SHORT QUESTIONS

1. **Which are two main concerns of DES?**

   DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion).

2. **Define message integrity?**

   Message integrity means that a message has not been tampered with or altered. The most common approach is to use a hash function that combines all the bytes in the message with a secret key and produces a message digest that is difficult to reverse

3. **Diff b/w brute force attack and cryptanalysis?**

   A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

   Cryptanalysis is the reverse of cryptography. It is the science of cracking codes, decoding secrets, and in general, breaking cryptography protocol. It is a process of attempting to discover plain text or key.

4. **What are different rounds where 2bit applied in DES?**

   2-Bits are applied in Expansion Box of f(n) in a round of DES. Here 32 bits plain text is converted into 48 bits plain text by adding 2 extra bits in very block of plain text, One bit in start and one at end of block.

5. **What is encapsulating security payload?**

   The Encapsulating Security Payload (ESP) protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection.

6. **Diff b/w risk and vulnerability?**

   Vulnerability refers to a weakness in your hardware, software, or procedures. (In other words, it's a way hackers could easily find their way into your system.) And risk refers to the potential for lost, damaged, or destroyed assets.

7. **Which algorithm is used for encryption and decryption in email security?**

   RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys.

Confusion = Substitution
a --> b
Caesar Cipher

Diffusion = Transposition or Permutation
abcd --> dacb

8. Diff b/w confusion and diffusion?

Confusion refers to making the relationship between the ciphertext and the symmetric key as complex and involved as possible; diffusion refers to dissipating the statistical structure of plaintext over the bulk of ciphertext.

9. Disadvantages of symmetric cryptography?

While symmetric encryption offers a wide range of benefits, there is one major disadvantage associated with it: the inherent problem of transmitting the keys used to encrypt and decrypt data. When these keys are shared over an unsecured connection, they are vulnerable to being intercepted by malicious third parties.

10. Role of tunnel in VPN?

A VPN tunnel is an encrypted connection between your device and a VPN server. It's uncrackable without a cryptographic key, so neither hackers nor your Internet Service Provider (ISP) could gain access to the data.
This protects users from attacks and hides what they're doing online

11. Fermat's Little theorem?

Fermat's little theorem states that if p is a prime number, then for any integer a, the number a p – a is an integer multiple of p. ap ≡ a (mod p).

12. What are two measure that should be taken in router security? AS LONG

Set Up a Secure Password. ...
Change Your Network Name/SSID. ...
Hide Your Network. ...
Enable The Firewall. ...
Turn on Wireless Network Encryption. ...
Update Your Router Software. ...
Enable MAC Address Filtering.
Disable Remote Administration

13. Authentication header?

The Authentication Header (abbreviated as AH) is a security mechanism that aims to help with authenticating the origins of packets of data that are transmitted under IP conditions (also known as the datagrams)

14. CCA?

A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts.

Two-factor authentication is a security mechanism, which has grown more prevalent as data breaches become commonplace. It involves logging into a system using "something you know" and " something you have

15. Three stages of MOM?

Method–Opportunity–Motive. A malicious attacker must have three things to ensure success: method, opportunity, and motive.

16. Direct authentication? Direct Autonomus Authentication

Direct authentication requires the presentation of credentials, which are typically a username and password. Service uses these credentials to authenticate the request. Credentials are used to authenticate with the broker, which issues a security token. The security token is then used to authenticate with services. i.e 2 step verficication

17. What is avalanche effect?

In cryptography, the avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly, the output changes significantly.

18. Replay attack?

A replay attack is a category of network attack in which an attacker detects a data transmission and fraudulently has it delayed or repeated. The delay or repeat of the data transmission is carried out by the sender or by the malicious entity, who intercepts the data and retransmits it.

19. Diff b/w security attack and security mechanism?

➢ **Security Attack:** Any action that compromises the security of information.

➢ **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.

➢ **Security Service:** A service that enhances the security of data processing systems and information transfers.

20. AAA Model?

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

21. Define Transport layer security? TCP/IP & UDP user datagram protocol

Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

22. ICMP flood attack?

An Internet Control Message Protocol (ICMP) flood DDoS attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).

23. Diff b/w DoS & DDoS?

A denial-of-service attack is a cyber-attack in which the attacker seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network.

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

24. Diff b/w Authentication and authorization?

Authentication is the process of verifying who someone is, whereas Authorization is the process of verifying what specific applications, files, and data a user has access to.

25. Diff b/w IDS and Firewall?

Firewall is a device and/or a sotware that stands between a local network and the Internet, and filters traffic that might be harmful.

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.

26. Mention different way to prevent phishing attack?

- Keep Informed About Phishing Techniques
- Think Before You Click!
- Verify a Site’s Security
- Keep Your Browser Up to Date

- Use Firewalls
- Never Give Out Personal Information

27. What is Key exchange problem?

The key exchange problem. The key exchange problem describes ways to exchange whatever keys or other information are needed for establishing a secure communication channel so that no one else can obtain a copy.

28. Two techniques of crypto analysis?

Secret Key Cryptography.

Public Key Cryptography.

Hash Functions.

Simple Network Management Protocol is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks

29. What is role of SNMP in network security?

Devices that provides SNMP are

The purpose of SNMP is to provide network devices, such as routers, servers and printers, with a common language for sharing information with a network management system (NMS).

30. Define Hoax?

A hoax is a fake warning about a virus or other piece of malicious code. Typically a hoax takes the form of an e-mail or other message warning the reader of a dangerous new virus and suggesting that the reader pass the message on.

31. How to Protect File on computer?

Right-click on the folder or file and select Properties. Open the General tab, and select the Advanced button. Check the box next to Encrypt contents to secure data. After checking the box, select Apply and click OK.

32.Hot Site, Warm Site & Cold Site?

Hot Site is most expensive type of data replication. Data is replicated on two separate servers. One is operational and other is at different location.
Warm Site data replication occur from once every 24 hours to once a week. In event of disaster, it provide day-old data.
Cold Site is cost effective because do not need to purchase duplicate machines. Data is sent either on tape or on shared hardware on internet.

LONG QUESTION

1. Email Security in Detail?

Email security is the process of ensuring the availability, integrity and authenticity of email communications by protecting against the risk of email threats.

Since the earliest days of email, it has been abused and misused in different ways with no shortage of email threats. Abuse of email includes the following:

- phishing attempts
- spoofing
- spam phishing
- malware delivery
- business email compromise (BEC)
- denial of service (DoS) attacks

Email security aims to help prevent attacks and abuse of email communication systems.

How secure is email?

