i - 1 as its input.
- The 64 bits are split into a left part Li-1 and a right part Ri-1, each containing 32 bits.
- The right part is used for the left part in the next round, that is, Li = Ri-1.

WORKING OF MANGLER FUNCTION:

Work is done in the mangler function f.

- This function takes a 32-bit block Ri-1 as input, together with a 48-bit key Ki, and produces a 32-bit block that is XORed with Li-1 to produce Ri.
- The mangler function first expands Ri-1 to a 48-bit block and XORs it with Ki.
- The result is partitioned into eight chunks of six bits each.
    - Each chunk is then fed into a different S-box, which is an operation that substitutes each of the 64 possible 6-bit inputs into one of 16 possible 4-bit outputs.
- The eight output chunks of four bits each are then combined into a 32-bit value and permuted again.
- In Key generation in the first Step eight Parity bits are dropped i.e 8,16,24,32,40,48,56,64 are dropped to generate an Effective key of 56 bits.
- In Left Circular Shift Li where i refers to Rounds, for
    - i= 1,2,9,16 it is going to have one shift operation
    - & for other rounds it is going to have two shift operations.
- In Permuted Choice we perform Contraction Permutation and generate 48 bit Key by dropping 8 bits again.
- **WEAKNESS IN DES**
    - DES has been proven to be susceptible to Cryptanalysis.
    - 56-bit keys have a keyspace of $2^{56.}$
    - As we know the DES uses a 56 bit key to encrypt any plain text which can be easily cracked by using modern technologies.
    - To prevent this from happening double DES and triple DES were introduced which are much more secure than the original DES because it uses 112 and 168 bit keys respectively.
    - They offer much more security than DES.



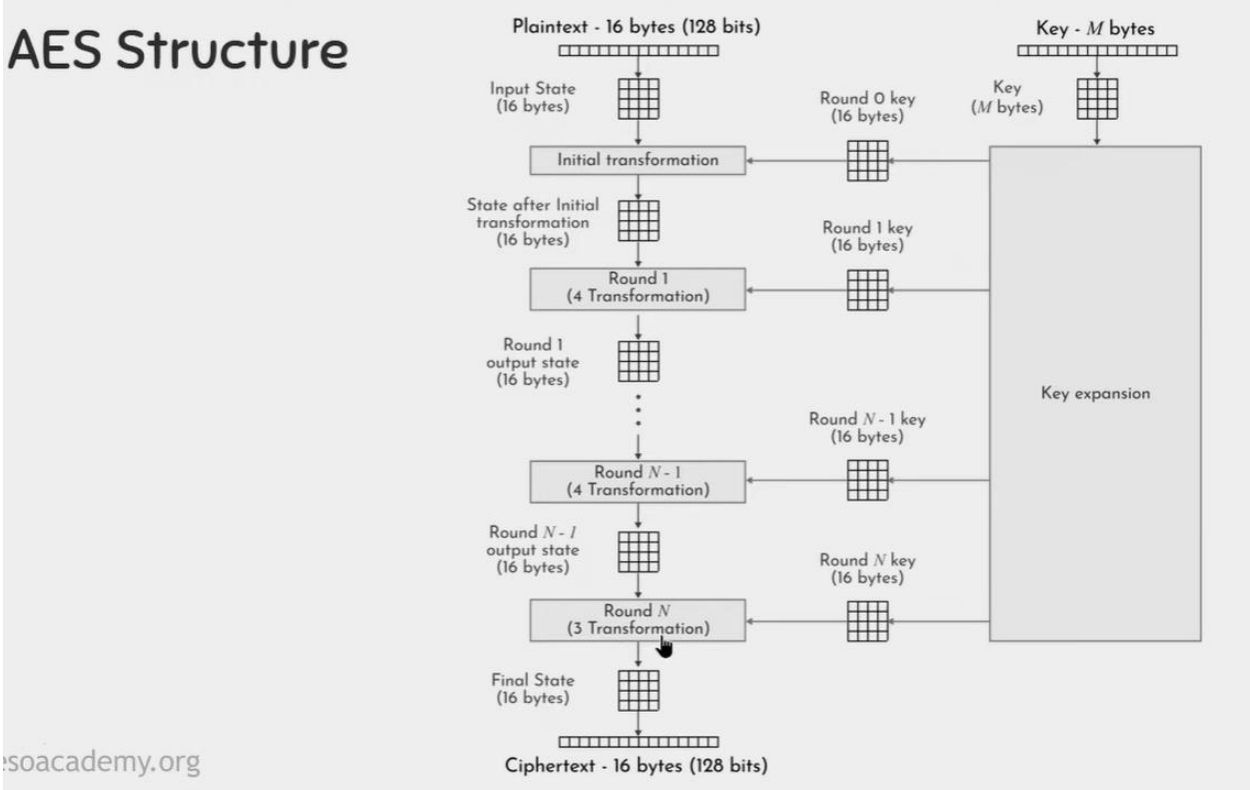
3. Explain aes

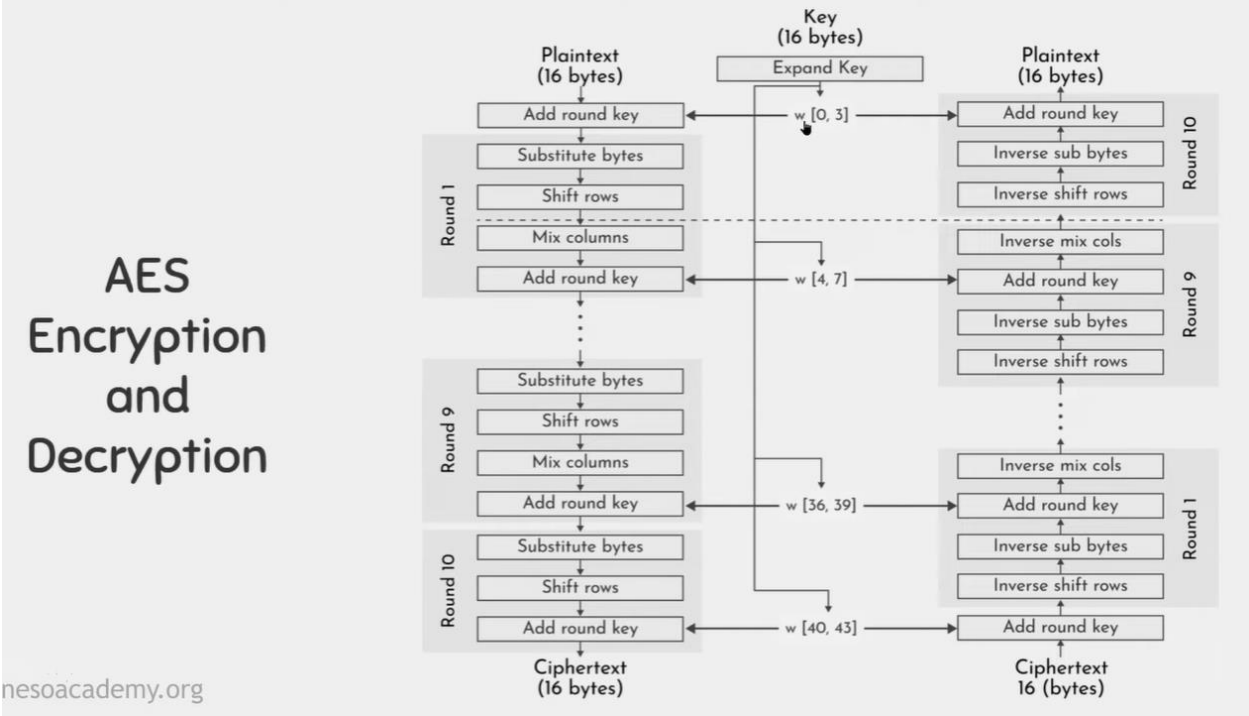
- The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001.

- AES is a symmetric block cipher that is intended to replace DES.
- It can work with three key sizes-128,192,256 bits,
- AES is considered highly secure due to its long key sizes and is still used in industries.
- Based on the key length i.e 16, 24, or 32 bytes (128, 192, or 256 bits),the algorithm is referred to as AES-128, AES-192, or AES-256.

Working of AES

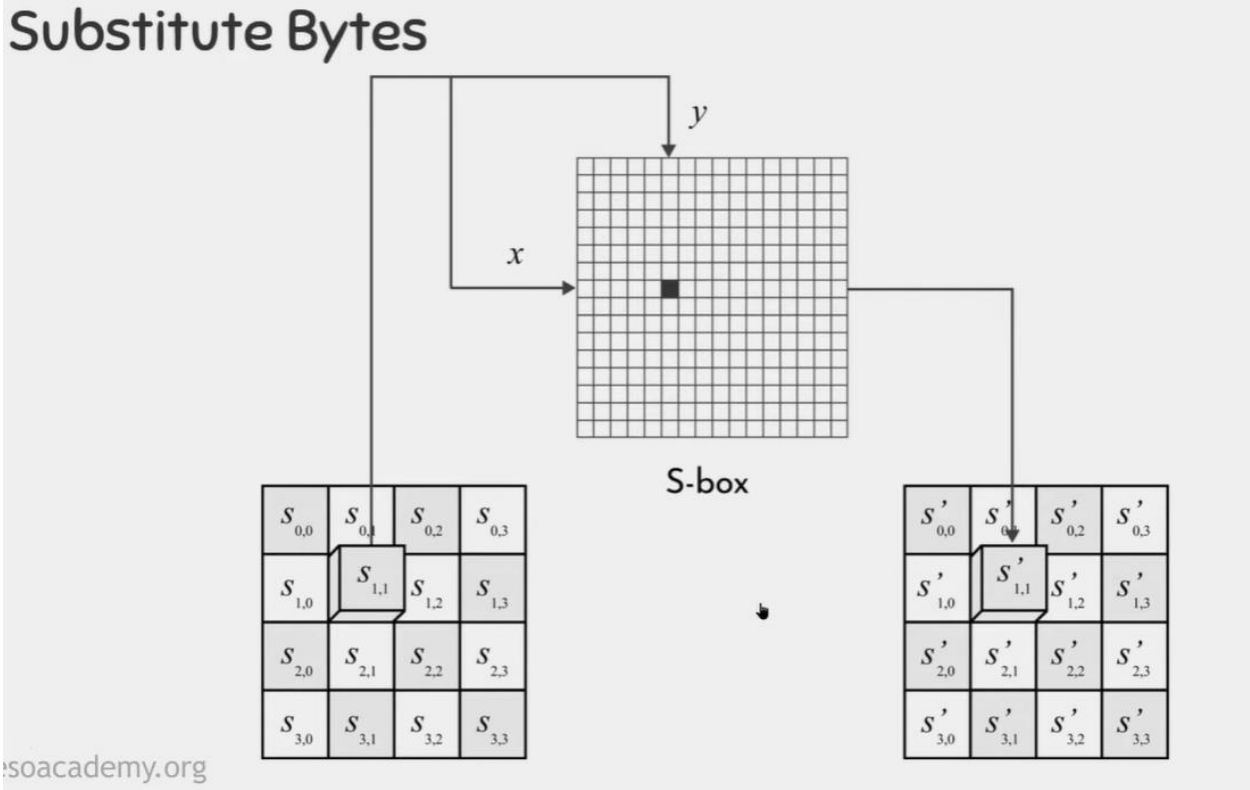
- The cipher takes a plaintext block size of 128 bits, or 16 bytes.
- The input to the encryption and decryption algorithms is a single 128-bit block.
- This block is depicted as a 4 * 4 square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption.
- After the final stage, State is copied to an output matrix.
- Similarly, the key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words. Figure shows the expansion for the 128-bit key. Each word is four bytes, and the total key schedule is 44 words for the 128-bit key.
- The cipher consists of N rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key.
- The first N -1 rounds consist of four distinct transformation functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey, which are described subsequently.
- The final round contains only three transformations, and there is a initial single transformation (AddRoundKey) before the first round, which can be considered Round 0.



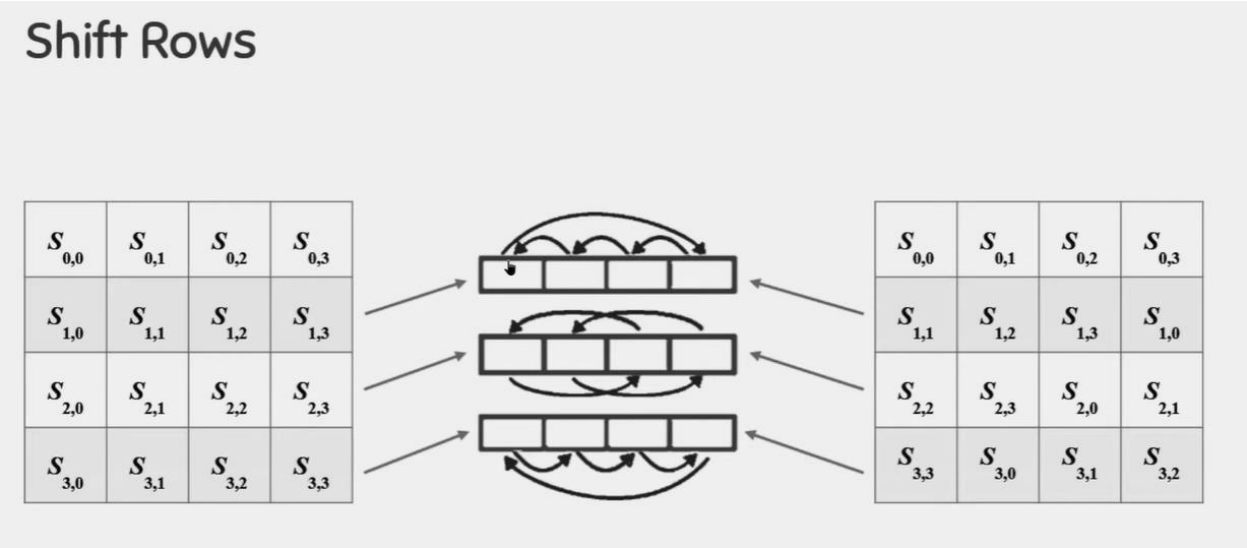


Four different stages are used, one of permutation and three of substitution:

1. **Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block.**
    - AES defines a 16 * 16 matrix of byte values, called an S-box (Table 6.2a), that contains a permutation of all possible 256 8-bit values.
    - Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value.
    - These row and column values serve as indexes into the S-box to select a unique 8-bit output value.
    - For example, the hexadecimal value {95} references row 9, column 5 of the S-box, which contains the value {2A}. Accordingly, the value {95} is mapped into the value {2A}.

