# Chapter 9
# Network Management & Security

# Contents

- Introduction to Network Management
- Principles of Cryptography (Symmetric Key: DES, Asymmetric key: RSA)
- Key Exchange Protocols (Diffie-Hellman, Kerberos)
- VPN
- Overview of IP Security
- Firewall, Digital Certificate
- Next Generation Network (NGN)

# SNMP

- ***Simple Network Management Protocol (SNMP)*** *is an application–layer protocol defined by the* ***Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices.***

- *It is a part of* ***Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.***

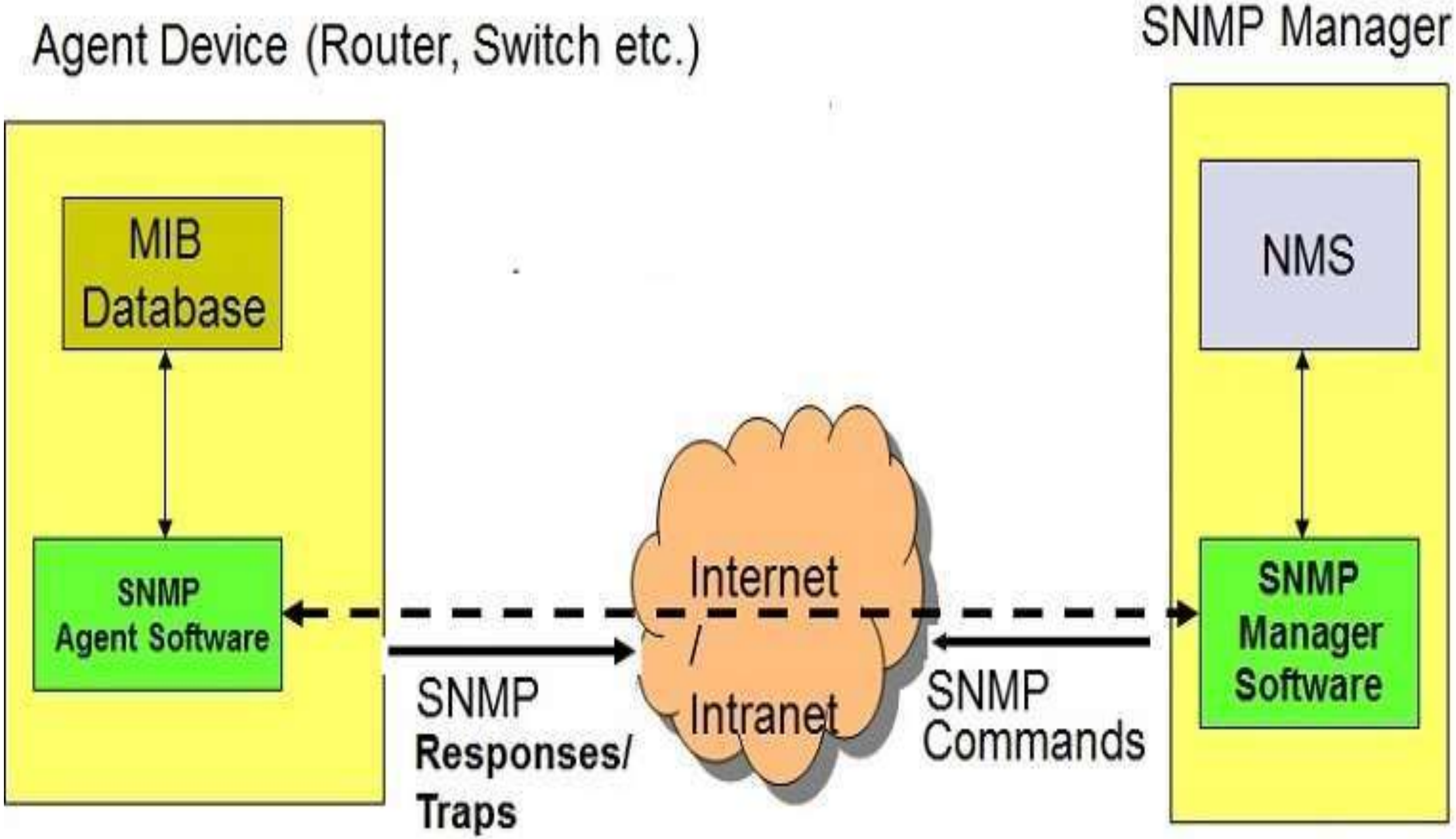
- ***SNMP is one of the widely accepted network protocols to manage and monitor network elements.***