By default, email is not secure for a variety of different reasons.

The original implementation of email protocols, including Simple Mail Transfer Protocol, Internet Message Access Protocol and Post Office Protocol 3, did not mandate the use of secure transport mechanisms, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

As such, connections to and from an email server were not done over an encrypted tunnel, which means that an intercepted message could have potentially been read by anyone.

Why is email security important?

Email is used for business communications and is often a foundational element of an organization's IT operations and ability to communicate both inside and outside of the company.

A risk to email, such as a lack of access due to a DoS attack, can potentially restrict the ability of a business to conduct business. Spam, which is another key email threat, can have negative impacts on a business, including filling up inboxes with useless information and potentially leading to phishing attacks.

Email can also often include sensitive data that is intended only for the recipient of an email message. Without email security, the sensitive information could be leaked to an unauthorized entity.

What are the benefits of email security?

As most organizations continue to rely on email for business operations, email security technologies and best practices provide several critical benefits for business of all sizes, including the following:

Availability. At the most basic level, email security can help to ensure the continued availability of email services so a business can continue to communicate with its employees and customers.
Authenticity. Having email authenticity measures in place can help to build trust for an organization and its users that email coming from its domain is authentic.
Fraud prevention. The ability to identify potential email security risks, such as spoofing, can potentially help an organization to reduce the opportunity for fraud.
Malware prevention. An appropriate set of security capabilities in place on an email platform can limit risks of malware transmitted by email.
Phishing protection. Phishing attacks can trick employees of a business to click on links or download things that could be harmful and lead to information disclosure and credential theft.

2. Solve All Steps of RSA with example?

Choose $p = 3$ and $q = 11$

Compute $n = p * q = 3 * 11 = 33$

Compute $\varphi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$

Choose e such that $1 < e < \varphi(n)$ and e and φ (n) are coprime. Let $e = 7$

Compute a value for d such that $(d * e) \% \varphi(n) = 1$. One solution is $d = 3$ $[(3 *7) \% 20 = 1]$

Public key is (e, n) => (7, 33)

Private key is (d, n) => (3, 33)

The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$

The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

3. Write down application and requirements for public key cryptosystem?

Applications for public-key cryptosystems

Encryption/decryption: sender encrypts the message with the receiver’s public key.

Digital signature: sender “signs” the message (or a representative part of the message) using his private key

Key exchange: two sides cooperate to exchange a secret key for later use in a secret key cryptosystem.

The main requirements of Public-key cryptography are:

1. Computationally easy for a party B to generate a pair.
2. Easy for sender A to generate ciphertext.
3. Easy for the receiver B to decrypt ciphertext using private key.
4. Computationally infeasible to determine private key (KRb) knowing public key (KUb)
5. Computationally infeasible to recover message M, knowing KUb and ciphertext C.
6. Either of the two keys can be used for encryption, with the other used for decryption.

4. Structure of AES?

AES:

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext.

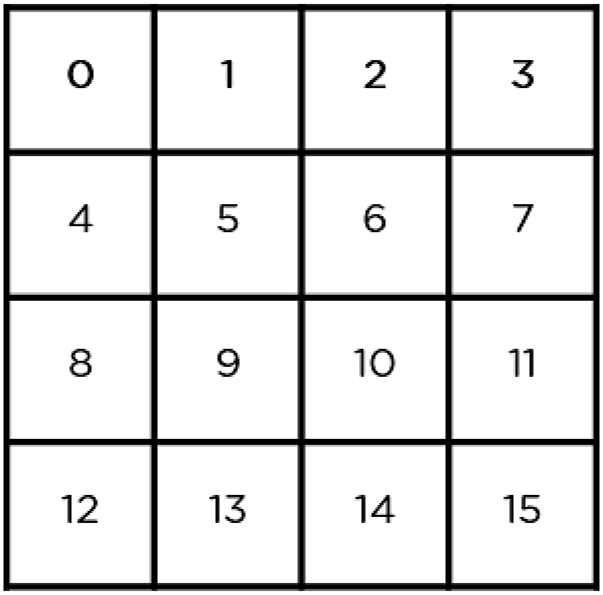
It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).

Features of AES:

- SP Network
- Key Expansion
- Byte Data
- Key Length

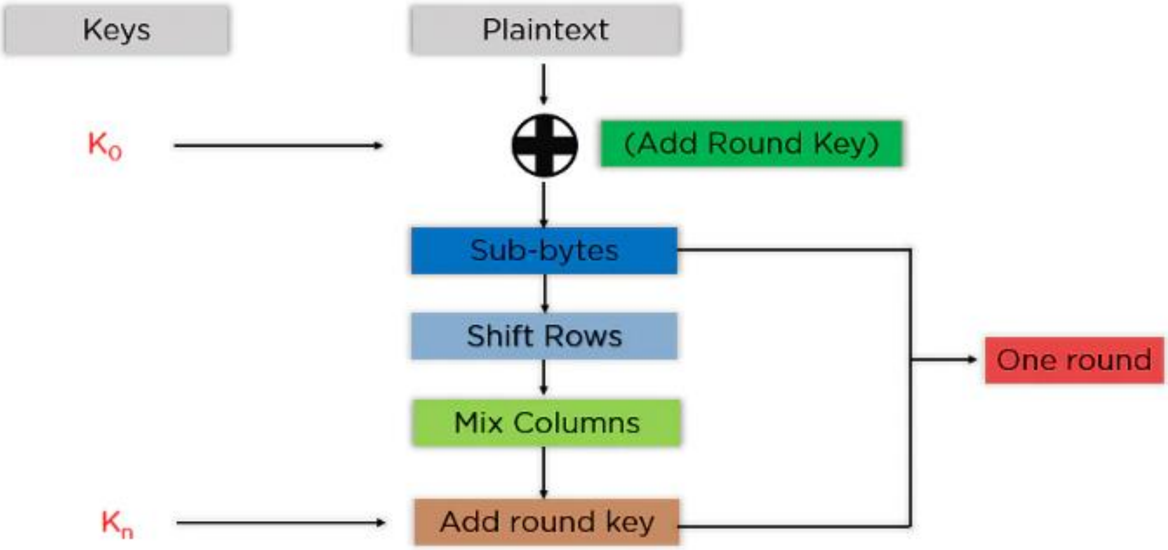
Structure of AES:

To understand the way AES works, you first need to learn how it transmits information between multiple steps. Since a single block is 16 bytes, a 4x4 matrix holds the data in a single block, with each cell holding a single byte of information.