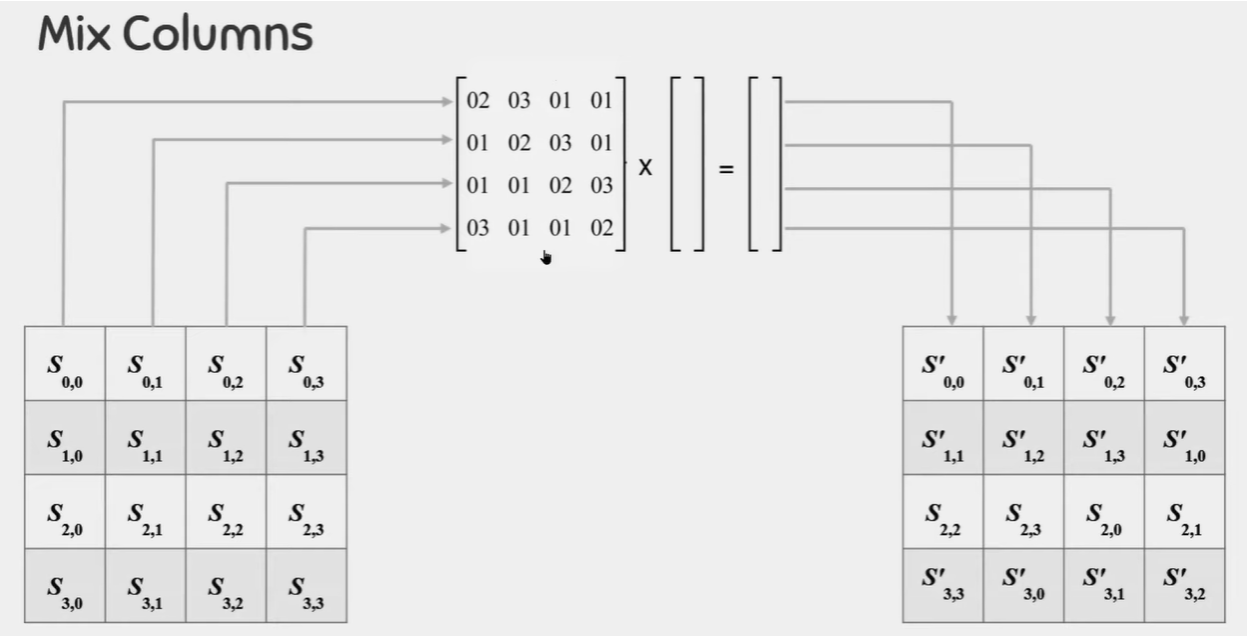


2. **ShiftRows: A simple permutation.**
   The first row of State is not altered. For the second row, a1- byte circular left shift is performed. For the third row, a2- byte circular left shift is performed. For the fourth row, a3- byte circular left shift is performed. The following is an example of Shift Rows:

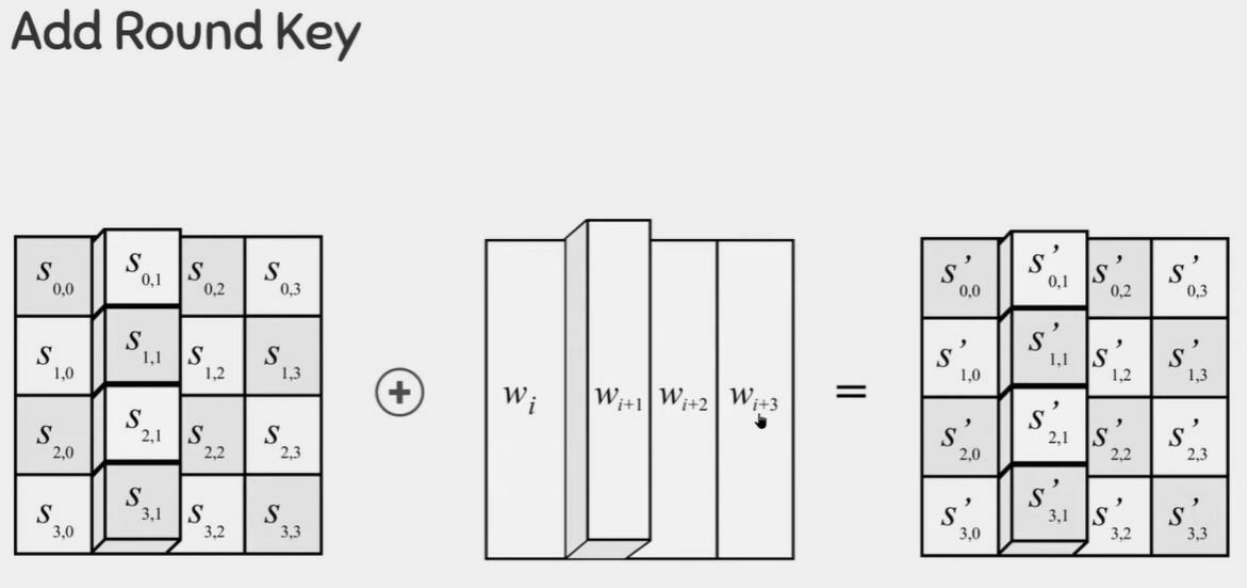


3. **MixColumns: A substitution that makes use of arithmetic over GF(28).**

Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The transformation can be defined by the following matrix multiplication on State



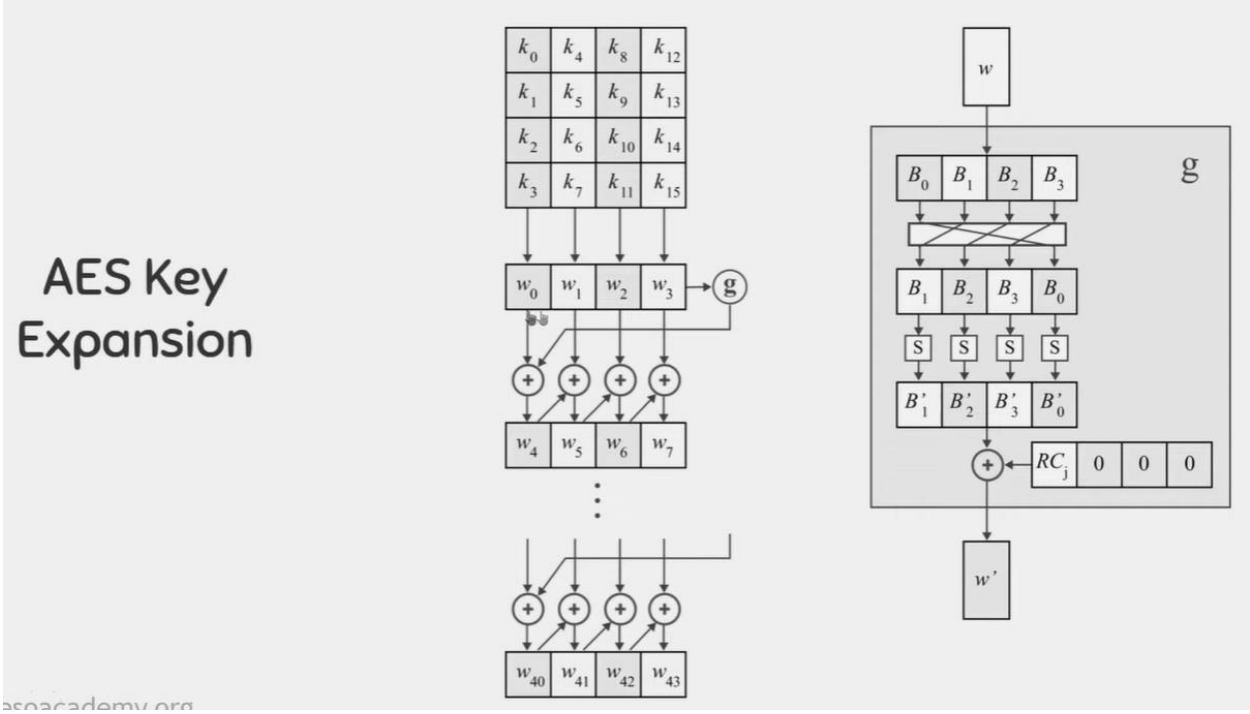
4. **AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key.**
   In AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key.



- **AES Key Expansion:**
  The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a

fourword round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher.

- RotWord performs a one-byte circular left shift on a word. This means that an input word [B0, B1, B2, B3] is transformed into [B1, B2, B3, B0].
- SubWord performs a byte substitution on each byte of its input word, using the S-box (Table 6.2a).
- The result of steps 1 and 2 is XORed with a round constant, Rcon[j].
- The round constant is a word in which the three rightmost bytes are always 0. [Rcon[j] = (RC[j], 0, 0, 0)]



4. Compare aes and des

Basis For Comparison	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)
Basic	The data block in **DES** is split into two halves.	The entire block in **AES** is processed as a single matrix.
Principle	It works on ***Feistel Cipher structure.***	The **substitution** and **permutation** principles are used in AES.
Year of Creation	**DES *(Data Encryption Standard)*** creation year is **1976.**	**AES (Advanced Encryption Standard)** creation year is **1999.**
Designed By	DES (Data Encryption Standard) was designed by **IBM.**	AES (Advanced Encryption Standard) was designed by **Vincent Rijmen** and **Joan Daeman.**
Rounds	16 rounds	10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo
Speed	DES is slower than AES.	AES is faster than DES.
Security	Because DES uses a smaller key, it is ***less secure.***	Because AES uses a large secret key, it is ***more secure.***
Key size	In comparison to **AES,** the key size of **DES** is lower.	In comparison to **DES, AES** has a larger key size,
Rounds Names	Expansion Permutation, Xor, S-box, P-box, Xor and Swap.	Subbytes, Shiftrow, Mix columns, Add roundkeys.
Plaintext	Plaintext is of **64 bits.**	Plaintext can be of **128,192,** or **256** bits.
Identified Attacks	Linear crypt-analysis, Differential crypt-analysis, and Brute-force.	There is no identified attack.
Block Size	128 bits	64 bits
Originate From	DES originate from the Lucifer cipher.	AES originate from the square cipher.

	AES	DES
1.	AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
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 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.
15.	No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective.	Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.
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.

5. Explain hashing along with its applications and properties

- Hash functions are extremely useful and appear in almost all information security applications.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.
- A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just "hash."
- Values returned by a hash function are called message digest or simply hash values.
- A hash function is a versatile one-way cryptographic algorithm that maps an input of any size to a unique output of a fixed length of bits.
- When you hash data, the resulting digest is typically smaller than the input that it started with.
- With hashing, it doesn't matter if you have a one-sentence message or an entire book — the result will still be a fixed-length chunk of bits

  Process of hashing-

  1. Create Information
  2. Calculate the Hash Value
  3. Encrypt the message
  4. Send the Encrypted message and the Hash Value
  5. Receive the Encrypted message and the Hash Value
  6. Decrypt the message
  7. Calculate its hash value at the receiving end
  8. Compare the hashes
  9. If matched, Process the information, else reject.

The typical features of hash functions are –

1. **Fixed Length Output Hash Value:** Hash function converts data of arbitrary length to a fixed length. This process is often referred to as hashing the data. In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions. Since a hash is a smaller representation of a larger data, it is also referred to as a digest. Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits.

2. **Efficiency of Operation:** Generally for any hash function h with input x, computation of hx is a fast operation. Computationally hash functions are much faster than a symmetric encryption.

3. **Pseudorandomness:** Means that it is difficult to predict in which order the iteration will visit each object, though there is no actual randomness.

4. **Pre-Image Resistance (One way Function):** This property means that it should be computationally hard to reverse a hash function. In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z. This property protects against an attacker who only has a hash value and is trying to find the input.

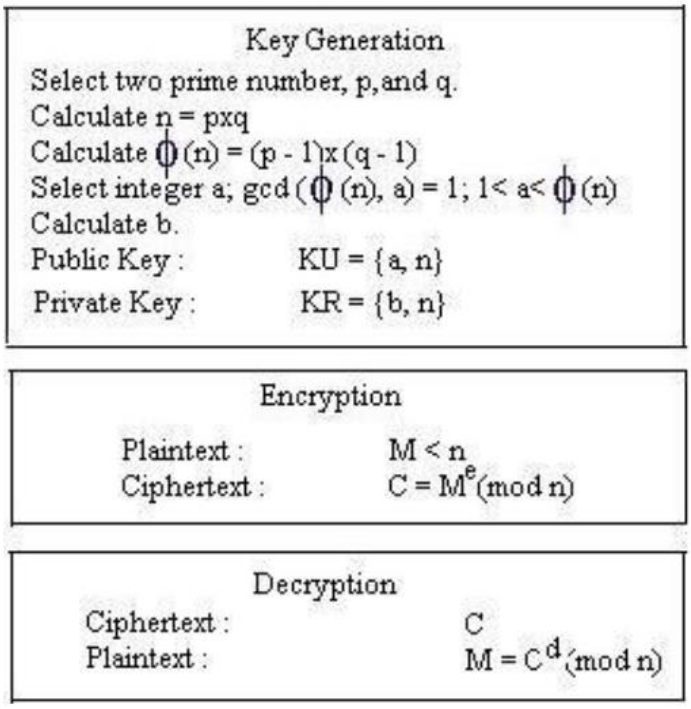
5. **Second Pre-Image Resistance:** This property means given an input and its hash, it should be hard to find a different input with the same hash. In other words, if a hash function h for an input x produces hash value hx, then it should be difficult to find any other input value y such that hy = hx. This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

6. **Collision Resistance:** This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function. In other words, for a hash function h, it is hard to find any two different inputs x and y such that hx = hy. Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find. This property makes it very difficult for an attacker to find two input values with the same hash.

6. Explain rsa algo:

- One of the first successful responses to the challenge was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978.
- The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.
- The RSA scheme is a cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024.
- RSA makes use of an expression with exponentials.

RSA Algorithm



b= a x b = 1 mod Φ(n)

SECURITY OF RSA:

Five possible approaches to attacking the RSA algorithm are

1. **Brute force:** This involves trying all possible private keys.
2. **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.
3. **Timing attacks:** These depend on the running time of the decryption algorithm.
4. **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm
5. **Hardware fault-based attack:** This involves inducing hardware faults in the processor that is generating digital signatures.

- The defense against the brute-force approach is the same for RSA as for other cryptosystems, namely, to use a large key space. Thus, the larger the number of

bits in d, the better. However, because the calculations involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run.

- THE FACTORING PROBLEM We can identify three approaches to attacking RSA mathematically.

1. Factor n into its two prime factors. This enables calculation of f(n) = (p - 1) * (q - 1), which in turn enables determination of d K e-1 (mod f(n)).
2. Determine f(n) directly, without first determining p and q. Again, this enables determination of d K e-1 (mod f(n)).
3. Determine d directly, without first determining f(n).

- A timing attack is somewhat analogous to a burglar guessing the combination of a safe by observing how long it takes for someone to turn the dial from number to number.
- Countermeasures:

1. Constant exponentiation time: Ensure that all exponentiations take the same amount of time before returning a result. This is a simple fix but does degrade performance.
2. Random delay: Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack. Kocher points out that if defenders don't add enough noise, attackers could still succeed by collecting additional measurements to compensate for the random delays.
3. Blinding: Multiply the ciphertext by a random number before performing exponentiation. This process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack.
    - The basic RSA algorithm is vulnerable to a chosen ciphertext attack (CCA). CCA is defined as an attack in which the adversary chooses a number of ciphertexts and is then given the corresponding plaintexts, decrypted with the target's private key.
    - Thus, the adversary could select a plaintext, encrypt it with the target's public key, and then be able to get the plaintext back by having it decrypted with the private key.
    - A solution can be optimal asymmetric encryption padding (OAEP)

7. Compare hmac and cmac

BASIS	HMAC	CMAC

Algorithm Type	HMAC is based on cryptographic hash functions, such as SHA-256 or SHA-3. It uses a hash function to create a fixed-size hash value from the message and a secret key.	CMAC is based on block ciphers, like AES (Advanced Encryption Standard). It uses a symmetric key to create a MAC value.
Security Properties	HMAC is a widely used and well-regarded construction for message authentication. It provides strong security guarantees, including resistance to collision attacks.	CMAC is also considered secure, but its security is closely tied to the strength of the block cipher used. If the underlying block cipher is secure, CMAC is secure.
Key Usage	HMAC requires a secret key, which must be kept confidential. The same secret key is used for both generating and verifying the MAC.	CMAC also requires a secret key, which is used for both generation and verification of the MAC.
Performance	HMAC is generally faster than CMAC because it operates using hash functions, which are often designed for speed.	CMAC may be slower in comparison, as it involves encryption operations with a block cipher.
Applications	HMAC is commonly used for data integrity verification and authentication in various network protocols and applications, including SSL/TLS, IPsec, and more.	CMAC is often used in applications where encryption is already required, such as in disk encryption systems.

8. Short note on digital signatures

- Informally, a digital signature is a technique for establishing the origin of a particular message in order to settle later disputes about what message (if any) was sent.
- The purpose of a digital signature is thus for an entity to bind its identity to a message.

- We use the term signer for an entity who creates a digital signature, and the term verifier for an entity who receives a signed message and attempts to check whether the digital signature is "correct" or not.
- Digital signatures have many attractive properties and it is very important to understand exactly what assurances they provide and what their limitations are.

Digital signatures Security Requirements:

- We will define a digital signature on a message to be some data that provides:
- Data origin authentication of the signer
    - A digital signature validates the message in the sense that assurance is provided about the integrity of the message and of the identity of the entity that signed the message.
- Non-repudiation
    - A digital signature can be stored by anyone who receives the signed message as evidence that the message was sent and of who sent it. This evidence could later be presented to a third party who could use the evidence to resolve any dispute that relates to the contents and/or origin of the message.