# Components of SNMP

SNMP consists of

- **SNMP Manager**
- **Managed devices**
- **SNMP agent**
- **Management Information Base (MIB)**

# SNMP Architecture

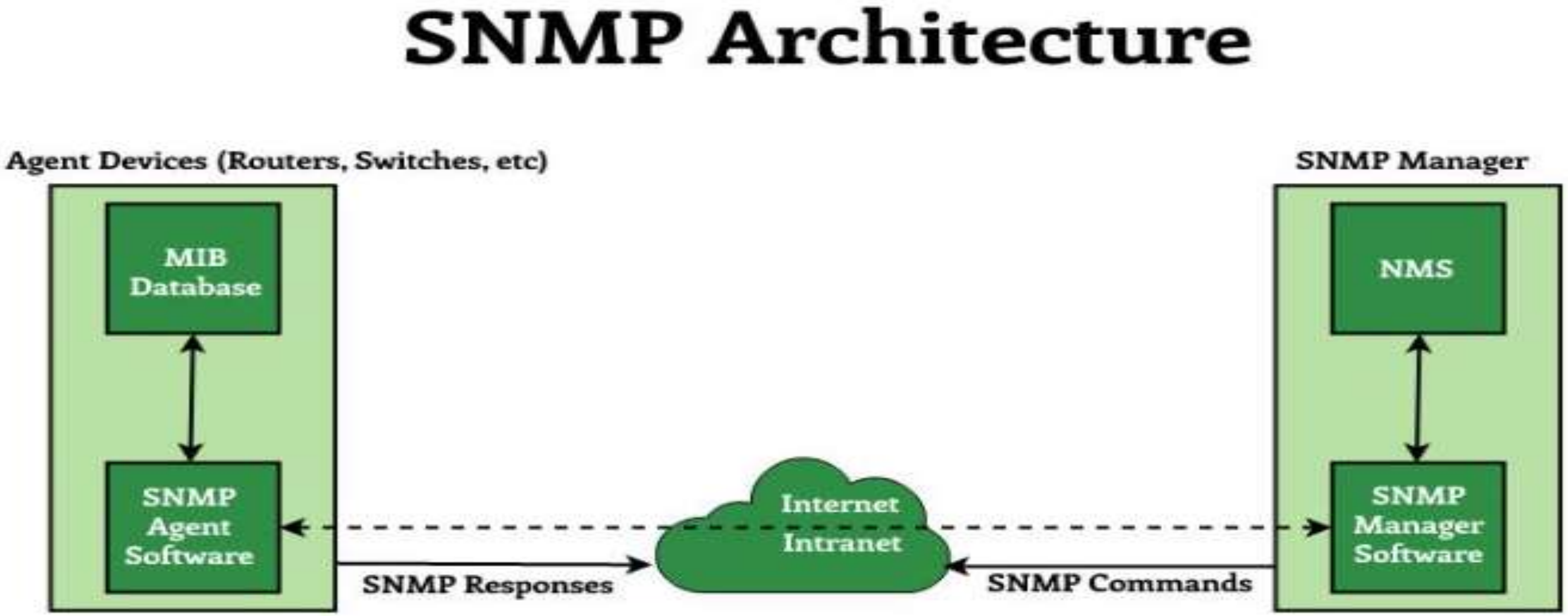


# Simple network management protocol

**Management with SNMP is based on three basic ideas:**

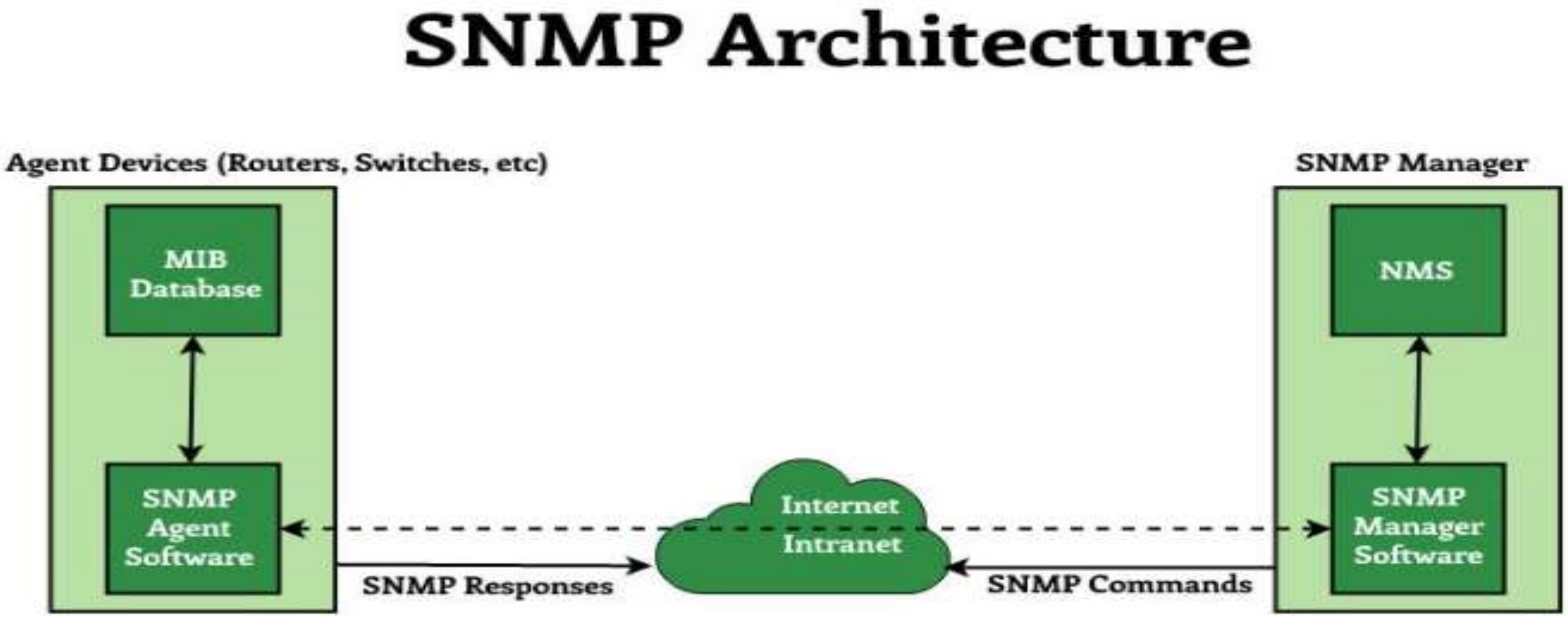
- A manager checks an agent by requesting information that reflects the behavior of the agent
- A manager forces an agent to perform the task by resetting values in he agent database
- An agent contributes to the management process by warning the manager of an unusual situation

**A model of network management looks like below**



# Simple network management protocol

- We know there are millions of hops, switches and routers; so it is a big network.
- Thus to monitor all these hops manually by user is really difficult.
- So for network management, a widely used standard is Simple Network Management Protocol (SNMP)
- For this mechanism, we do have SNMP agent and SNMP engine to monitor and control all the activities in the network.