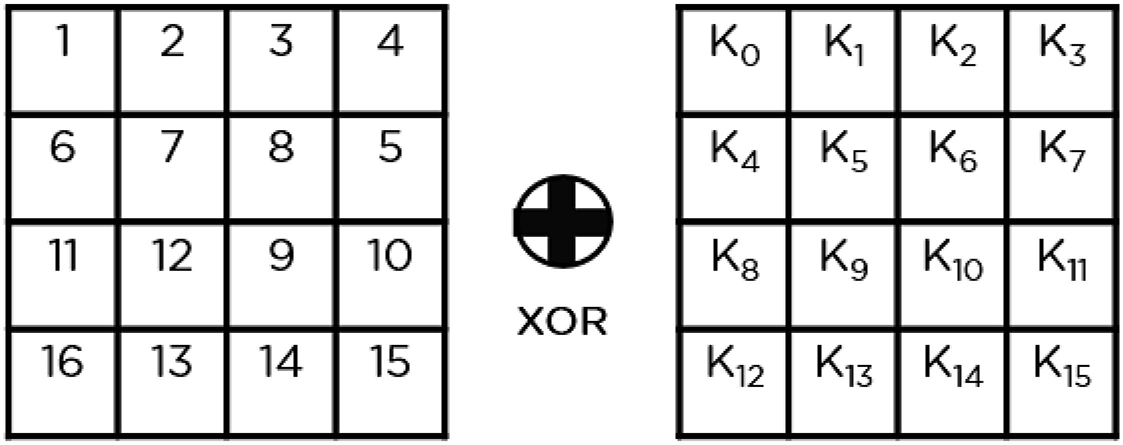
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

The steps to be followed in AES are in the below image.



The mentioned steps are to be followed for every block sequentially. The steps are as follows:

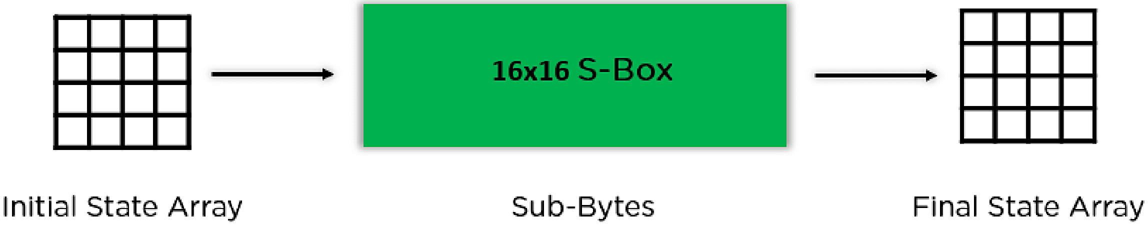
Add Round Key: You pass the block data stored in the state array through an XOR function with the first key generated (K0). It passes the resultant state array on as input to the next step.



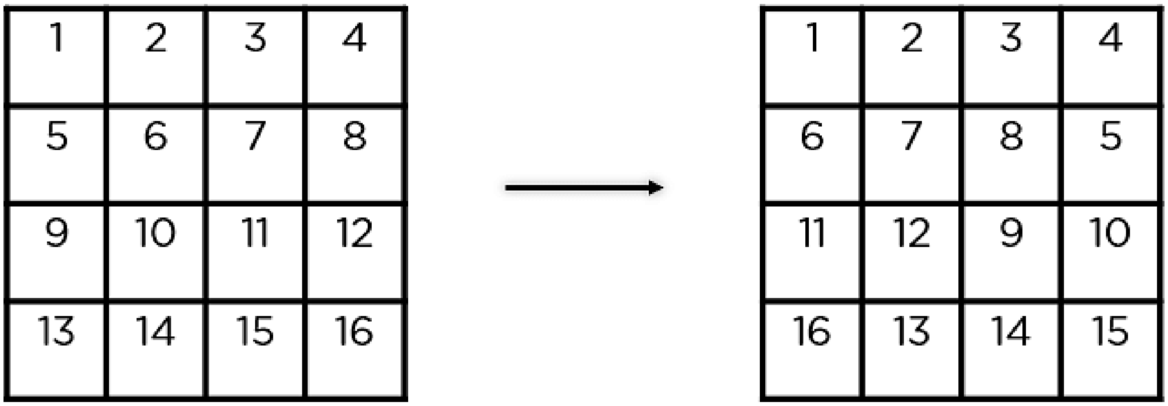
1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

Sub-Bytes: In this step, it converts each byte of the state array into hexadecimal, divided into two equal parts. These parts are the rows and columns, mapped with a substitution box (S-Box) to generate new values for the final state array.



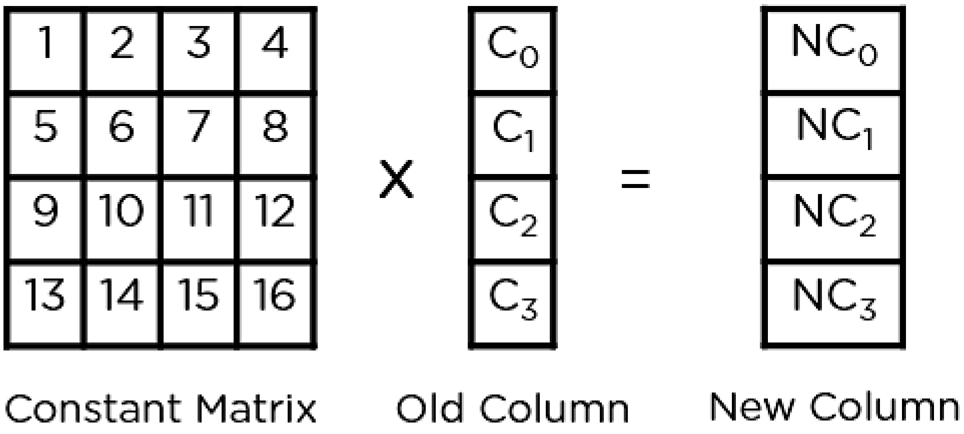
Shift Rows: It swaps the row elements among each other. It skips the first row. It shifts the elements in the second row, one position to the left. It also shifts the elements from the third row two consecutive positions to the left, and it shifts the last row three positions to the left.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