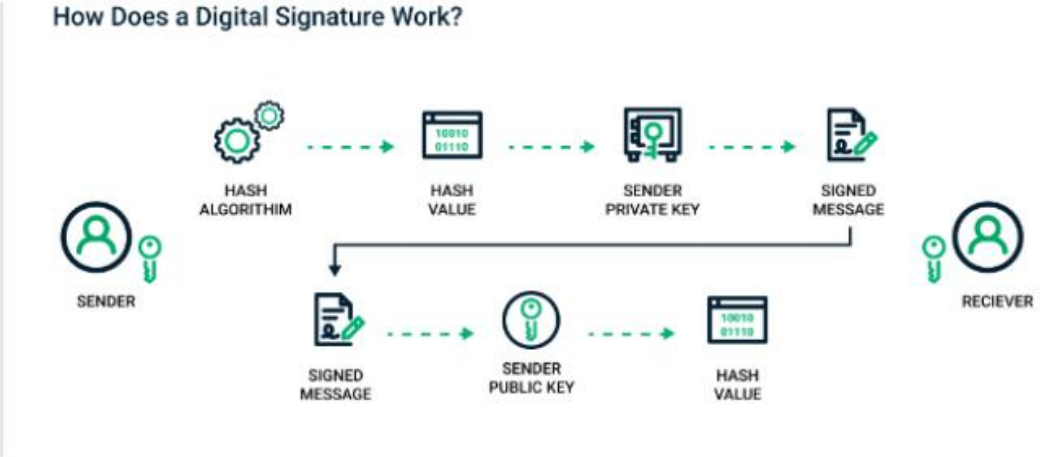
Properties of a Digital Signature

- Easy for the signer to sign a message
    - There is no point point in having a digital signature scheme that involves the signer needing to use slow and complex operations to compute a digital signature.
- Easy for anyone to verify a message
    - Similarly we would like the verification of a digital signature to be as efficient as possible.
- Hard for anyone to forge a digital signature
    - It should be practically impossible for anyone who is not the legitimate signer to compute a digital signature on a message that appears to be valid. By "appears to be valid" we mean that anyone who attempts to verify the digital signature is led to believe that they have just successfully verified a valid digital signature on a message.

How it Works?

- A Digital Signature Scheme will have two components, a private signing algorithm which permits a user to securely sign a message and a public verification algorithm which permits anyone to verify that the signature is authentic.
- The signing algorithm needs to "bind" a signature to a message in such a way that the signature cannot be pulled out and used to sign another document, or have the original message modified and the signature remain valid.

- For practical reasons it would be necessary for both algorithms to be relatively fast and if small computers such as smart cards are to be used, the algorithms can not be too computationally complex.



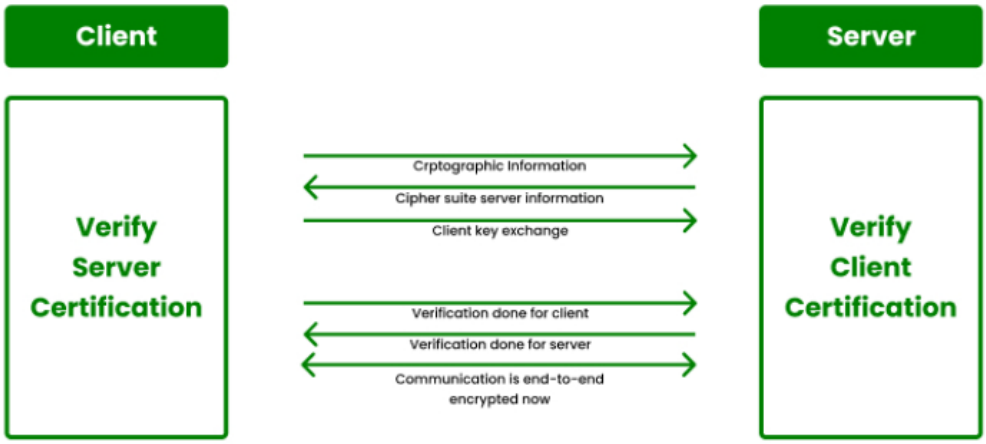
Here is how sending a digital signature works:

1. The sender selects the file to be digitally signed in the document platform or application,
2. The sender's computer calculates the unique hash value of the file content.
3. This hash value is encrypted with the sender's private key to create the digital signature.
4. The original file along with its digital signature is sent to the receiver
5. The receiver uses the associated document application, which identifies that the file has been digitally signed
6. The receiver's computer then decrypts the digital signature using the sender's public key

9. Ssl handshake

The SSL and TLS handshake establishes a system for SSL/TLS clients and servers to start communication between them in other words it is a negotiation between two parties on a network. Handshake Protocol is used to establish sessions. This protocol allows the client and server to verify each other by transferring a series of messages to each distance. Handshake protocol uses four phases to finalize its circle.

Steps enable the SSL or TLS client and server to communicate with each other:



Phase-1: Deciding which version of the Protocol to use. The system decides which protocol to use. Client and Server exchange hello-packets with each other to confirm. In this IP session, cipher suite, and Agree on which version of the protocol to use.

Phase-2: Server sends his certificate and Server-key-exchange. The server end phase-2 by exchanging the hello packet.

Phase-3: Verification, in this phase, the Client replies to the server by sending his certificate and Client-exchange-key.

Phase-4: In this phase, the Change Cipher suite is passed and all the verifications and security checks are done after this Handshake Protocol ends.

10. Digital certificate 8.509

- X.509 is a digital certificate that is built on top of a widely trusted standard known as ITU or International Telecommunication Union X.509 standard, in which the format of PKI certificates is defined.
- X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information. These are primarily used for handling the security and identity in computer networking and internet-based communications.
- 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.
- Once an X.509 certificate is provided to a user by the certified authority, that certificate is attached to it like an identity card. The chances of someone stealing it or losing it are less, unlike other unsecured passwords. With the help of this analogy, it is easier to imagine how this authentication works: the certificate is basically presented like an identity at the resource that requires authentication.

Generally, the certificate includes the elements given below:

- **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.

Module 3:

1. Define malware.

- Malware is short form for malicious software.
- It is a software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- It can appear in the form of code, scripts, active content, and other software.
- Malware is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software.
- Malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general. However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

(for examples you can refer Q.2,3,4,5,6 and expand the answer and also the ppt)

2. Short note on backdoors.

- In cybersecurity terms, a Backdoor Attack is an attempt to infiltrate a system or a network by maliciously taking advantage of software's weak point.
- Backdoors allow the attackers to quietly get into the system by deceiving the security protocols and gain administrative access. It is similar to the real-life robbery in which burglars take advantage of the loopholes in a house and get a 'backdoor' entry for conducting the theft.
- After gaining high-level administrative privilege, the cyber attackers could perform various horrendous tasks like injecting spyware, gaining remote access, hack the device, steal sensitive information, encrypt the system through ransomware, and many more.

- Backdoors are originally meant for helping software developers and testers, so they are not always bad.
- Types of Backdoor:

1. **Administrative Backdoor:**
    - Sometimes software developers intentionally leave a backdoor into the program so that in case of any failure or error, they can easily reach the core of the software's code and quickly solve the issue.
    - Such Backdoors are called the Administrative Backdoors.
    - These deliberate Backdoors can also help the software testers to testify the codes.
    - Though such Backdoors are only known to the developers, a skillful hacker can take advantage of it and silently use it for his benefit.
    - So Administrative Backdoor can be called a type of loophole in the program.
2. **Malicious Backdoor:**
    - Malicious Backdoors are the backdoors installed on the system by cybercriminals using malware programs like Remote Access Trojan (RAT). These are specifically designed for taking control of the system or network and conduct malicious tasks.
    - RAT is a malware program that can reach the root of the system and install the backdoor.
    - RAT is generally spread through a malicious program.

3. Rootkits:

- Rootkits are malicious software that gives hackers the full administrator rights of your PC.
- It helps hackers in changing or altering the system settings or files the way an administrator could do. It creates a backdoor for other users to log in and provides full access to the system.
- The rootkit is derived from two words Root and Kit. The **Root** is referred to as a full access user account in the Unix based operating systems. While the **Kit** word represents a collection of tools. Meaning a collection of tools to access the root account.
- **TYPES OF ROOTKITS-**
    a. **Hardware or firmware rootkit:** The name of this type of rootkit comes from where it is installed on your computer. This type of malware could infect your computer's hard drive or its system BIOS, the software that is installed on a small memory chip in your computer's motherboard. It can even infect your router. Hackers can use these rootkits to intercept data written on the disk.
    b. **Bootloader rootkit:** Your computer's bootloader is an important tool. It loads your computer's operating system when you turn the machine on. A bootloader toolkit, then, attacks this system, replacing your computer's

legitimate bootloader with a hacked one. This means that this rootkit is activated even before your computer's operating system turns on.

c. **Memory rootkit:** This type of rootkit hides in your computer's RAM, or Random Access Memory. These rootkits will carry out harmful activities in the background. The good news? These rootkits have a short lifespan. They only live in your computer's RAM and will disappear once you reboot your system — though sometimes further work is required to get rid of them.

d. **Application rootkit:** Application rootkits replace standard files in your computer with rootkit files. They might also change the way standard applications work. These rootkits might infect programs such as Word, Paint, or Notepad. Every time you run these programs, you will give hackers access to your computer. The challenge here is that the infected programs will still run normally, making it difficult for users to detect the rootkit.

e. **Kernel mode rootkits:** These rootkits target the core of your computer's operating system. Cybercriminals can use these to change how your operating system functions. They just need to add their own code to it. This can give them easy access to your computer and make it easy for them to steal your personal information.

4. Phishing

- Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money.
- As with real fishing, there's more than one way to reel in a victim: Email phishing, smishing, and vishing are three common types.

How the attack works:

- The phisher begins by determining who their targeted victims will be (whether at an organization or individual level) and creates strategies to collect data they can use to attack.
- Next, the phisher will create methods like fake emails or phony web pages to send messages that lure data from their victims.
- Phishers then send messages that appear trustworthy to the victims and begin the attack.
- Once the attack has been deployed, phishers will monitor and collect the data that victims provide on the fake web pages.
- Finally, phishers use the collected data to make illegal purchases or commit fraudulent acts..

TYPES OF PHISHING ATTACKS

- **Email phishing**
  The most common form of phishing, this type of attack uses tactics like

phony hyperlinks to lure email recipients into sharing their personal information. Attackers often masquerade as a large account provider like Microsoft or Google, or even a coworker.

- **Spear phishing**
  Where most phishing attacks cast a wide net, spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customized, making them particularly effective at bypassing basic cybersecurity.
- **Smishing**
  A combination of the words “SMS” and “phishing,” smishing involves sending text messages disguised as trustworthy communications from businesses like Amazon or FedEx. People are particularly vulnerable to SMS scams, as text messages are delivered in plain text and come across as more personal.
- **Vishing**
  In vishing campaigns, attackers in fraudulent call centers attempt to trick people into providing sensitive information over the phone. In many cases, these scams use social engineering to dupe victims into installing malware onto their devices in the form of an app.
- **Whaling**
  When bad actors target a “big fish” like a business executive or celebrity, it’s called whaling. These scammers often conduct considerable research into their targets to find an opportune moment to steal login credentials or other sensitive information. If you have a lot to lose, whaling attackers have a lot to gain.

5. DOS:

- DDoS stands for Distributed Denial of Service. This type of attack involves sending large amounts of traffic from multiple sources to a service or website, intending to overwhelm it.
- Distributed Denial of Service, which is a malicious network attack that involves hackers forcing numerous Internet-connected devices to send network communication requests to one specific service or website with the intention of overwhelming it with false traffic or requests.
- This has the effect of tying up all available resources to deal with these requests, and crashing the web server or distracting it enough that normal users cannot create a connection between their systems and the server.
- DoS stands for Denial of Service. The difference between DoS and DDoS attacks is whether one computer is used in the attack, or the attack is sent from multiple sources.
- DDoS attacks are carried out with networks of Internet-connected machines.

- These networks consist of computers and other devices (such as IoT devices)which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.
- Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.
- When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.
- Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

6. Botnets:

- A botnet is a distributed network consisting of many compromised internet-connected devices, which are controlled by a centralized botmaster, and are utilized to perform synchronized tasks.
- Each infected machine is called a bot, and together their power is used to carry out various attacks.
- The botnet is a network of robots. Developers assign them to commit a malicious task. The handlers of a botnet who controls it are called the **botmaste**r They have access to thousands of devices. They gain access by injecting a Trojan horse or other malware through email, drive-by downloads, or other means.
- Once the botnet carrier enters your device, it would inform the botmaster, and the botmaster would take control of your system.
- For botnets to evolve and become more vigorous, it must connect more and more devices to its network. The more the bots, the bigger the botnet, and the more significant the impact. Take an example. If ten people hit a website simultaneously, it won't be disturbed much. However, if a thousand people hit it simultaneously, the site would get slow, and it may even crash with an increase in number. So size is vital for a botnet.

TYPES OF BOTNET ATTACKS

- **Distributed Denial of Service (DDoS) attacks:** It is the most common executable attack using the network of bots. In a DDOS attack, bots send unusual traffic to the targeted website server. By doing so, intended users can not access the site. The infected bot army overloads the site to such a point that the server gets crashed.If thousands of users visit a website, it will show an access denied error message. Thus, the user won't be able to complete the desired task.

- **Email Spamming:** By using the thousands of devices connected through a botnet, bot herders send emails to millions of people to spam their inboxes with unnecessary ads and offers.
- **Cryptocurrency Mining:** The processing power of thousands of computers can collectively mine cryptocurrency like Bitcoins. Users would not be able to detect that their system's RAM and other resources are in control of a botnet.
- **Ad fraud:** Cybercriminals can use the botnet to run fraud ad clicks by utilizing the processing power of the infected devices. The botmaster would direct all the infected machines to click on ads placed on a website. For every click, they get a small percentage of the advertising fees.
- **Generating Fake Traffic**: Like the fraud ad clicks, a botnet can also generate fake traffic on a third-party website. It is generally used to get unethical financial gains from website visits.
- **Steal Information:**A botnet can steal personal information from the infected devices and transfer those pieces of information to cybercriminals. Further, cybercriminals use this information for carrying out extortion and other illegal activities.
- **Banner and Pop-Up Ads:**Botnet bombards the infected device with intrusive banners and pop-up ads. Pop-up ads are intriguing to trick the user so that they click on them, and malicious programs can enter the system.
- **Botnet Selling and Renting:** After a botnet serves its purpose, cybercriminals can sell or rent it. Other cyber criminals use this robot network to perform notorious tasks.

Module 4:

1. **Explain IPSec**

- IP Security (IPSec) is a collection of protocols which is designed by Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
- Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure." The Internet Protocol is the main routing protocol used on the Internet; it designates where data will go using IP addresses.
- Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. IPSec is a suite of cryptography-based protection services and security protocols.
- IP-level security encompasses three functional areas: authentication, confidentiality, and key management.
- The authentication mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in transit.

- The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
- The key management facility is concerned with the secure exchange of keys.

Applications of IPsec

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

- **Secure branch office connectivity over the Internet:** A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- **Secure remote access over the Internet:** An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.
- **Establishing extranet and intranet connectivity with partners:** IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- **Enhancing electronic commerce security:** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

Some of the benefits of IPsec:

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.
- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

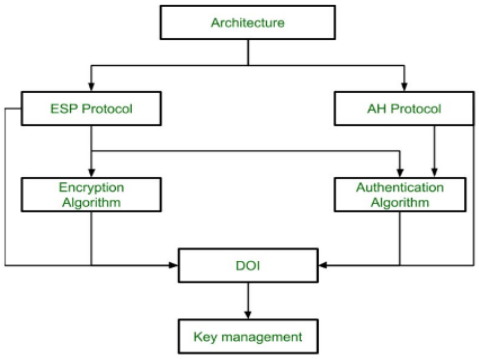
IPSEC ARCHITECTURE

ESP Protocol: ESP(Encapsulation Security Payload) provides a confidentiality service.