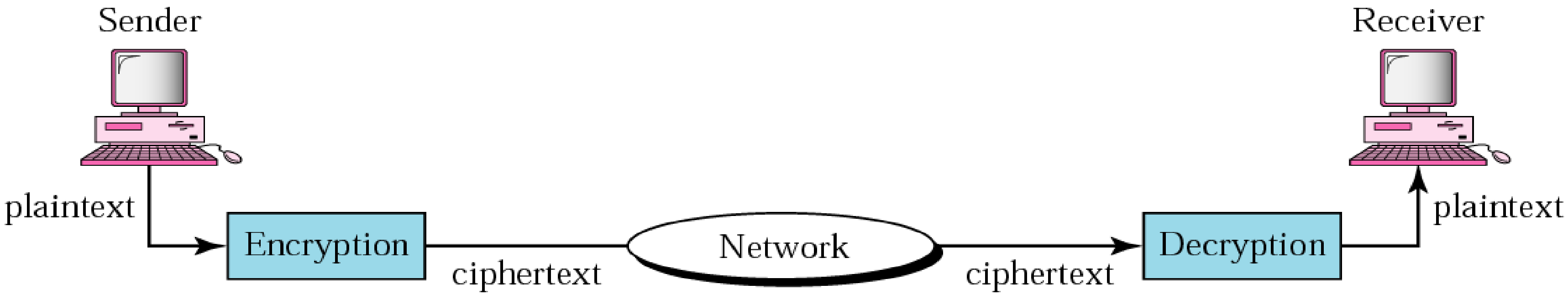


SNMP Architecture

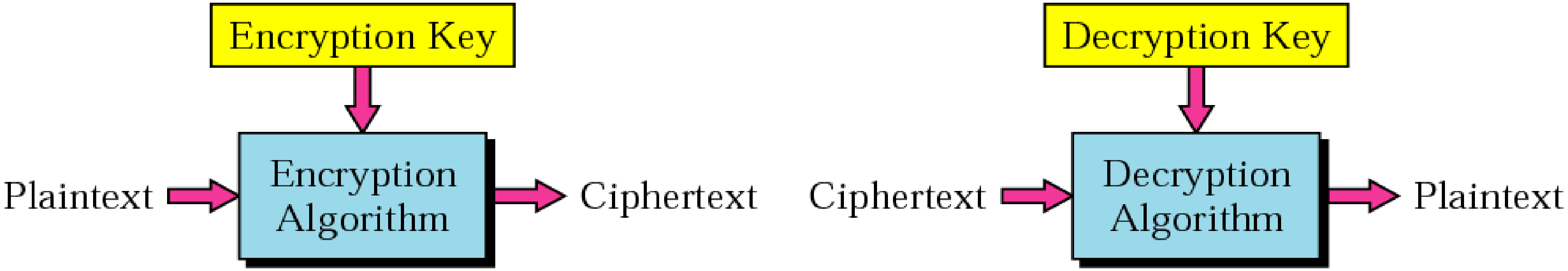
# Cryptography : What it is ??

- Cryptography in Greek means “Secret Writing”
- Science and Art of transforming message to make them secure and immune to attack.
- Original message before transformation => Plaintext.
- An Encryption algorithm transforms => Plaintext to Ciphertext.
- Decryption algorithm transforms => Ciphertext to Plaintext
- Cipher refers to different categories of algorithm in Cryptography.