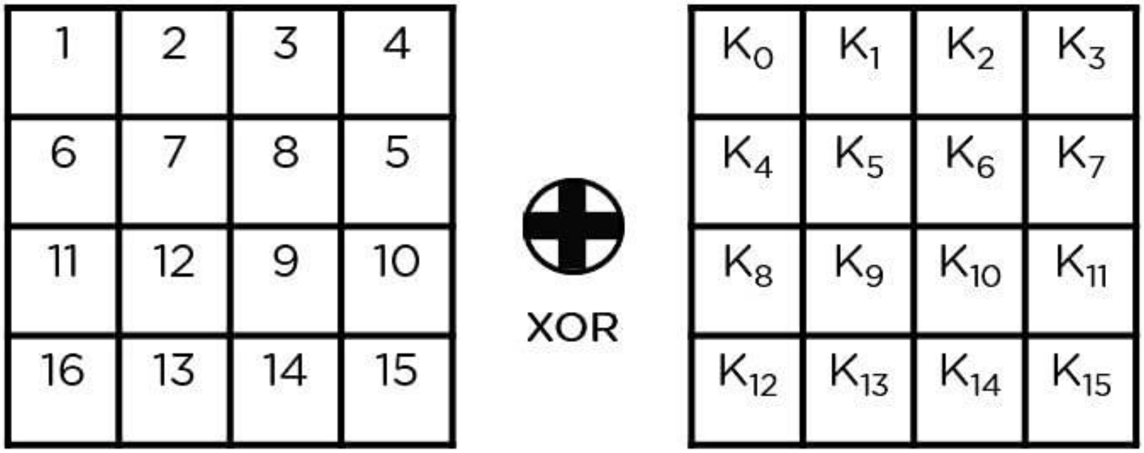
1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

Mix Columns: It multiplies a constant matrix with each column in the state array to get a new column for the subsequent state array. Once all the columns are multiplied with the same constant matrix, you get your state array for the next step. This particular step is not to be done in the last round.



$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix} \times \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} NC_0 \\ NC_1 \\ NC_2 \\ NC_3 \end{bmatrix}$$

Add Round Key: The respective key for the round is XOR'd with the state array is obtained in the previous step. If this is the last round, the resultant state array becomes the ciphertext for the specific block; else, it passes as the new state array input for the next round.



1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

5. How Asymmetric key distributed advantages of Asymmetric key?

Asymmetric Cryptography:
Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use.

A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key.
A private key -- also known as a secret key -- is shared only with key's initiator.

How Asymmetric Key Distributed:

Asymmetric Key Distribution is a unique scheme for generating and distributing unequal shares via a Trusted Dealer to all the registered peers in the system such that without the combination of the single compulsory share from the Special Server no transaction can be completed.

Asymmetric key distribution is an algorithm to ensure that the keys generated for such a scenario will not be symmetric and that authoritative power will remain in the hands of one Special Server. It ensures that no certificate can be signed legitimately without the signature of the Special Server.

Advantages of Asymmetric Key:

1. It allows message authentication.
As public key encryption allows using digital signatures, message recipients will be able to verify messages to be truly coming from a particular sender.
2. It is convenient.
Asymmetric encryption solves the problem of distributing keys for encryption, with everyone publishing their public keys, while private keys being kept secret.
3. It allows for non-repudiation.
Digitally signed messages are like physically signed documents. Basically, it is like acknowledging a message, and therefore, the sender will not be able to deny it.
4. It detects tampering.
With digital signatures in public key encryption, message recipients can detect if a message was altered in transit.

6. Explain Ceaser Cipher With Example? Pro’s and Con’s?

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

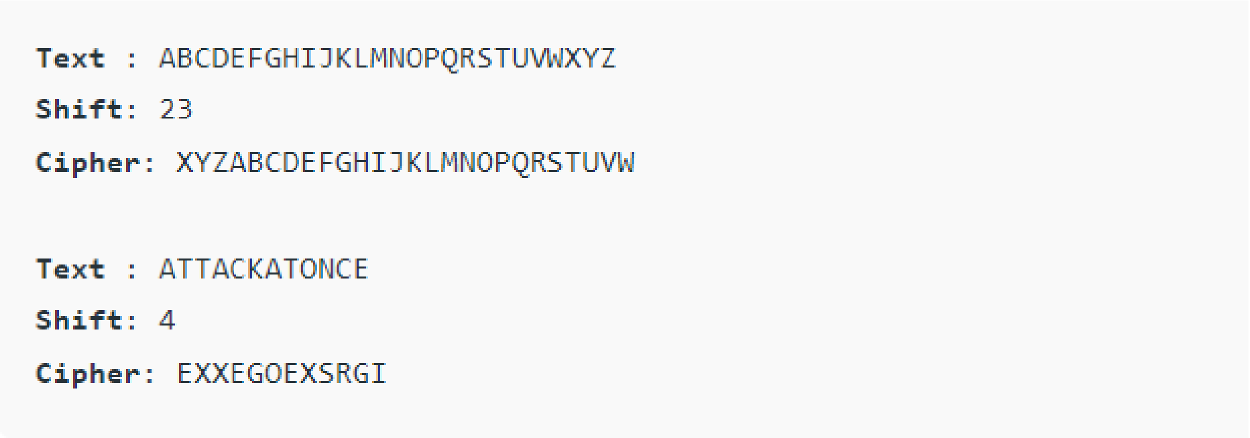
$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

EXAMPLE:



```
Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI
```

Algorithm for Caesar Cipher:

Input:

- A String of lower case letters, called Text.
- An Integer between 0-25 denoting the required shift.

Procedure:

- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
- Return the new string generated.

Program that receives a Text (string) and Shift value(integer) and returns the encrypted text.

Advantages of using a Caesar cipher include:

- One of the easiest methods to use in cryptography and can provide minimum security to the information
- Use of only a short key in the entire process
- One of the best methods to use if the system cannot use any complicated coding techniques
- Requires few computing resources

Disadvantages of using a Caesar cipher include:

- Simple structure usage
- Can only provide minimum security to the information
- Frequency of the letter pattern provides a big clue in deciphering the entire message

7. Explain difference between IDS & Firewall ? Define types of firewall?

IDS:

- An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
- Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts.
- Traffic Patterns are Analyzed.
- Alerts/alarms on detection of anomaly.

Firewall:

- Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules.

- Filters traffic based on IP address and port numbers.
- Layer 3 mode or transparent mode.
- Traffic Patterns are Not analyzed.
- It Blocks the traffic.

Different Types of Firewall:

There are four types of firewalls, which are all available on Linux platforms. These are, in order of complexity and features, packet filtering, application proxies, stateful inspection, and hybrid.

Packet Filtering: These are the first generation of firewalls, generally what you see on modern routers these days. While useful, they are generally trivial to circumvent an attacker using a number of common attack methods.