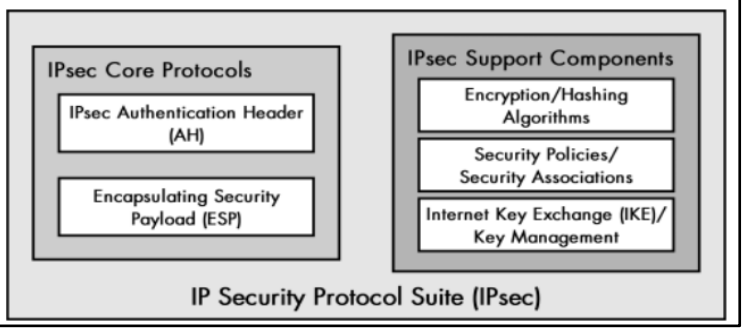
AH Protocol: AH (Authentication Header) Protocol provides both Authentication and Integrity service.

DOI (Domain of Interpretation): DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.

Key Management: Key Management contains the document that describes how the keys are exchanged between sender and receiver. (using ipseckey or **Internet Key Exchange Protocol**)



IPSEC COMPONENTS AND PROTOCOLS



1) Authentication header

IPSec Authentication Header

- This protocol provides authentication services for IPsec. It allows the recipient of a message to verify that the supposed originator of a message was actually fact the one that sent it.
- It also allows the recipient to verify that intermediate devices en route haven't changed any of the data in the datagram.
- It also provides protection against so-called replay attacks, whereby a message is captured by an unauthorized user and resent.
- It provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.

Field Name	Size (Bytes)	Description
Next Header	1	Contains the protocol number of the next header after the AH. Used to link headers together.
Payload Len	1	Despite its name, this field measures the length of the authentication header itself, not the payload. (I wonder what the history is behind that!) It is measured in 32-bit units, with 2 subtracted for consistency with how header lengths are normally calculated in IPv6.
Reserved	2	Not used; set to zeros.
SPI	4	A 32-bit value that, when combined with the destination address and security protocol type (which is obviously the one for AH here), identifies the security association (SA) that will be used for this datagram. (SAs are discussed earlier in this chapter.)
Sequence Number	4	A counter field that is initialized to zero when an SA is formed between two devices, and then incremented for each datagram sent using that SA. This uniquely identifies each datagram on an SA and is used to provide protection against replay attacks by preventing the retransmission of captured datagrams.
Authentication Data	Variable	Contains the result of the hashing algorithm, called the integrity check value (ICV), performed by the AH protocol.

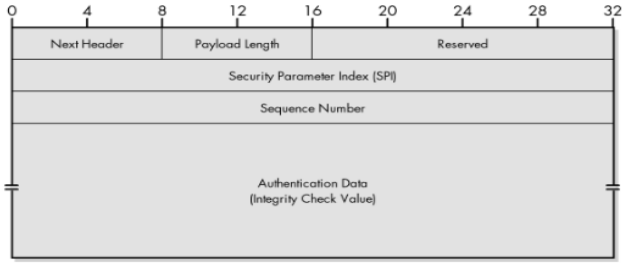


Figure 29-8: *IPsec Authentication Header (AH) format*

IPSec Authentication Header

- It uses a special hashing algorithm and a specific key known only to the source and the destination.
- An SA between two devices specifies these particulars, so that the source and destination know how to perform the computation but nobody else can.
- On the source device, AH performs the computation and puts the result (called the integrity check value, or ICV) into a special header with other fields for transmission.
- The destination device does the same calculation using the key that the two devices share. This enables the device to see immediately if any of the fields in the original datagram were modified

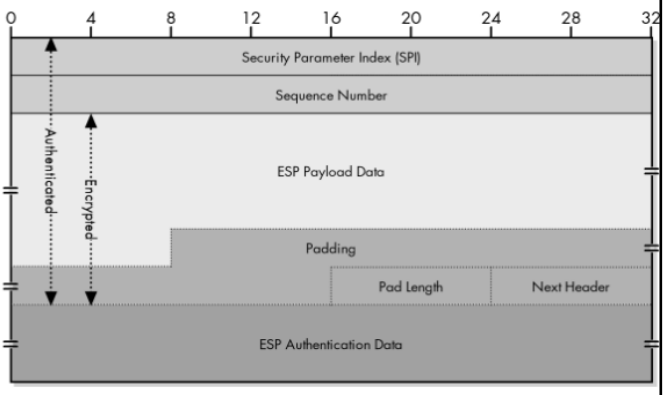
2) ESP

IPsec Encapsulating Security Payload (ESP)

- The IPsec AH provides integrity authentication services to IPsec-capable devices so that they can verify that messages are received intact from other devices. For many applications, however, this is only one piece of the puzzle.
- We want to not only protect against intermediate devices changing the datagrams, but also to protect against them examining their contents as well.
- For this level of private communication, AH is not enough; we need to use the ESP protocol.
- The main job of ESP is to provide the privacy we seek for IP datagrams by encrypting them.
- An encryption algorithm combines the data in the datagram with a key to transform it into an encrypted form.
- This is then repackaged using a special format that you will see shortly, and then transmitted to the destination, which decrypts it using the same algorithm

Table 29-3: IPsec Encapsulating Security Payload (ESP) Format

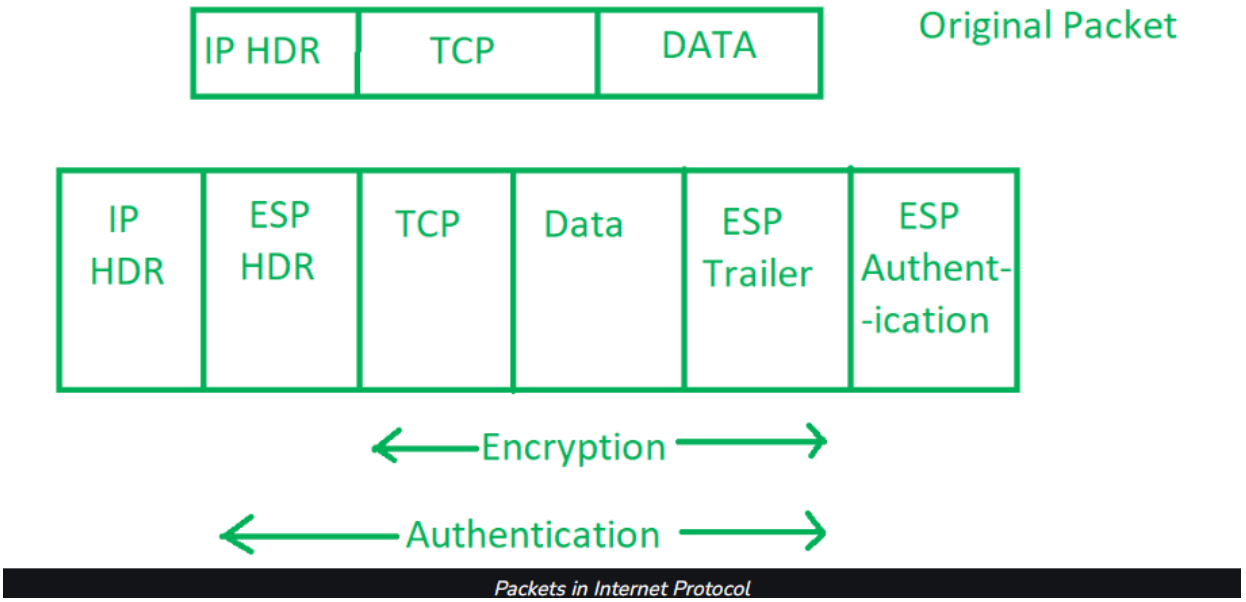
Section	Field Name	Size (Bytes)	Description	Encryption Coverage	Authentication Coverage
ESP Header	SPI	4	A 32-bit value that is combined with the destination address and security protocol type to identify the SA that will be used for this datagram. (SAs are discussed earlier in this chapter.)		
	Sequence Number	4	A counter field initialized to zero when an SA is formed between two devices, and then incremented for each datagram that's sent using that SA. This is used to provide protection against replay attacks.		
Payload	Payload Data	Variable	The encrypted payload data, which consists of a higher-layer message or encapsulated IP datagram. It may also include support information such as an initialization vector that's required by certain encryption methods.		
ESP Trailer	Padding	Variable (0 to 255)	Additional padding bytes are included as needed for encryption or for alignment.		
	Pad Length	1	The number of bytes in the preceding Padding field.		
	Next Header	1	Contains the protocol number of the next header in the datagram. Used to chain together headers.		
ESP Authentication Data		Variable	Contains the ICV resulting from the application of the optional ESP authentication algorithm.		



3) Internet Key Exchange (IKE) protocol

- It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.
- The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.

- The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec.
- 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.
- Packets that are not authorized are discarded and not given to the receiver.



Packets in Internet Protocol

Next page cha part ppt madhla ahe above theory & diagram and tyat kahi correlation nahiye!!!.

There are two phases to this negotiation process:

1. IKE Phase 1 establishes the initial tunnel (referred to as the IKE or ISAKMP SA). Peers are authenticated, encryption and hashing algorithms are negotiated, and keys are exchanged based on the IKE Policy Sets.
   Two modes can be used for Phase 1 negotiation: • Main Mode – slower, but more secure • Aggressive Mode – faster, but less secure
2. IKE Phase 2 establishes the IPSEC tunnel (IPSEC SA), which details the AH or ESP parameters for securing data.
   These parameters are contained in an IPSEC Transform Set.
   IKE Phase 1 negotiates parameters for the tunnel (key exchange) itself, while IKE Phase 2 negotiates parameters for the data traversing that tunnel.
   OAKLEY Key Determination Protocol is used for establishing shared key with an assigned identifier and associated authenticated identities of the two communicating parties.

Advantages of IPSec

1. Strong security: IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
2. Wide compatibility: IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
3. Flexibility: IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
4. Scalability: IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
5. Improved network performance: IPSec can help improve network performance by reducing network congestion and improving network efficiency.

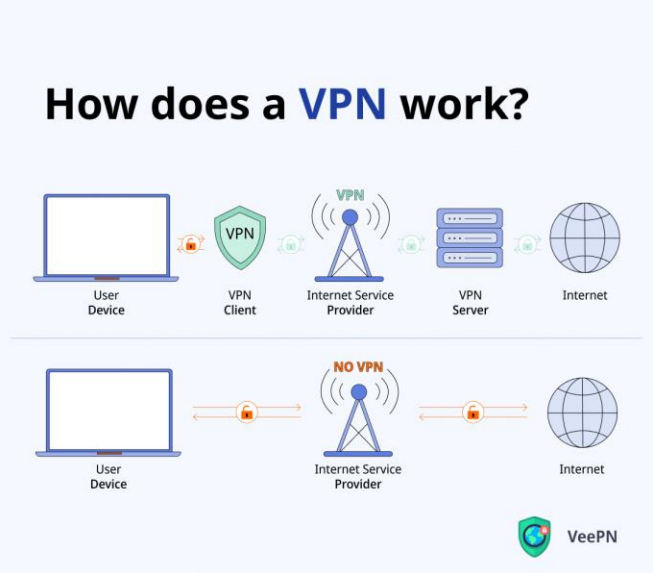
Disadvantages of IPSec

1. Configuration complexity: IPSec can be complex to configure and requires specialized knowledge and skills.
2. Compatibility issues: IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
3. Performance impact: IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
4. Key management: IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
5. Limited protection: IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

2. **Short note on vpn**
    - A virtual private network (VPN) is a framework that consists of multiple remote peers transmitting private data securely to one another over an otherwise public infrastructure (generally a shared IP backbone), such as the Internet.
    - In this framework, inbound and outbound network traffic is protected by using tunnels that encrypt all data at the IP level.
    - The framework permits networks to extend beyond their local topologies while providing remote users with the appearance and features of a direct network connection.
    - Typically, remote peers (sites and users) are connected to the central site over a shared infrastructure in a hub-and-spoke topology, although it is possible to configure remote access VPNs in two other ways. These other configurations are called "full mesh" and "partial mesh." Performance Monitor supports all of these VPN types.
    - **Working Principle of VPN**
    - The working principle of a VPN involves creating a secure and encrypted connection between the user's device and a VPN server. This connection

is created using a combination of encryption protocols and network protocols.

- When a user connects to a VPN, their device sends a request to the VPN server to establish a secure connection. The VPN server responds by sending the user's device a set of encryption keys, which are used to encrypt all data that is transmitted between the device and the VPN server.
- Once the connection has been established, all data that is transmitted between the user's device and the VPN server is encrypted using the encryption keys. This means that even if a hacker intercepts the data, they will not be able to read it.
- In addition to encryption, a VPN also uses network protocols to ensure that the data is transmitted securely. The most common network protocol used by VPNs is the Internet Protocol Security (IPsec) protocol. IPsec provides a set of security protocols that ensure the integrity, confidentiality, and authenticity of the data that is transmitted over the internet.



There are mainly three types of VPN. They are –

1. **Remote Access VPN:** A remote access VPN allows users to connect to a private network from a remote location. This type of VPN is often used by employees who need to access company resources from a remote location.
2. **Site-to-Site VPN:** A site-to-site VPN connects two or more networks together over the internet. This type of VPN is often used by companies with multiple locations.
3. **Client-to-Site VPN:** A client-to-site VPN allows individual users to connect to a private network from a remote location. This type of VPN is often used by individuals who need to access their home network from a remote location.

VPN Benefits

- **Secure encryption:** To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.
- **Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.
- **Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively "change" your location.
- **Secure data transfer:** If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

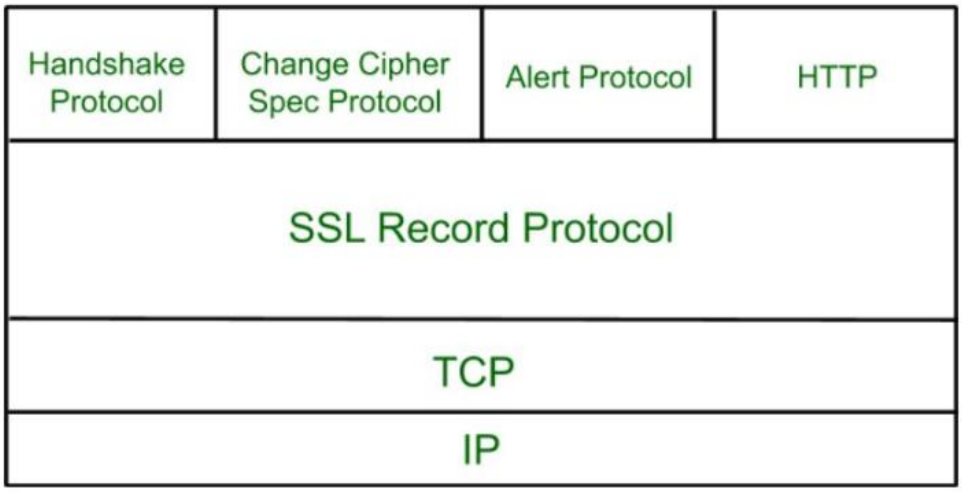
Table B-3 Primary VPN Components

Component	Description
Tunnels	Virtual channels through a shared medium. They provide a secure communications path (an encapsulated traffic flow) between two peers. Every VPN tunnel can consist of multiple sessions.
Endpoints	A network device on which a tunnel ends. The following devices can serve as endpoints: a computer running a VPN client, a router, a gateway, or a network access server. The two ends of a tunnel are commonly called the source and the destination endpoints. • A source endpoint initiates the tunnel. • A destination endpoint terminates the tunnel.
Sessions	Portions of tunnels that pertain to the transmission of a specific user in a single, tunneled PPP call between two peers. A remote access tunnel can contain one or more PPP connections. Each connection represents one user. However, Performance Monitor refers to *any* user connection to a device as a session.

3. Explain ssl

- SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol.
- It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications.
- It resides between Application layer and Transport Layer.
- SSL is the predecessor to the modern TLS encryption used today.
- A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP."
- In order to provide a high degree of 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 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.