# Cryptography : Components

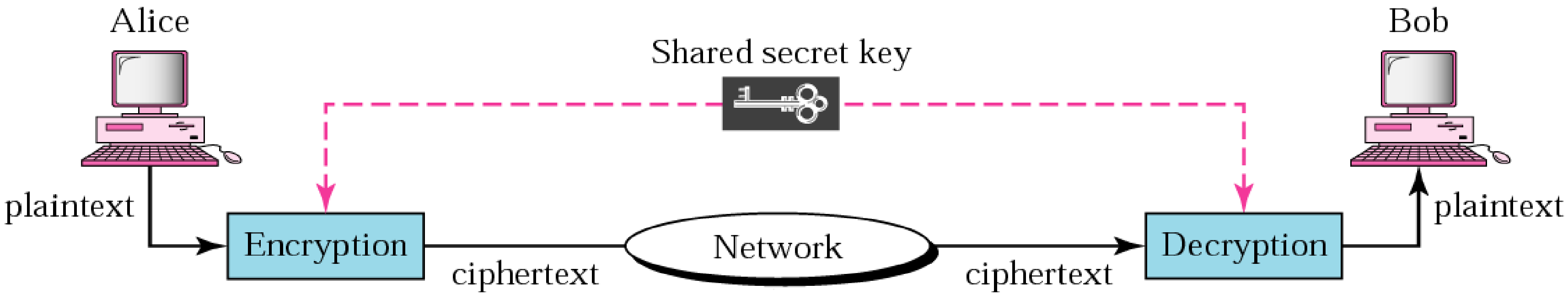


# Cryptography : Encryption and Decryption

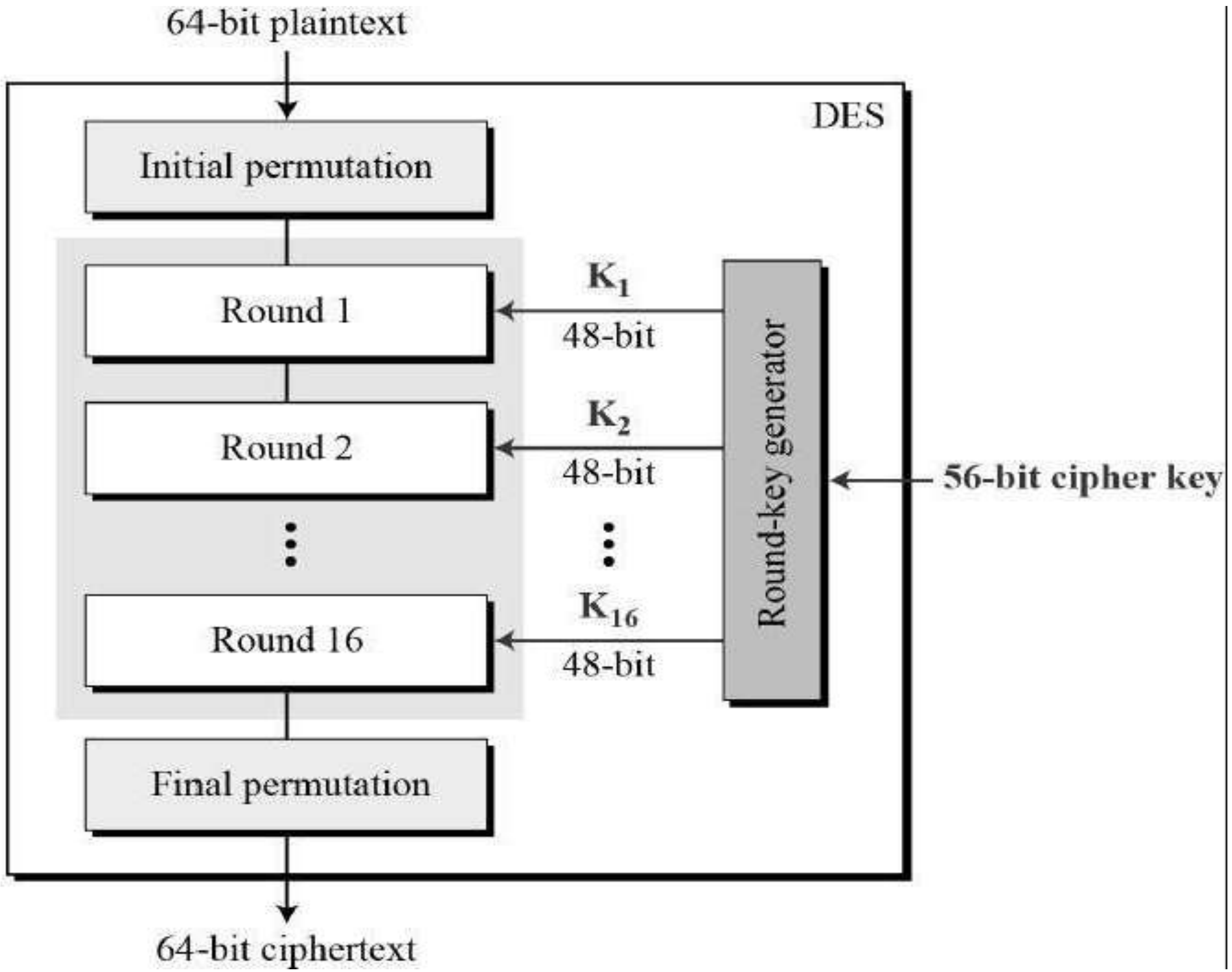


**a. Encryption** **b. Decryption**