Application Proxies: This is the second generation of firewall technology, although it could be said this is actually the first in some ways. An application layer firewall is a proxy server, like the HTTP proxy server, Squid, for example. They also provide a layer of granularity into security policy that you won't find in stateful inspection or packet filtering firewalls. Basically, an application proxy is an application that runs on your firewall or gateway that relays traffic between you and your destination. The added advantage here is that the traffic is being sent/received between both endpoints by a third-party application, meaning you can enforce very specific guidelines on the way the traffic is crafted between both points.

Stateful Inspection: This would be the third generation of firewall technology, this is related to the packet filtering method, but it extends the capabilities of firewalling by continuing to inspect the packets as they pass through the firewall. Net filter/iptables is a stateful inspection type firewall. Net filter/iptables' main features are

- stateful packet filtering (connection tracking)

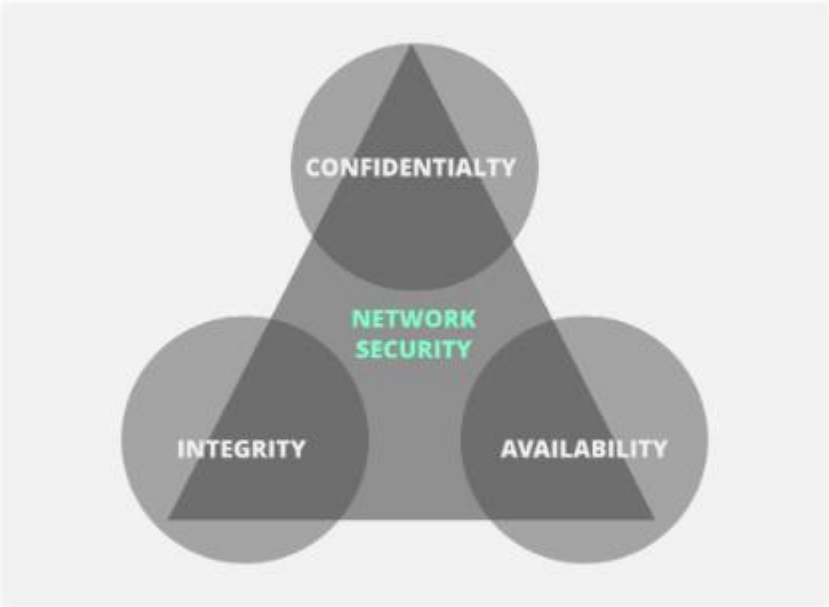
- all kinds of network address translation
- flexible and extensible infrastructure
- large number of additional features as patches

Hybrids: Hybrids are the fourth generation. They are a combination of the previous three, giving the users more control of the methods they intend to employ to carry out their firewall policy.

8. Role of CIA model in cryptography?

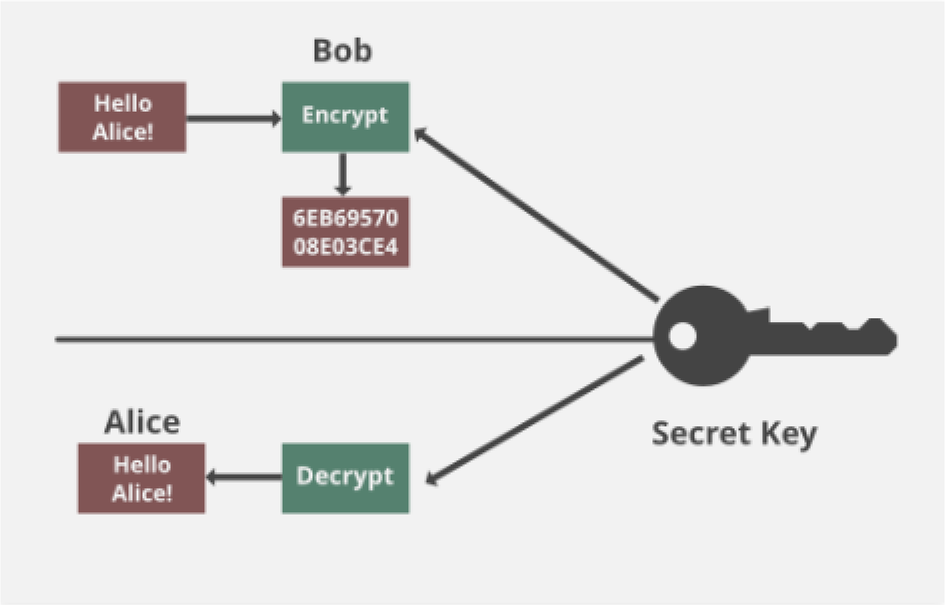
When talking about network security, the CIA triad is one of the most important models which is designed to guide policies for information security within an organization.
CIA stands for :

- Confidentiality
- Integrity
- Availability



1. **Confidentiality :**
   Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet

and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. Encryption standards include **AES** (Advanced Encryption Standard) and **DES** (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.



2. **Integrity :**

The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.

We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, SHA-3.

Let's assume Host 'A' wants to send data to Host 'B' maintaining integrity. A hash function will run over the data and produce an arbitrary hash value **H1** which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value **H2**. Now, if **H1 = H2**, this means that the data's integrity has been maintained and the contents were not modified.

3. **Availability:**

   This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.