SSL Protocol stack:



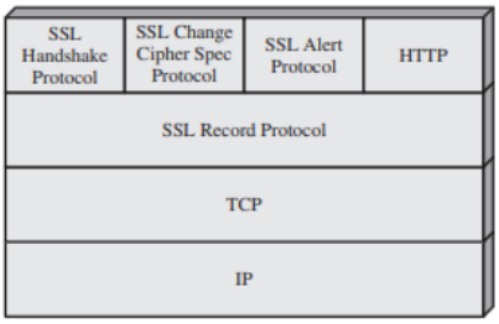


Figure 17.2 SSL Protocol Stack

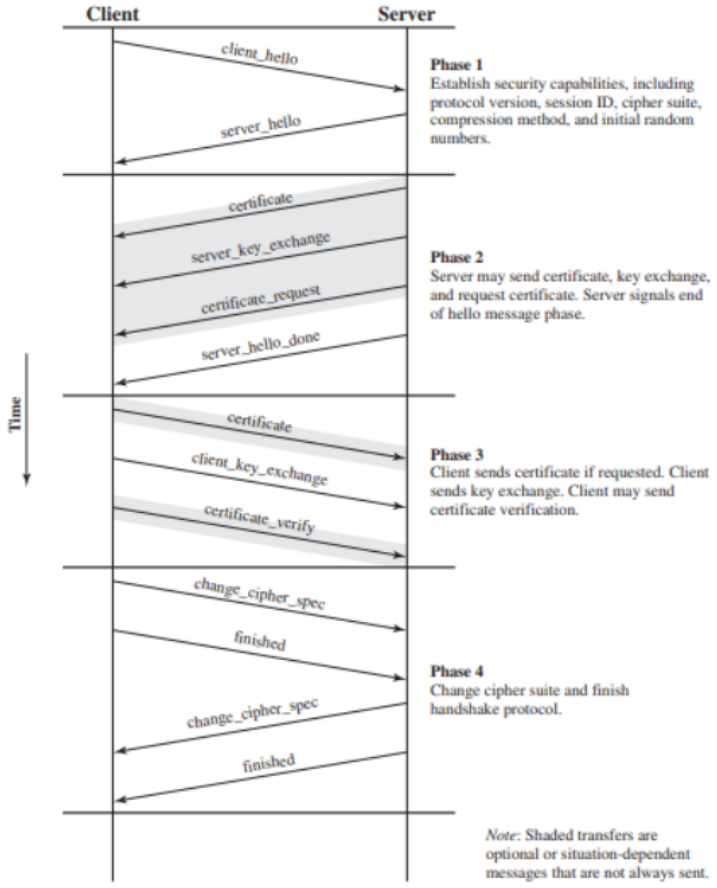


Figure 17.6 Handshake Protocol Action

Secure Socket Layer Protocols:

1. **SSL record protocol**

SSL Record Protocol

The SSL Record Protocol provides two services for SSL connections:

- **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
- **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

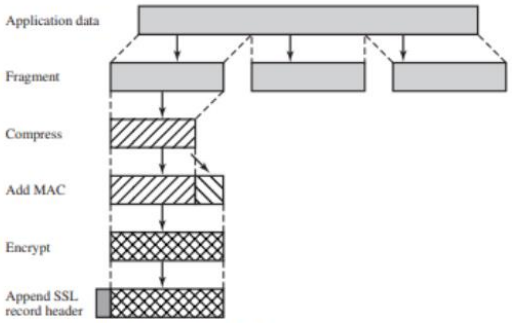


Figure 17.3 SSL Record Protocol Operation

The final step of SSL Record Protocol processing is to prepare a header consisting of the following fields:

- **Content Type (8 bits):** The higher-layer protocol used to process the enclosed fragment.
- **Major Version (8 bits):** Indicates major version of SSL in use. For SSLv3, the value is 3.
- **Minor Version (8 bits):** Indicates minor version in use. For SSLv3, the value is 0.
- **Compressed Length (16 bits):** The length in bytes of the plaintext fragment (or compressed fragment if compression is used). The maximum value is $2^{14} + 2048$.

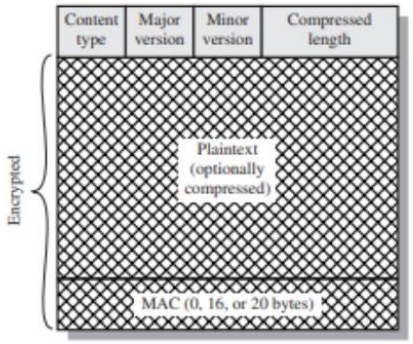


Figure 17.4 SSL Record Format

2. **Handshake protocol**

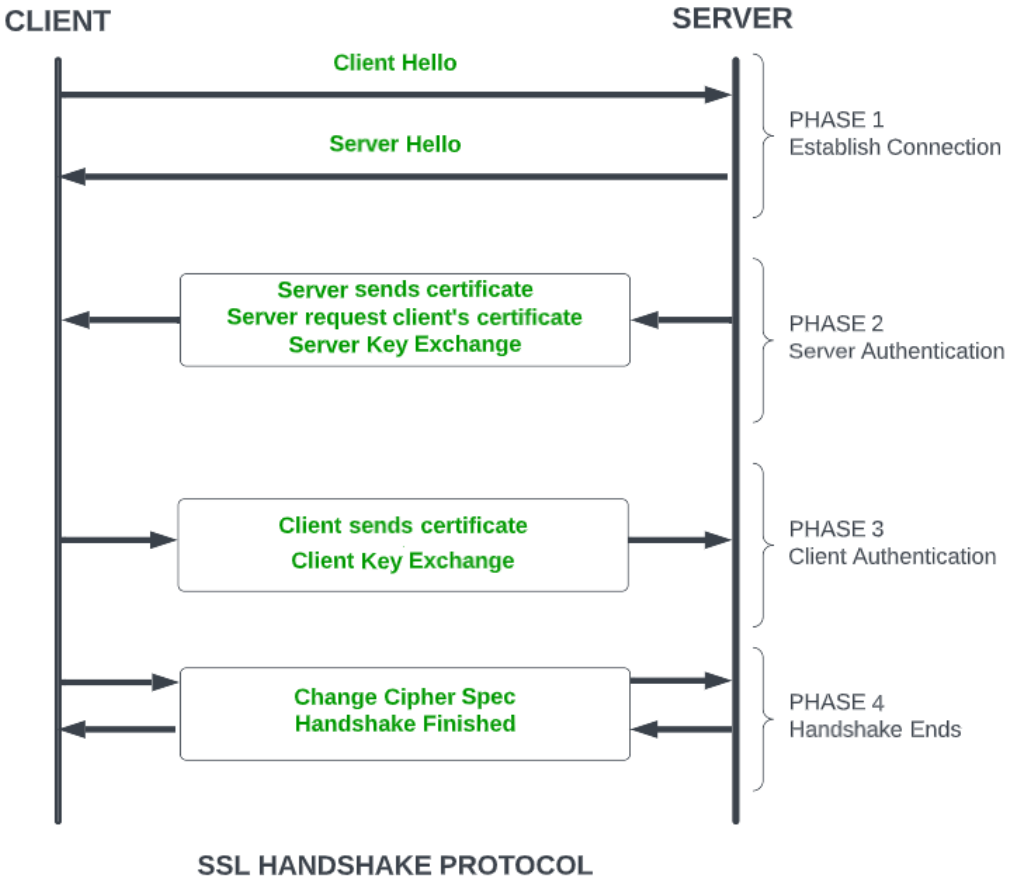
   Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

   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 occurred and after this Handshake Protocol ends.



3. **Change-cipher spec protocol**
   The change cipher spec protocol is one of the three SSL-specific protocols that use SSL Record protocol and it is the simplest. This protocol consists of a single message which consists of a single byte with value 1. The sole purpose of this message is to cause the pending state to be copied into the current state which updates the cipher suite to be used on this connection.
4. **Alert protocol**
   The Alert protocol is used to convey SSL-related alerts to the peer entity. As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state.
   Each message in this protocol consists of two bytes (Figure 17.5b). The first byte takes the value warning (1) or fatal (2) to convey the severity of the message. If the level is fatal, SSL immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established. The second byte contains a code that indicates the specific alert. First, we list those alerts that are always fatal (definitions from the SSL specification):

- **unexpected_message:** An inappropriate message was received.
- **bad_record_mac:** An incorrect MAC was received.
- **decompression failure:** The decompression function received improper input (e.g., unable to decompress or decompress to greater than maxi- mum allowable length).

- **handshake_failure:** Sender was unable to negotiate an acceptable set of security parameters given the options available.
- **illegal parameter:** A field in a handshake message was out of range or inconsistent with other fields.
- The remaining alerts are the following.
- **close_notify:** Notifies the recipient that the sender will not send any more messages on this connection. Each party is required to send a close_ notify alert before closing the write side of a connection.
- **no_certificate:** May be sent in response to a certificate request if no appropriate certificate is available.
- **bad_certificate:** A received certificate was corrupt (e.g., contained a signature that did not verify).
- **unsupported_certificate:** The type of the received certificate is not supported.
- **certificate_revoked:** A certificate has been revoked by its signer.
- **certificate expired:** A certificate has expired.
- **certificate_unknown:** Some other unspecified issue arose in processing the certificate, rendering it unacceptable.

4. Short note on ssh

- SSH is a protocol to secure remote login and other secure network services over an insecure network.
- Secure channel between two computers provides data confidentiality and integrity.
- Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.
- In addition to providing strong encryption, SSH is widely used by network administrators to manage systems and applications remotely, enabling them to log in to another computer over a network, execute commands and move files from one computer to another.
- SSH uses the client-server model, connecting a Secure Shell client application, which is the end where the session is displayed, with an SSH server, which is the end where the session runs.

Layering of SSH protocols

1) Transport Layer Protocol

Provides server authentication, confidentiality, and integrity

- Public-key host authentication
  Lets the client know the correct server is on the other end
  DSS or RSA, raw or through OpenPGP
- Strong symmetric encryption
  Uses Diffie-Hellman algorithm for secure key exchange
  Many ciphers are supported: 3des, blowfish, twofish, aes, etc., most with multiple key sizes

New keys generated every 1 GB or 1 hour
- Data integrity via MACS (message authentication codes)
  SHA-1 and MD5 are supported

2) **User Authentication Protocol**
   Authenticates the client-side user to the server
   - Multiple authentication methods
     public-key, password, host-based
     Extensible
   - Server tells client which methods can be used, client picks the most convenient
   - Provides a single authenticated channel to the connection protocol
3) **Connection Protocol**
   Multiplexes the tunnel into logical channels
   - Provides multiple channels:
     interactive login sessions
     remote execution of commands
     forwarded X11 connections
     forwarded TCP/IP connections
   - All channels are multiplexed into a single encryption tunnel
4) **New protocols can coexist with the existing ones**
   Attacks on SSH
   - **Man-in-the-middle**
     Very easy if the client does not have the server's public key prior to connecting
     Attacker masquerades between the client and server
   - **Denial of service**
   - **Covert channels**

5. **S/mime**
   - Secure/Multipurpose Internet Mail Extension (S/MIME) is an industry-standard for email encryption and signature that is commonly used by

businesses to improve email security. S/MIME is supported by the majority of corporate email clients.

- S/MIME encrypts and digitally signs emails to verify that they are verified and that their contents have not been tampered with.
- S/MIME works based on asymmetric encryption. This means that there is a set of keys involved to encrypt and decrypt an email.
- An S/MIME certificate is installed on the email clients of both the recipient and the sender. When an email is sent, the sender encrypts the email using the recipient's public key and the recipient decrypts the email using the private key. S/MIME also attaches a digital signature to an email. This ensures that the sender is authorized to send emails from a certain domain.

You receive a slew of cryptographic security features when you use an S/MIME certificate for email apps.
Authentication – It refers to the verification of a computer user's or a website's identity.
Message consistency – This is a guarantee that the message's contents and data have not been tampered with. The message's secrecy is crucial. The decryption procedure entails checking the message's original contents and guaranteeing that they have not been altered.
Use of digital signatures that invoke non-repudiation – This is a circumstance in which the original sender's identity and digital signatures are validated so that there is no doubt about it.
Protection of personal information – A data breach cannot be caused by an unintentional third party.
Encryption is used to protect data – It relates to the procedures described above, in which data security is ensured by a mix of public and private keys representing asymmetric cryptography.

6. **Els**
   IDK WTF IS THIS TOPIC

7. **Https (GPT ans)**

HTTPS is an extension of HTTP (Hypertext Transfer Protocol) used for secure data transfer over the internet. It is the foundation of secure communication on the World Wide Web, ensuring that data transmitted between a user's web browser and a website remains confidential and protected from eavesdropping and tampering. HTTPS is essential for secure online transactions, safeguarding user privacy, and maintaining the integrity of web content.

Key Components of HTTPS:

1. Encryption: One of the primary purposes of HTTPS is to encrypt the data exchanged between the client (e.g., web browser) and the server (e.g., web server). This encryption is achieved using cryptographic protocols like SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security). These protocols ensure that the data is transformed into an unreadable format while in transit and can only be decrypted by the intended recipient.

2. Data Integrity: HTTPS also provides data integrity by verifying that the data exchanged between the client and the server remains unchanged during transmission. This is achieved using message authentication codes (MACs) and hash functions.

3. Authentication: HTTPS enables users to verify the authenticity of the website they are visiting. It uses digital certificates issued by trusted Certificate Authorities (CAs) to confirm the identity of the server. When you connect to a website, the server presents its digital certificate to your browser, and if the certificate is signed by a trusted CA, your browser trusts the website as legitimate.

How HTTPS Works:

1. Handshake: When a user accesses a website by entering "https://" in their browser, a secure connection is established through a process called the "handshake." This involves the following steps:

a. The client (web browser) requests a secure connection to the server by sending a "ClientHello" message, which includes its supported encryption algorithms and other relevant information.

b. The server responds with a "ServerHello" message, selecting a mutual encryption method and providing its digital certificate.

c. The client verifies the server's certificate. It checks if it's signed by a trusted CA and if it hasn't expired or been revoked.

d. If the certificate is valid, the client generates a shared secret key used for encryption.

e. The client and server exchange messages to confirm that they both have the shared secret key.

2. Data Transfer: Once the secure connection is established, data is transferred between the client and server in an encrypted and secure manner. The encryption prevents eavesdropping and data tampering.

3. Data Integrity and Authentication: Throughout the data transfer, HTTPS ensures data integrity (so data remains unchanged) and authenticates the server to the client.

Advantages of HTTPS:

1. Data Security: It protects sensitive information such as login credentials, personal data, and payment information from being intercepted by malicious actors.

2. Trustworthiness: HTTPS builds trust by confirming the authenticity of websites through digital certificates issued by trusted CAs.

3. SEO Benefits: Search engines like Google prioritize websites that use HTTPS, potentially boosting a site's search ranking.
4. Compliance: HTTPS is often required for compliance with data protection and privacy regulations, such as GDPR and HIPAA.
5. Improved Performance: Modern web technologies (HTTP/2 and HTTP/3) are often used with HTTPS, providing better performance and faster page loading.
6. Security Against Man-in-the-Middle Attacks: HTTPS mitigates the risk of man-in-the-middle attacks by ensuring secure, encrypted communication.

In conclusion, HTTPS is crucial for secure internet communication. It provides encryption, data integrity, and authentication, ensuring that online interactions are private and trustworthy. The widespread adoption of HTTPS has become a standard for secure web browsing and online transactions.

HTTP	HTTPS
It stands for Hyper Text Transfer Protocol	It stands for Hyper Text Transfer Protocol Secure
They do not encrypt the text	They encrypt the code so that no one can access it
It does not require SSL at Transport Layer	They use Secure Socket Layer to encrypt the code.
They do not require TLS or SSL	Here security is provided by TLS(Transport layer Security) and SSL(secure socket layer)
It used port no 80	It uses port no 443
URL begins with http://	URL begins with https://
It is unsecure	It is safe transfer protocol
It does not require any validation	It requires validation like domain verification
It has simple address bar	It has green colored address bar that show that it is secure
It can be hacked	It cannot be attacked by hackers

Module 5
1. Snmp

Simple Network Management Protocol (SNMP)

What is it?

A Protocol that Facilitates the exchange of management information between network devices.