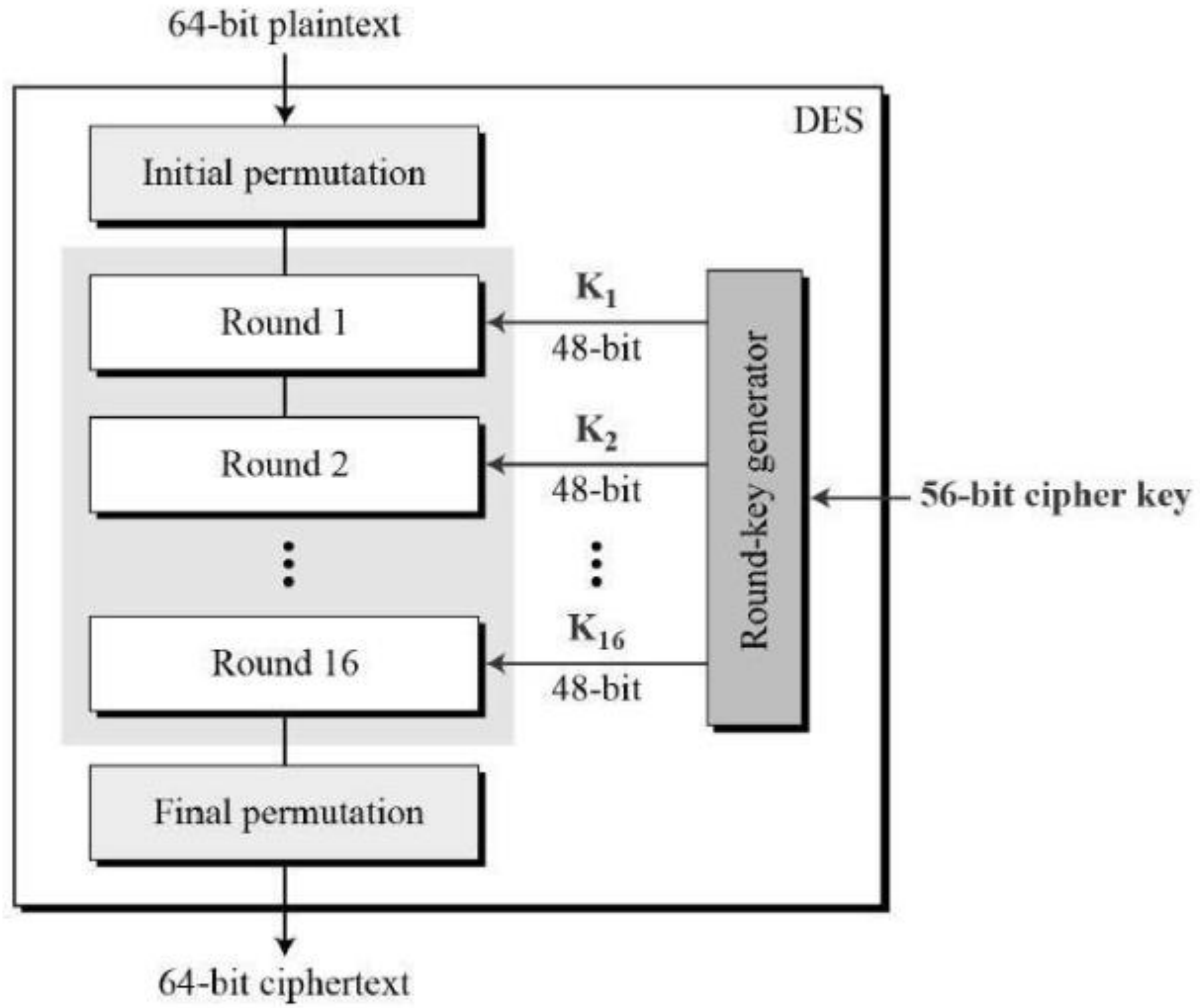
9. How will you ensure network layer security by protecting all assets?

10. Basic Structure of DES?

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

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

Basic Structure of DES is shown below:



Since DES is based on the Feistel Cipher, all that is required to specify DES is−

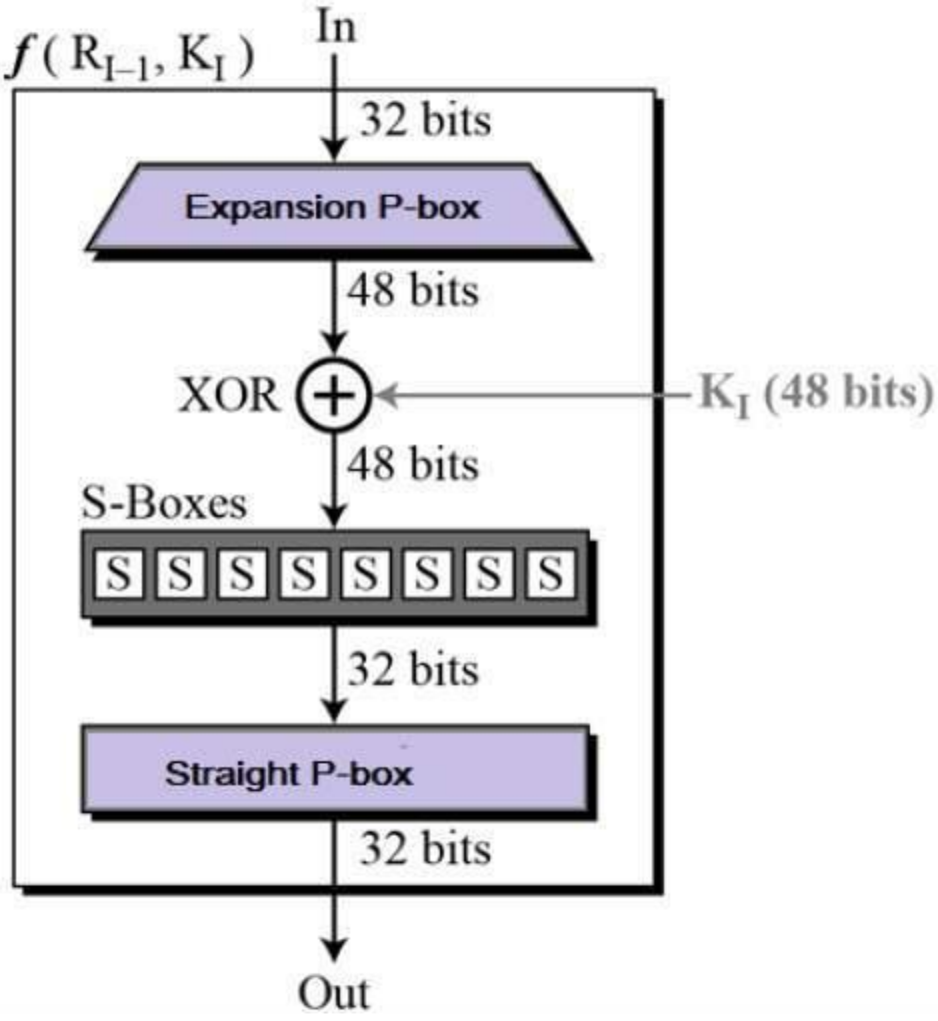
- Initial and final permutation
- Round function
- Key Generation

1) Initial and Final Permutation:

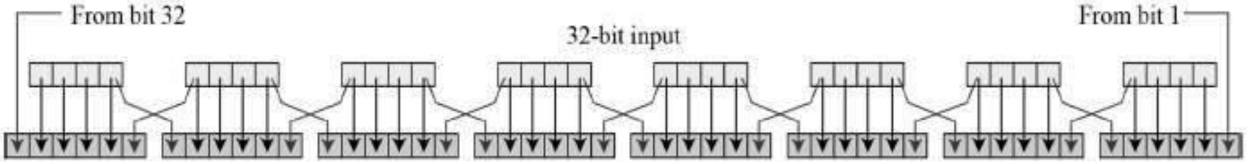
The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES