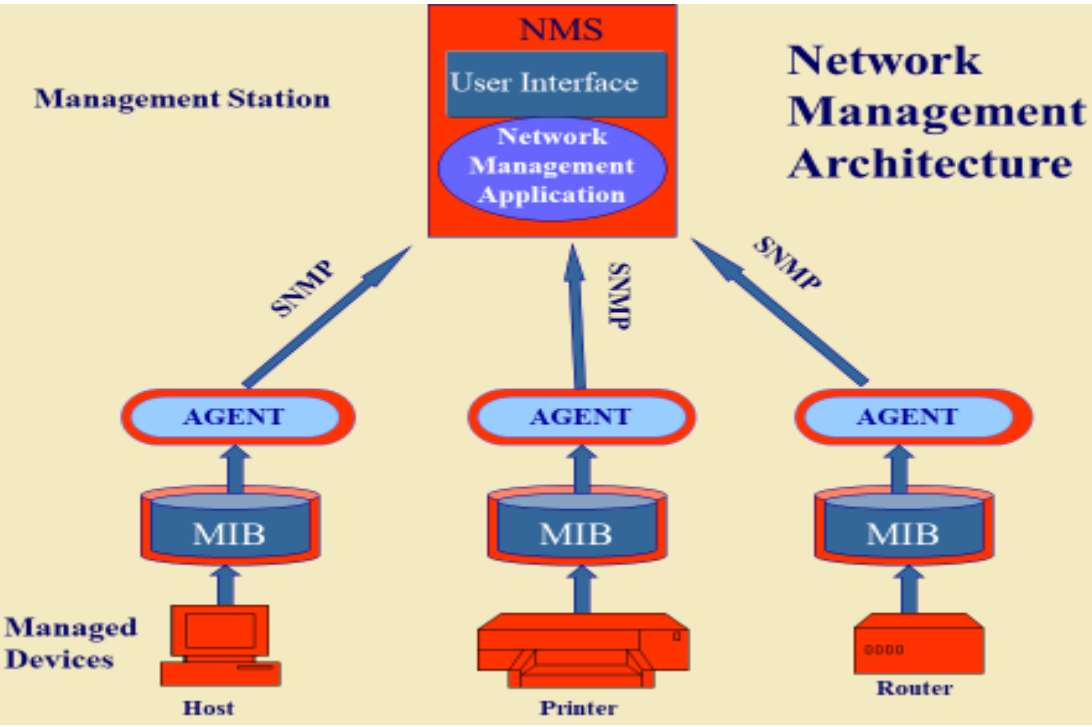
Why was it developed?

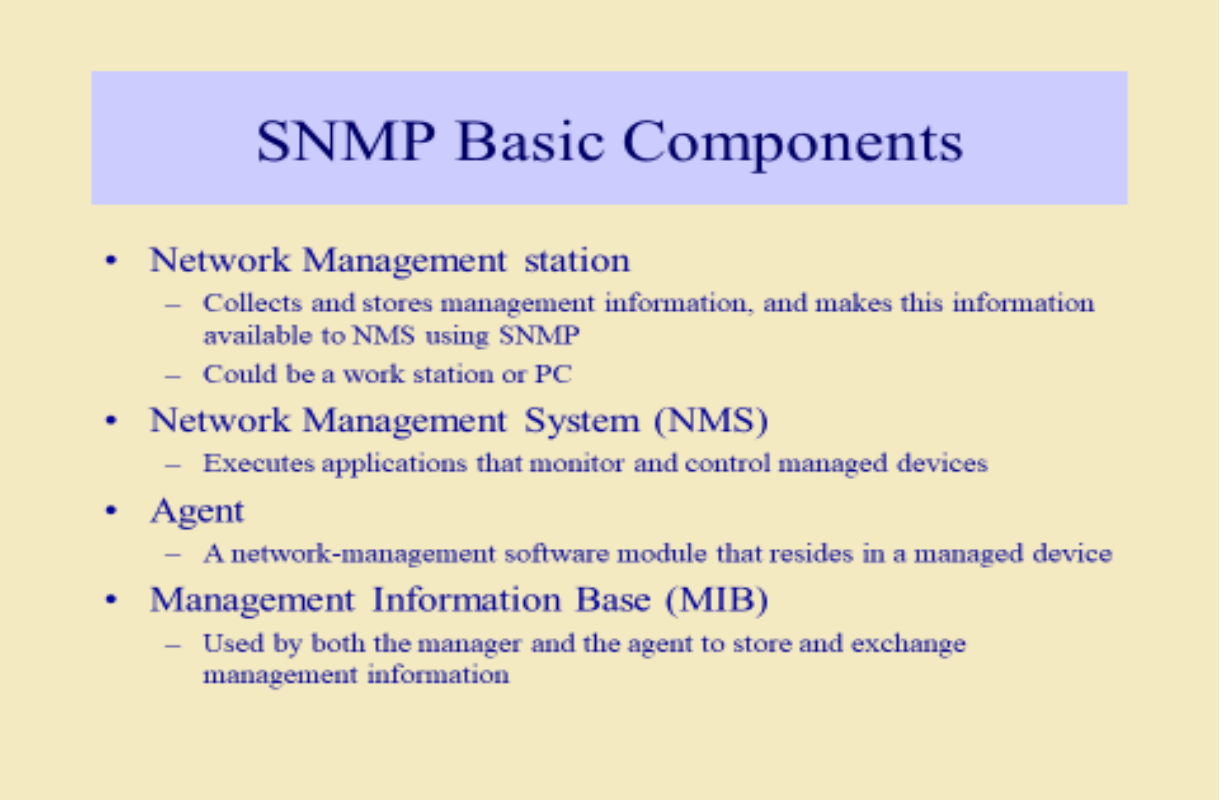
To **control and monitor status** of network devices

How is it beneficial?

Enables network administrators to:

- Manage network performance
- Find and solve network problems
- Plan for network growth





Managers & Agents:

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management Components:

Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).

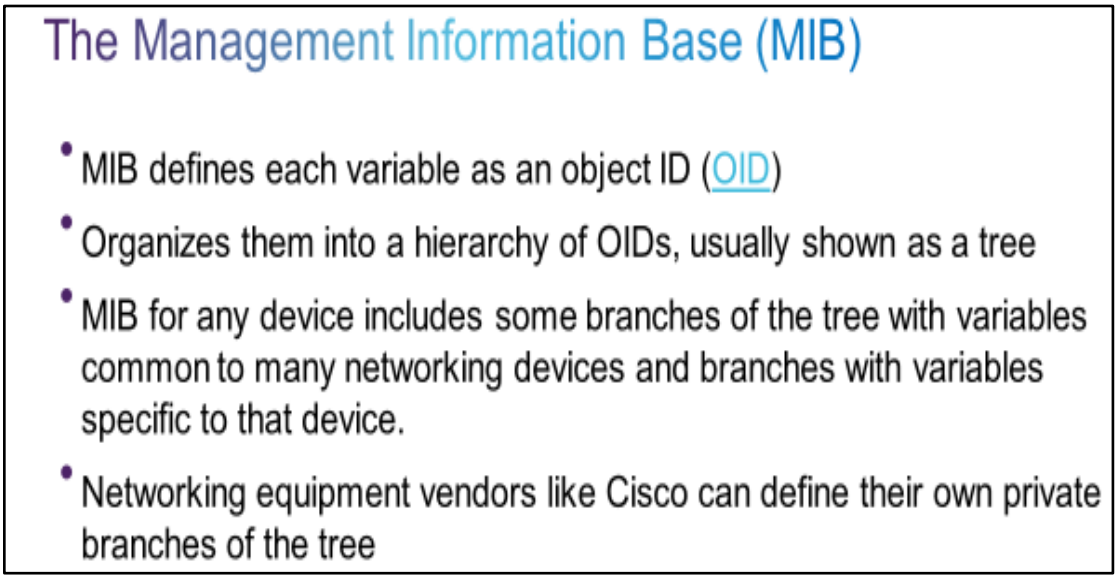
1. SMI:

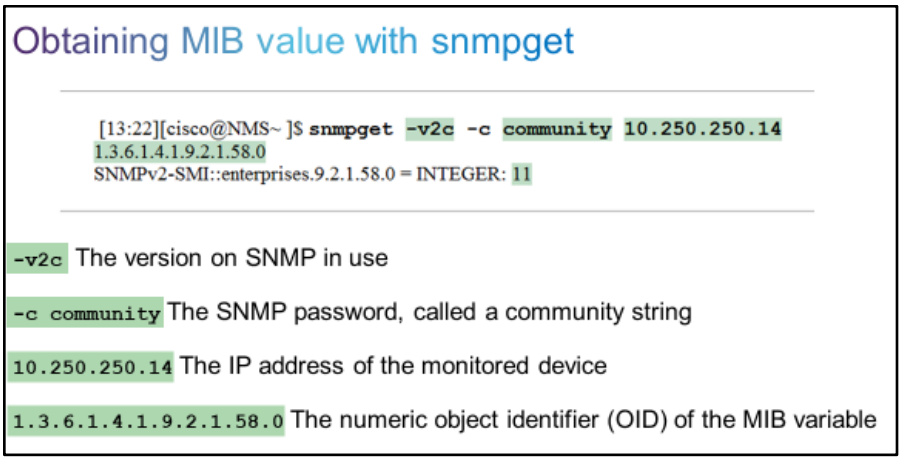
- The SMI (Structure of management information) is a component used in network management.
- Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

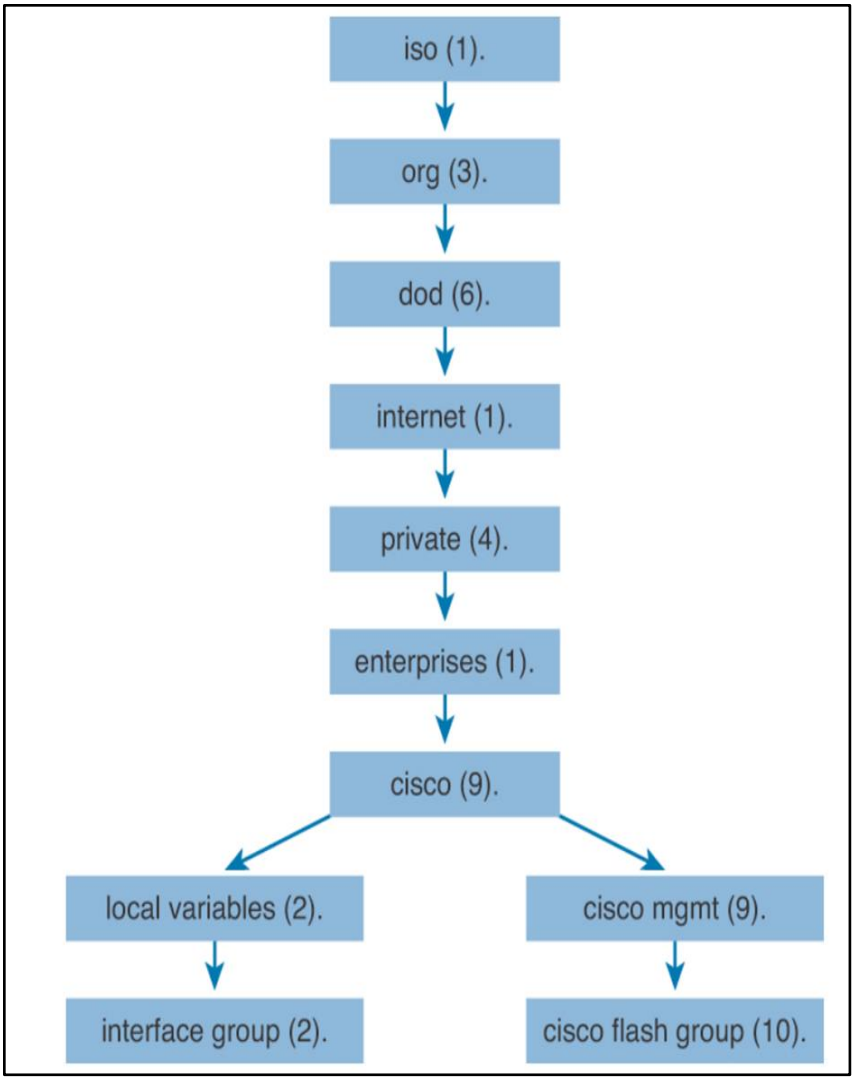
MIB:

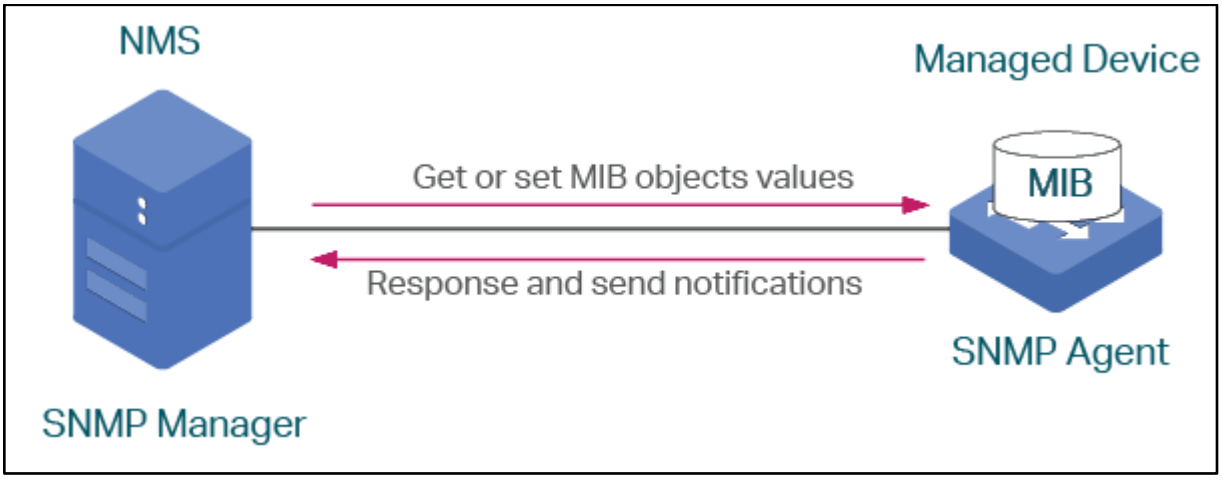
A database of an NMS is a physical database containing the network objects and values. It is implemented using any proprietary database software. MIB is a virtual database that is used by network management and agent applications to exchange information about the network objects.

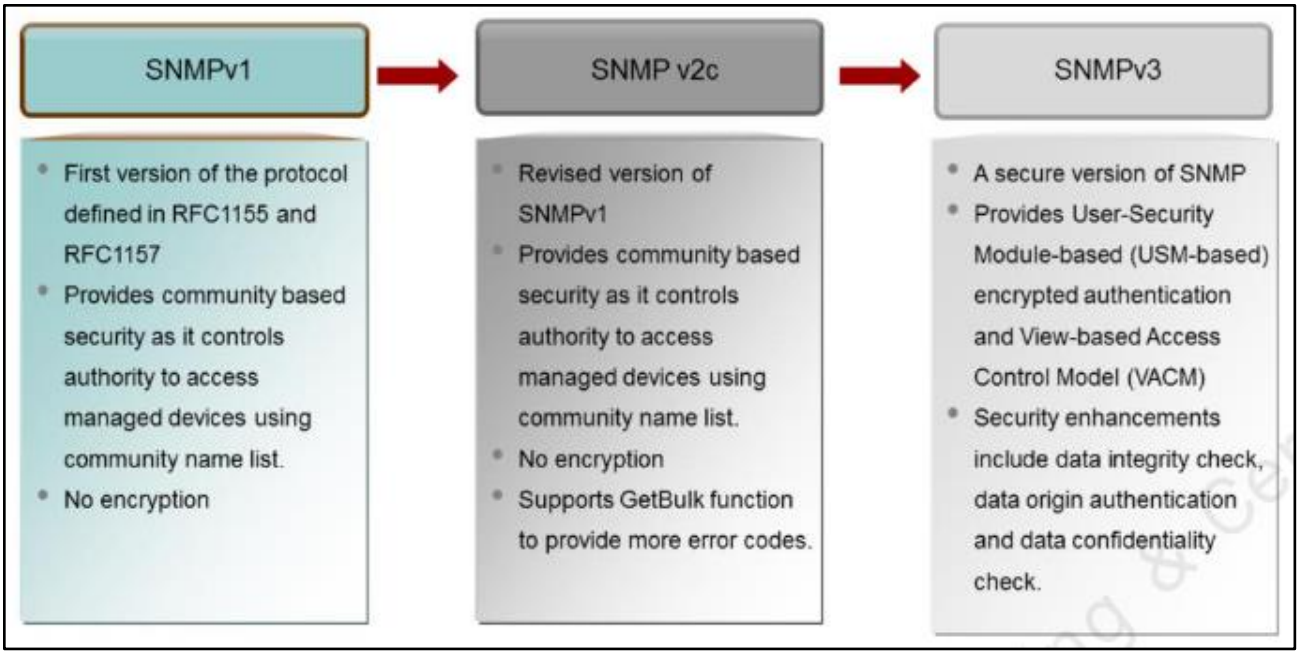
- MIB files contain management information of SNMP devices.
- For instance, while monitoring a switch, the data could be the amount of incoming/outgoing traffic, the total number of busy ports, packet loss rate, and so on.
- These small pieces of management information are available as data objects in a MIB file within a device.
- Each object has a specific address called object identifier (OID) for unique identification in an extended MIB database.






iso (1).
org (3).
dod (6).
internet (1).
private (4).
enterprises (1).
cisco (9).
local variables (2).
interface group (2).
cisco mgmt (9).
cisco flash group (10).