2) Round Function:

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



- **Expansion Permutation Box –**
  Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −

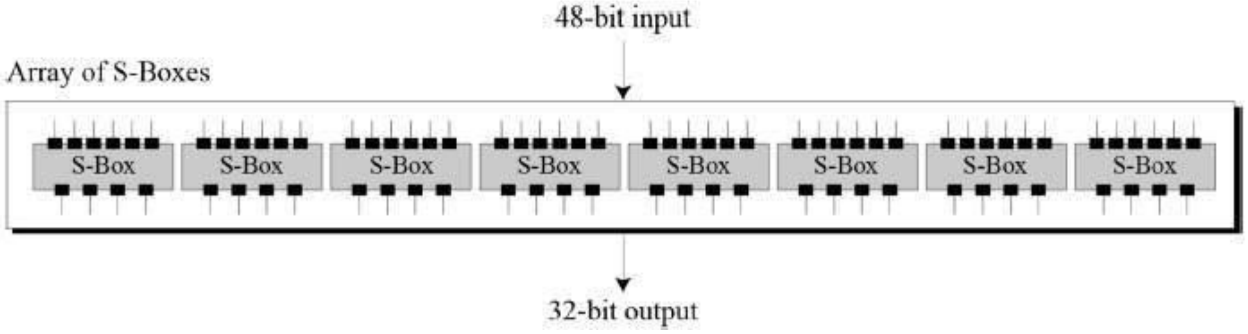


XOR (Whitener). –

After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

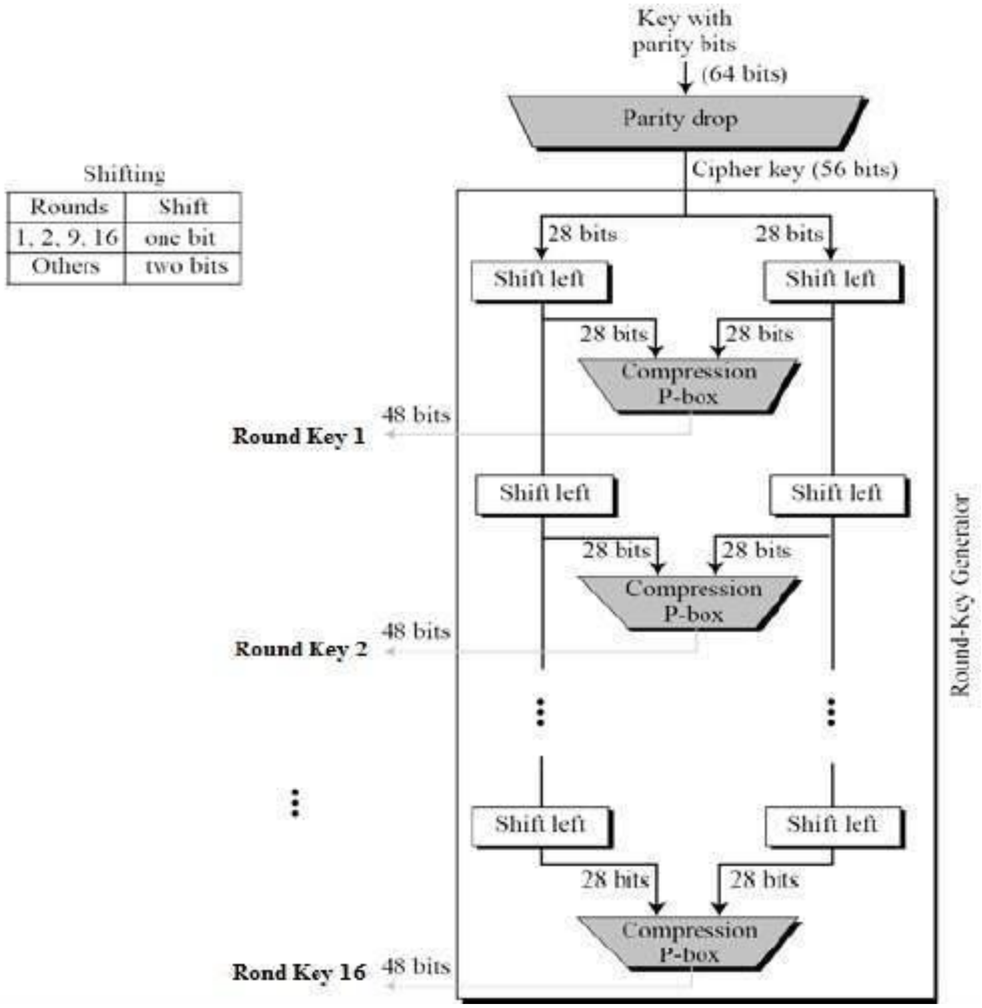
Substitution Boxes. –

The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration −



3) Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −

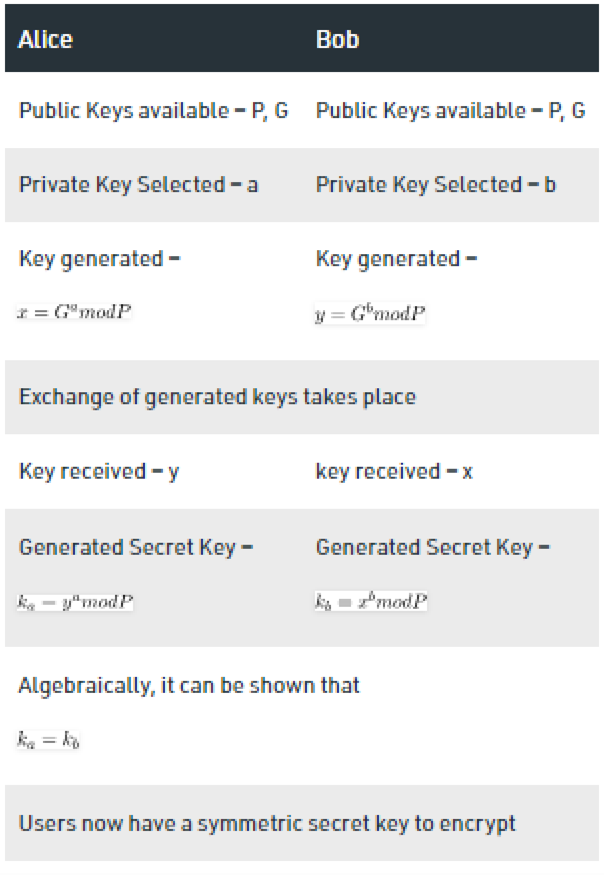


11. Write down Diffie Hellman Algorithm with example?

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

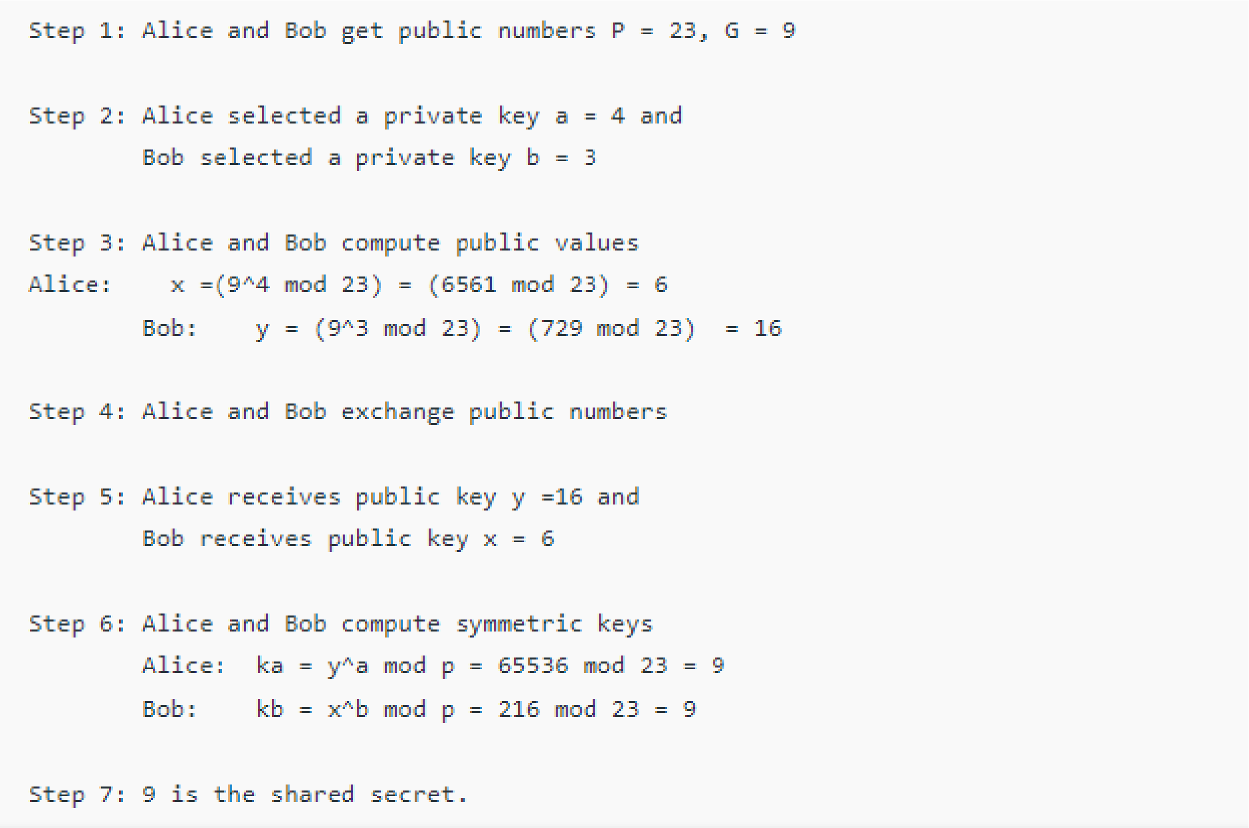
- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step by Step Explanation



Alice	Bob
Public Keys available - P, G	Public Keys available - P, G
Private Key Selected - a	Private Key Selected - b
Key generated - $x = G^a modP$	Key generated - $y = G^b modP$
Exchange of generated keys takes place	
Key received - y	key received - x
Generated Secret Key - $k_a = y^a modP$	Generated Secret Key - $k_b = x^b modP$
Algebraically, it can be shown that $k_a = k_b$	
Users now have a symmetric secret key to encrypt	

Example:



```
Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and
        Bob selected a private key b = 3

Step 3: Alice and Bob compute public values
Alice:    x =(9^4 mod 23) = (6561 mod 23) = 6
        Bob:    y = (9^3 mod 23) = (729 mod 23)  = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and
        Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys
        Alice:  ka = y^a mod p = 65536 mod 23 = 9
        Bob:    kb = x^b mod p = 216 mod 23 = 9

Step 7: 9 is the shared secret.
```

AAA MODEL:

Authentication, authorization and accounting provide security to Cisco IOS routers and network devices.

AAA provide methods for identifying users who are logged in to a router and have access to servers and concentrators. AAA also identifies the level of access that has been granted to each user and monitors user activity to produce accounting information.

Network data can be accessed via different methods include following:

- Dialup connections
- Integrated services and digital networks
- Broadband cable and asymmetric digital subscriber line
- Access through virtual private networks

The AAA model was designed in such a way that all these access methods can benefit from AAA security features.

The three phases ensure that only legitimate users are permitted access as explained as follows:

Authentication:

It is the process of verifying who someone is? Verification of who you are? Remote users must be authenticated before being permitted access.

Authentication allow the users to submit their usernames and passwords through a series of challenges and responses.

Authorization:

Authorization is the process of verifying what specific applications, files, and data a user has access to. It controls what you can do. Once the user is identified, the accessible resources are defined by authorization mechanism. Authorization defines what services users are permitted to access.

Accounting:

Tracking of what you have done. Timestamps, command history, and type of resources are examples of information collected by accounting mechanism.

Accounting allows network administrators to log and view what actions were performed, such as whether router was reloaded or configuration was changed. Accounting function allows network administrators to view which actions were performed and at what time.

TCP/IP Security Issues: LLL

- IP Address spoofing
- Covert Channels
- IP Fragments Attacks
- TCP Flags
- Connection Hijacking

PHYSICAL SECURITY OF NETWORK:

1) Outside and external security

- Electronic Fence
- Electromagnetic IDs
- Camera Systems
- Entrance Security
- Permanent Guards

2) Internal Security

3) Disaster recovery plans

- Hot Site
- Warm Site
- Cold Site

4) Personal Awareness

INTRUSION DETECTION SYSTEM:

1) Notification Alarms:

- False Positive
- False Negative

2) Signature Base IDS

Types of Signature Base IDS:

- Simple and stateful pattern matching
- Protocol decode based analysis
- Heuristic based analysis

3) Policy Based IDS

4) Anomaly Based IDS

5) Network IDS & Host IDS