NMS
Managed Device
Get or set MIB objects values
MIB
Response and send notifications
SNMP Agent
SNMP Manager



*******READ ABOUT SNMPV3*******

2. NAC and principle elements of NAC

https://www.geeksforgeeks.org/what-is-network-access-control/

- Network access control, or NAC solutions support network visibility and access management through policy enforcement on devices and users of corporate networks.
- With organizations now having to account for exponential growth of mobile devices accessing their networks and the security risks they bring, it is critical to have the tools that provide the visibility, access control, and compliance capabilities that are required to strengthen your network security infrastructure.
- A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network.
- Network access control (NAC) is an umbrella term for managing access to a network. NAC authenticates users logging into the network and determines what data they can access and actions they can perform.
- NAC also examines the health of the user's computer or mobile device (the endpoints).
- Principles Elements
  NAC systems deal with three categories of components:
  1. **Access requestor (AR):** The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices. ARs are also referred to as supplicants, or simply, clients.

2. **Policy server:** Based on the AR's posture and an enterprise's defined policy, the policy server determines what access should be granted. The policy server often relies on backend systems, including antivirus, patch management, or a user directory, to help determine the host's condition.
3. **Network access server (NAS):** The NAS functions as an access control point for users in remote locations connecting to an enterprise's internal network. Also called a media gateway, a remote access server (RAS), or a policy server, an NAS may include its own authentication services or rely on a separate authentication service from the policy server.

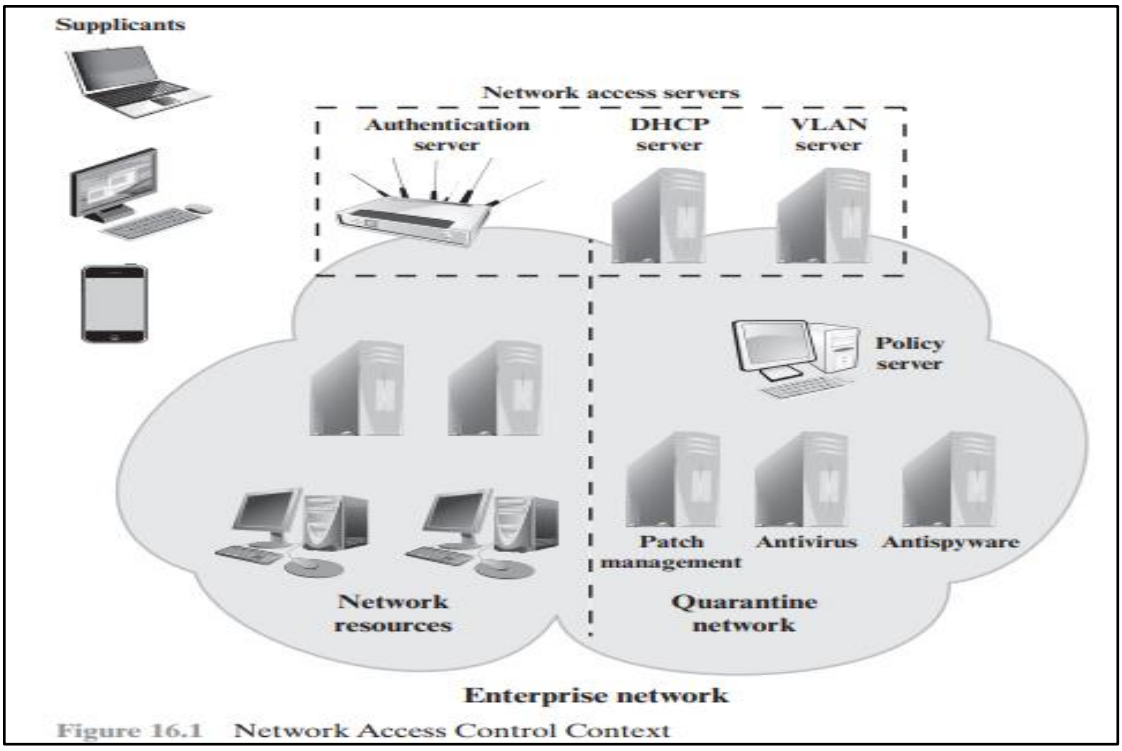


Figure 16.1 Network Access Control Context

3. Explain NAC enforcement methods

Enforcement methods are the actions that are applied to ARs to regulate access to the enterprise network. Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods. The following are common NAC enforcement methods.

1. **IEEE 802.1X:** This is a link layer protocol that enforces authorization before a port is assigned an IP address. IEEE 802.1X makes use of the Extensible Authentication Protocol for the authentication process.
2. **Virtual local area networks (VLANs):** In this approach, the enterprise network, consisting of an interconnected set of LANs, is segmented logically into a number of virtual LANs.1 The NAC system decides to which of the network's VLANs it will direct an AR, based on whether the device needs security remediation, Internet access only, or some level of network access to enterprise resources. VLANs can be created dynamically and VLAN membership, of both enterprise servers and ARs, may overlap. That is, an enterprise server or an AR may belong to more than one VLAN.

3. **Firewall:** A firewall provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user.
4. **DHCP management:** The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that enables dynamic allocation of IP addresses to hosts. A DHCP server intercepts DHCP requests and assigns IP addresses instead. Thus, NAC enforcement occurs at the IP layer based on subnet and IP assignment. A DCHP server is easy to install and configure, but is subject to various forms of IP spoofing, providing limited security.

4. Explain how NAC solutions can be implemented

- **Gather data-** If you're going to restrict how your users access the network, you'll first need to understand how they're using it. Who's connecting to what, and from which devices? Is there a business requirement behind their current level of access? Don't forget to consider servers, printers, phones, IoT devices, and anything else connected to the network.
- **Catch up on identity management-** If like most organizations, you plan on including an authentication component in your NAC policy, you'll need to make sure you're on top of identity management. If a new hire can't get online because your active directory servers aren't syncing with an HR database, then that shiny new NAC solution might wind up costing the company more money than it's worth. On the other hand, NAC security won't help you if you never bothered to de-provision an employee who left the company six months ago.
- **Determine permissions and access levels-** It's up to you to decide how to apply the capabilities of your NAC solution. Ideally, you'd implement the purest form of the principle of least privilege and limit all users to the minimum network resources needed to carry out their jobs. However, most large networks simply aren't segmented enough to strictly adhere to this principle. Implementing role-based access control can be a good middle ground without compromising too much on security.
- **Test your setup-** Most NAC solutions can be configured in a "monitor" mode, meaning the impact of policies can be measured before actually enforcing them. This is an important step, as it allows you to spot any potential problems before they generate a large volume of support tickets. It's a good idea to test your NAC policies both before you implement them and as you make changes.
- **Monitor and tune-** Network access control is not a "set it and forget it" type of security control. You'll need to make adjustments as the organization (and the threats facing it) evolve over time. Make sure you have the resources needed to continually monitor and optimize the solution before beginning an NAC implementation journey.

Module 6

1. Define IDS and types of IDS

- Intrusion detection systems are designed to identify suspicious and malicious activity through network traffic, and an intrusion detection system (IDS) enables you to discover whether your network is being attacked.
- An Intrusion Detection System is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall.
- This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).
- An IDS is composed of the following three components:
    a. Sensors: - which sense the network traffic or system activity and generate events.
    b. Console: - to monitor events and alerts and control the sensors,
    c. Detection Engine: - that records events logged by the sensors in a database and uses a system of rules to generate alerts from the received security events.
- Limitations of IDS:
    a. Does not prevent attacks.
    b. High rate of False alerts
    c. Complex systems
    d. Bypassing IDS
- There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts.
- Types of Intrusion-Detection systems-(On WHAT THEY MONITOR)
    a. **Network Intrusion Detection System**: - identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.
    b. **Host-based Intrusion Detection System**: - consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.
    c. **Hybrid Intrusion Detection System**: - combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.
- Types of Intrusion-Detection systems-(On HOW THEY MONITOR)
    a. **Signature based detection**:- This detection technique uses specifically known patterns to detect malicious code. These specific patterns are called signatures. Identifying the worms in the network is an example of signature based detection.
    b. **Anomaly Detection**:- These techniques are designed to detect abnormal

behavior in the system. The normal usage pattern is baselined and alerts are generated when usage deviates from the normal behavior. Example if a user logs on and off 20 times a day while the normal behavior is 1-2 times.

2. Explain different deployment methods of IDS

Intrusion detection systems are designed to identify suspicious and malicious activity through network traffic, and an intrusion detection system (IDS) enables you to discover whether your network is being attacked.

Various Deployment methods:

1. **Based on what they monitor**-
    a. Network Intrusion Detection System: - identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.
    b. Host-based Intrusion Detection System: - consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.
    c. Hybrid Intrusion Detection System: - combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.
2. **Based on how they monitor**-
    a. Signature based detection:- This detection technique uses specifically known patterns to detect malicious code. These specific patterns are called signatures. Identifying the worms in the network is an example of signature based detection.
    b. Anomaly Detection:- These techniques are designed to detect abnormal behavior in the system. The normal usage pattern is baselined and alerts are generated when usage deviates from the normal behavior. Example if a user logs on and off 20 times a day while the normal behavior is 1-2 times.
3. **Passive and Reactive detection**-
    - In a passive system, the IDS sensor detects a potential security breach, logs the information and signals an alert on the console.
    - In a reactive system, which is known as an Intrusion Prevention System (IPS) the IDS responds to the suspicious activity by resetting the connection it believes to be suspicious or by reprogramming the firewall to block network traffic from the suspected malicious source, either autonomously or at the command of an operator.
    - Though they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening.

- The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network.
- An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

3. Explain firewalls and their design principles

- A Firewall is hardware or software to prevent a private computer or a network of computers from, it acts as a filter to avoid unauthorized users from accessing private computers and networks.
- It is a vital component of network security. It is the first line of defense for network security.
- It filters network packets and stops malware from entering the user's computer or network by blocking access and preventing the user from being infected.
- It acts as a barrier between internal private networks and external sources (such as the public Internet).
- A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.
- Typically, firewalls intercept network traffic at a computer's entry point, known as a port.
- Firewalls control the flow of network traffic
- Firewalls have applicability in networks where there is no internet connectivity
- Firewalls operate on number of layers and an also act as VPN gateways
- Active content filtering technologies

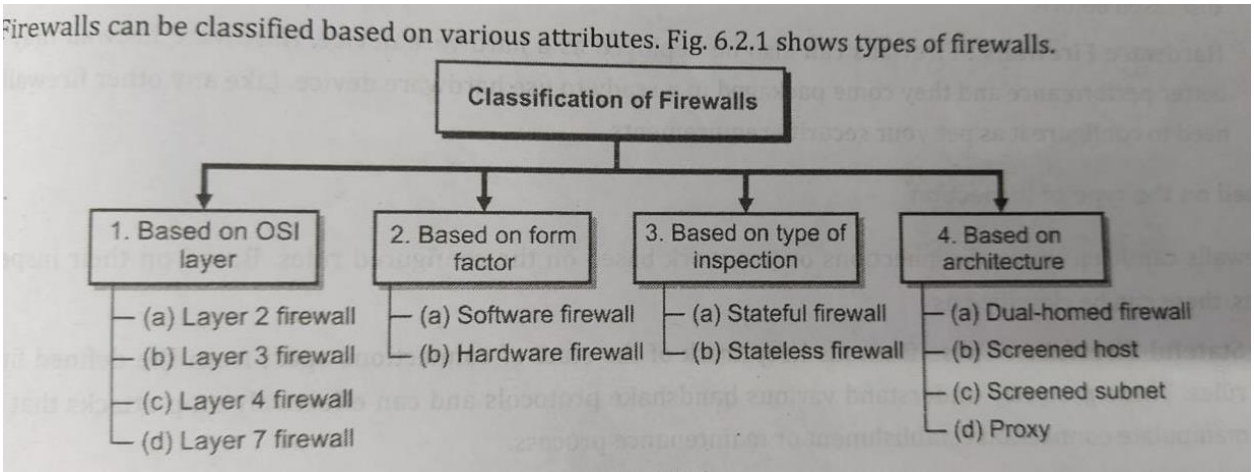
Design Principles of Firewalls:

1. **Developing Security Policy**: Security policy is a very essential part of firewall design. Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass. Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else. A properly developed security policy also knows what to do in case of a security breach.
2. **Simple Solution Design**: If the design of the solution is complex. then it will be difficult to implement it. If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure. The problem that comes with complex designs is a configuration error that opens a path for external attacks.
3. **Choosing the Right Device**: Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable. if the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless. Firstly the designing part must be done then the product requirements must be found out, if the

product is already available then it is tried to fit in a design that makes security weak.

4. **Layered Defense**: A network defense must be multiple layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat. It gives an edge to the security design and finally neutralizes the attack over the system.
5. **Consider Internal Threats**: While giving a lot of attention to safeguarding the network or device from external attacks. The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly. Different levels can be set in network security while designing internal security. Filtering can be added to keep track of the traffic moving from lower-level security to higher level.

4. Explain different types of firewalls and their advantages and disadvantages.



1. Packet Filtering Firewall

- Operate on transport and network layers of the TCP/IP stack
- Decides what to do with a packet depending upon the following criteria:
    a. Transport protocol (TCP,UDP,ICMP),
    b. Source and destination IP address
    c. The source and destination ports
    d. ICMP message type/code
    e. Various TCP options such as packet size, fragmentation etc.
- **Terminologies**
    a. Stateless Firewall: The firewall makes a decision on a packet by packet basis.
    b. Stateful Firewall: The firewall keeps state information about transactions (connections).
- **Functions**
    a. Forward the packet(s) on to the intended destination.
    b. Reject the packet(s) and notify the sender (ICMP dest unreach/admin prohibited)

c. Drop the packet(s) without notifying the sender.
d. Log accepted and/or denied packet information.
e. NAT - Network Address Translation, that is, it translates public IP address(es) to private IP address(es) on a private LAN.

- **Advantages**
  a. Simplicity: Packet filtering firewalls are easy to configure and operate, making them a cost-effective and straightforward choice for network security.
  b. Low Overhead: They have minimal impact on network performance, as they make filtering decisions based on header information, resulting in lower processing overhead.
  c. Efficiency: Packet filtering is efficient at blocking or allowing traffic based on specific criteria, helping prevent unwanted or malicious packets from entering the network.
  d. Speed: Packet filtering can be performed quickly, making it suitable for high-speed networks.
  e. Flexibility: Administrators have control over which packets are allowed or denied based on a wide range of parameters, enabling customization to meet specific security and network needs.
- **Disadvantages**
  a. Filters can be difficult to configure. It's not always easy to anticipate traffic patterns and create filtering rules to fit.
  b. Filter rules are sometimes difficult to test
  c. Packet filtering can degrade router performance
  d. Attackers can "tunnel" malicious traffic through allowed ports on the filter.

2. Application Gateway (Proxy Server)

- Operate at the application protocol level. (Telnet, FTP, HTTP)
- Application Gateways "Understand" the protocol and can be configured to allow or deny specific protocol operations.
- Typically, proxy servers sit between the client and actual service. Both the client and server talk to the proxy rather than directly with each other.
- **Advantages**
  a. Deep Packet Inspection: Application gateways can inspect data packets at the application layer, identifying and blocking application-layer threats and attacks.
  b. Granular Control: They offer precise control over which applications and services are allowed or blocked, enabling the enforcement of specific security policies.
  c. Content Filtering: Application gateways can perform content filtering, allowing administrators to block or restrict access to specific websites, URLs, or content categories.

d. Enhanced Security for Web Applications: They effectively protect web applications from common attacks like SQL injection, XSS, and CSRF, safeguarding sensitive data.
e. Protocol Awareness: Application gateways are aware of application-specific protocols, enabling the enforcement of security policies tailored to individual applications, enhancing network security.

- **Disadvantages**
  a. Requires modification to client software application.
  b. Some client software applications don't accommodate the use of a proxy.
  c. Some protocols aren't supported by proxy servers.
  d. Some proxy servers may be difficult to configure and may not provide all the protection you need.

3. Firewall Hardware/Software

- Dedicated hardware/software application such as Cisco PIX Firewall which filters traffic passing through the multiple network interfaces.
- A Unix or Windows based host with multiple network interfaces, running a firewall software package which filters incoming and outgoing traffic across the interfaces.
- A Unix or Windows based host with a single network interface, running a firewall software package which filters the incoming and outgoing traffic to the individual interface.
- **Hardware Firewall: Advantages**
  a. Network-Wide Protection: They can protect multiple devices and users simultaneously, making them ideal for businesses and organizations.
  b. Simplified Configuration: Hardware firewalls are often easier to set up and configure, making them accessible to users with varying levels of technical expertise.
  c. Single Point of Control: Centralized control and management for network security, which can simplify monitoring and policy enforcement.
  d. Better Performance: Hardware firewalls don't consume system resources on individual devices, ensuring network performance remains optimal.
  e. Physical Isolation: Being separate devices, they provide an added layer of security by physically isolating the network from potential threats.
- **Hardware Firewall: Disadvantages**
  a. Cost: Hardware firewalls can be expensive to purchase and maintain.
  b. Limited Scalability: They may have limitations in terms of accommodating a growing network.
  c. Physical Maintenance: Ongoing physical maintenance is required.
  d. Complex Configuration: Setting up can be complex, requiring technical expertise.

e. Single Point of Failure: If the hardware firewall fails, the entire network's security is compromised.

- **Software Firewalls: Advantages**
    a. Cost-Effective: Software firewalls are often more cost-effective for individual users or small businesses, as they don't require dedicated hardware.
    b. Customizable Rules: Users can customize firewall rules to meet specific needs and configurations, allowing for fine-grained control.
    c. Easy Updates: Software firewalls can be easily updated with the latest security patches and definitions.
    d. Operating System Integration: They can integrate with the host operating system, providing protection at the software level.
    e. No Additional Hardware: Software firewalls don't require additional hardware, making them a convenient choice for personal devices.
    f. Portability: They can be used on a wide range of devices, from computers to mobile devices, providing flexibility and protection on the go.
    g. Layered Security: They can complement hardware firewalls, providing an additional layer of defense for individual devices.
- **Software Firewalls: Disadvantages**
    a. Resource Consumption: They consume system resources, potentially impacting performance.
    b. Operating System Dependency: They depend on the host OS, making them vulnerable if the OS is compromised.
    c. Vulnerabilities: Lack of regular updates can leave them vulnerable to exploits.
    d. Complexity: Configuring them can be intricate, leading to security holes if not done correctly.
    e. Software Conflicts: They may conflict with other software, causing compatibility issues.
    f. Not Ideal for Network-wide Protection: They are primarily designed for individual device protection.

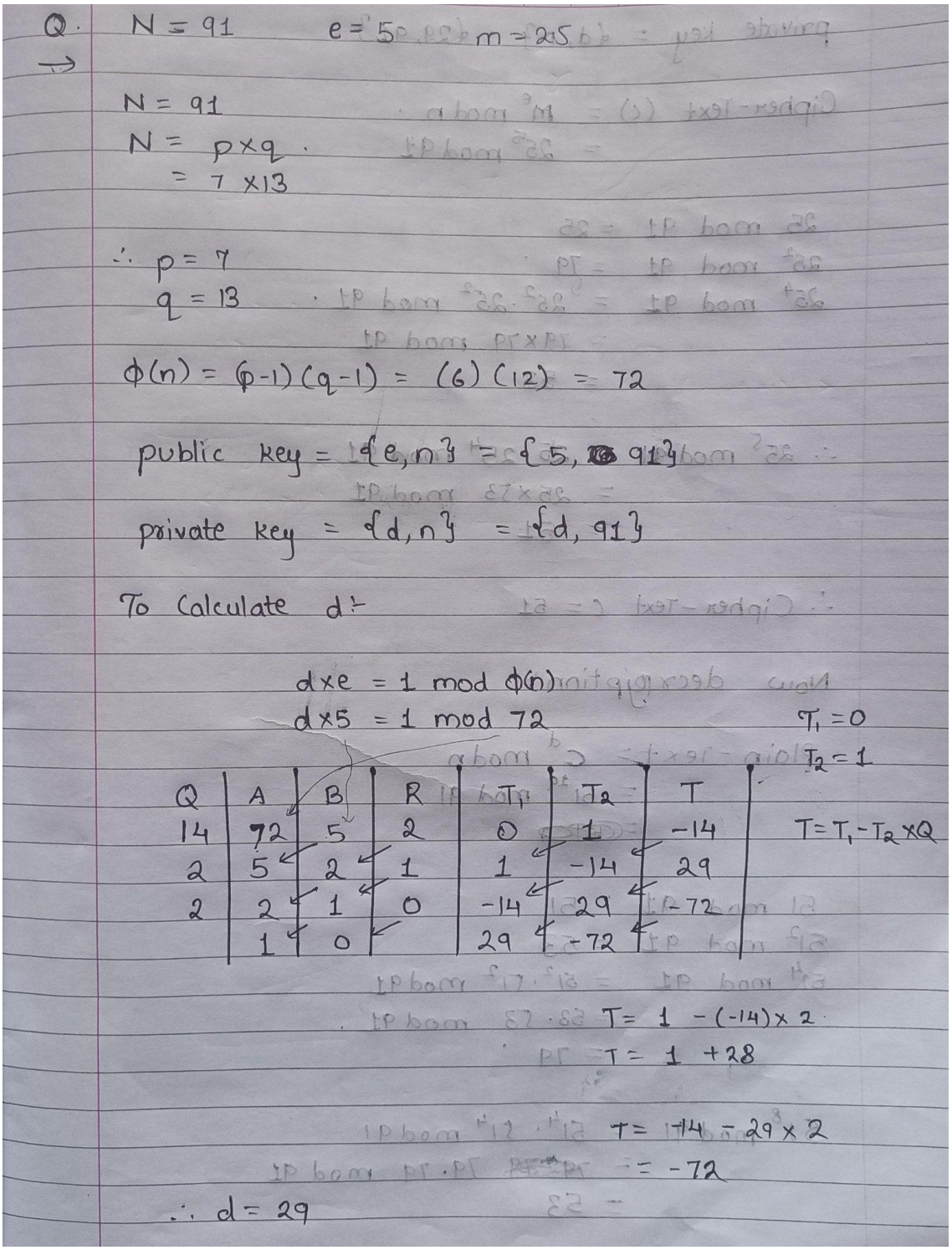
5. Difference between IDS and firewalls

Aspect	Intrusion Detection System (IDS)	Firewall
Purpose	Detects and alerts on unauthorized access, attacks, and security breaches	Establishes a barrier to control and filter traffic between trusted and untrusted networks
Functionality	Monitors network activity for suspicious or malicious behavior, generates alerts	Controls incoming and outgoing traffic based on predefined rules, allowing or denying traffic
Action Taken	Generates alerts and reports when suspicious activity is detected, does not block traffic	Actively blocks, allows, or modifies traffic based on access control policies
Awareness	Has a deep understanding of specific attack patterns or deviations from normal behavior	Lacks detailed knowledge of specific attack methods, focuses on source and destination of traffic
Prevention vs. Detection	Primarily for detection and notification of security incidents	Focused on preventing unauthorized access and protecting against known threats
Deployment	Can be deployed throughout the network to monitor traffic within and between network segments, includes Host-based IDS (HIDS)	Deployed at network gateways (e.g., perimeter firewall) and within internal network segments
Response Time	Generates alerts for post-event analysis, response time depends on the speed of human or automated analysis	Provides real-time response to network traffic by enforcing access control rules

Firewall	IDS
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.
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)
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
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
No man-power is required to manage a firewall.	An administrator (man-power) is required to respond to threats issued by IDS
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).

PAST YEAR QUESTIONS

1)In an RSA system, given N=91 e=5 Calculate Φ(n),p, q and private key d. What is the cipher text when you encrypt message m=25 using the public key. Also perform decryption.



Q. $N = 91$ $e = 5$ $m = 25$

→

$N = 91$

$N = p \times q$

$= 7 \times 13$

$\therefore p = 7$

$q = 13$

$\phi(n) = (p-1)(q-1) = (6)(12) = 72$

public key $= \{e, n\} = \{5, 91\}$

private key $= \{d, n\} = \{d, 91\}$

To Calculate d:-

$d \times e = 1 \bmod \phi(n)$

$d \times 5 = 1 \bmod 72$

$T_1 = 0$

$T_2 = 1$

$T = T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2	T
14	72	5	2	0	1	-14
2	5	2	1	1	-14	29
2	2	1	0	-14	29	-72
	1	0		29	-72	

$T = 1 - (-14) \times 2$

$T = 1 + 28$

$T = -14 - 29 \times 2$

$= -72$

$\therefore d = 29$

private key = $\{d, n\} = \{29, 91\}$

Cipher-Text $(c) = m^e \bmod n$.

$= 25^5 \bmod 91$

$25 \bmod 91 = 25$

$25^2 \bmod 91 = 79$

$25^4 \bmod 91 = 25^2 \cdot 25^2 \bmod 91$.

$= 79 \times 79 \bmod 91$

$= 53$

$\therefore 25^5 \bmod 91 = 25 \cdot 25^4 \bmod 91$

$= 25 \times 53 \bmod 91$

$= 51$

$\therefore$ Cipher-Text $C = 51$

Now decryption

Plain-Text $= c^d \bmod n$

$= 51^{29} \bmod 91$

$51 \bmod 91 = 51$

$51^2 \bmod 91 = 53$

$51^4 \bmod 91 = 51^2 \cdot 51^2 \bmod 91$

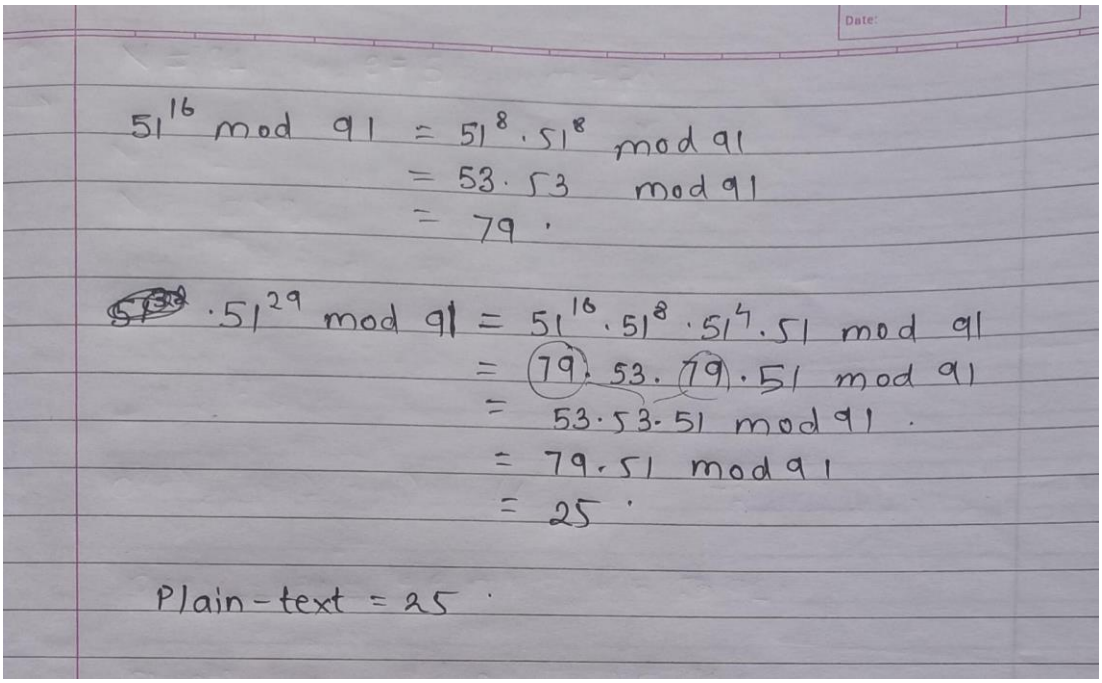
$= 53 \cdot 53 \bmod 91$.

$= 79$.

$51^8 \bmod 91 = 51^4 \cdot 51^4 \bmod 91$

$= 79 \cdot 79 \bmod 91$

$= 53$



2) A secure e-voting system is to be designed. Discuss the security goals that must be met and enlist mechanisms for the same.

3)Describe different types of Denial of service attacks

4)Explain in detail with a diagram, How Kerberos can be used for authentication.

5)Use cases for NAC

- NAC for guests/contractors: Whether accounting for contractors, visitors, or partners, organizations use NAC solutions to make sure that non-employees have access privileges to the network that are separate from those of employees.
- NAC for BYOD: The exponential growth in mobile devices has liberated the workforce from their desks and given employees freedom to work remotely from their mobile devices. NAC for BYOD ensures compliance for all employee owned devices before accessing the network.
- NAC for the Internet of Things: IoT devices, whether they be in manufacturing, healthcare, or other industries, are growing exponentially and serve as additional entry points for attackers to enter the network. NAC can reduce these risks in IoT devices by applying defined profiling and access policies for various device categories.
- NAC for incidence response: NAC vendors can share contextual information (for example, user ID or device type) with third-party security components. They can respond to cybersecurity alerts by automatically enforcing security policies that isolate compromised endpoints.

- NAC for medical devices: As more medical devices come online, it's critical to identify devices entering a converged network. NAC solutions can help protect devices and medical records from threats, improve healthcare security, and strengthen ransomware protection.

6)**Explain Security Services and mechanisms to implement it:**

X.800:

"a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

RFC 2828:

"a processing or communication service provided by a system to give a specific kind of protection to system resources"

Table 1.2 Security Services (X.800)

AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-Origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block. **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-Flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

SECURITY MECHANISMS:

The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.
Specific security mechanisms: encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
Pervasive security mechanisms: trusted functionality, security labels, event detection, security audit trails, security recovery

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The 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.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** *Data collected and potentially used to facilitate a* security audit, which is an independent review and examination of system records and activities.
	Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

SPECIFIC SECURITY MECHANISMS

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

7)What is Network Management Security? Explain SNMP V3.

For NWS refer chp qs

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with during transit.
- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the content of a packet to prevent it from being learned by an unauthorized source.

1. v3 is the latest version of SNMP which involves great management services with enhanced security.
2. The SNMPv3 architecture makes the use of User-based Security Model (USM) for security of the messages & the View-based Access Control Model (VACM) for accessing the control over the services.
3. **SNMP v3 security models supports authentication and encrypting.**
4. SNMPv3 supports Engine ID Identifier, which uniquely identifies each SNMP identity. The Engine ID is used to generate a unique key for authenticating messages.
5. v3 provides secure access to the devices that send traps by authenticating users & encrypting data packets which are sent across the network.
6. It also introduces the ability to configure and modify the SNMP agent using SET for the MIB objects. These commands enable deletion, modification, configuration and addition of these entries remotely.
7. **Mechanism Support of version 3 :**
    - 16-byte key between sender & receiver
    - Triple Data Encryption Standard
    - Advanced Encryption Standard
    - Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode
    - MD5 message-digest algorithm