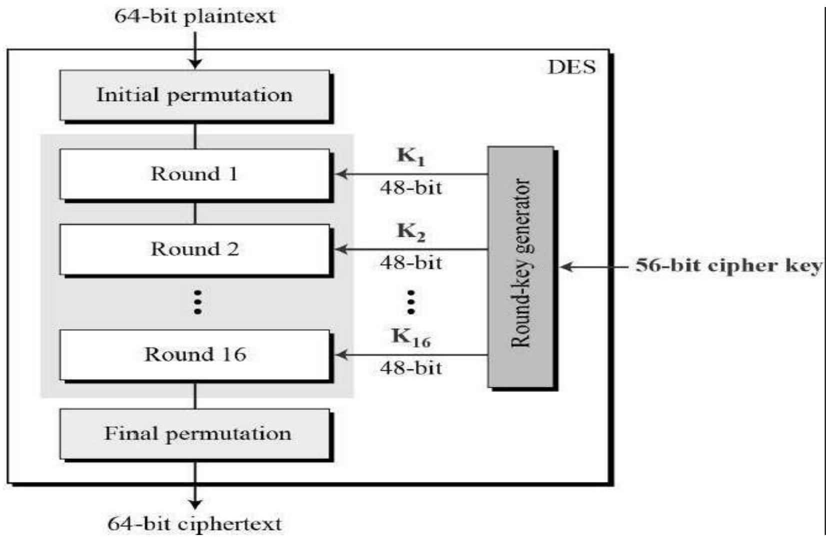
# Cryptography : Symmetric- Key Cryptography



# Data encryption standard (DES)

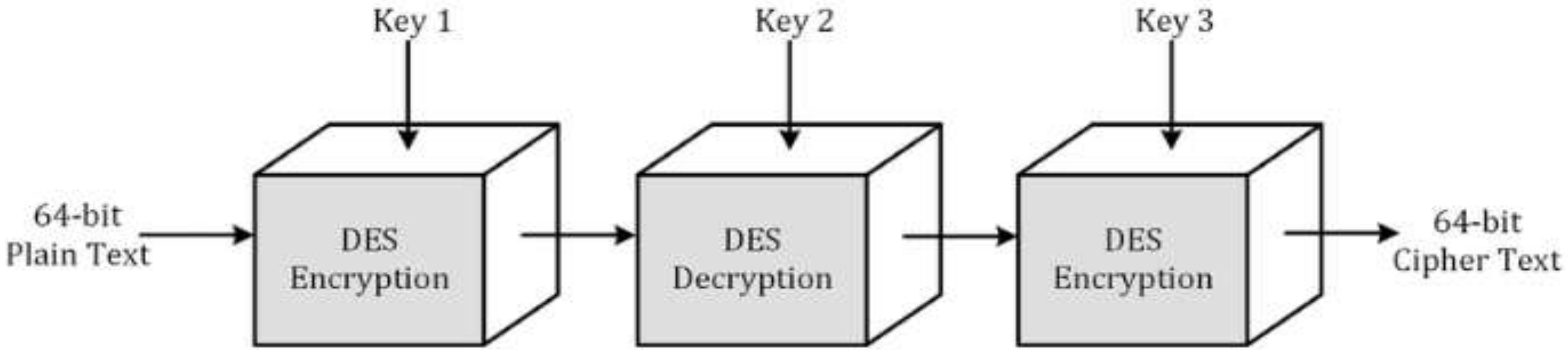


# Data encryption standard (DES)



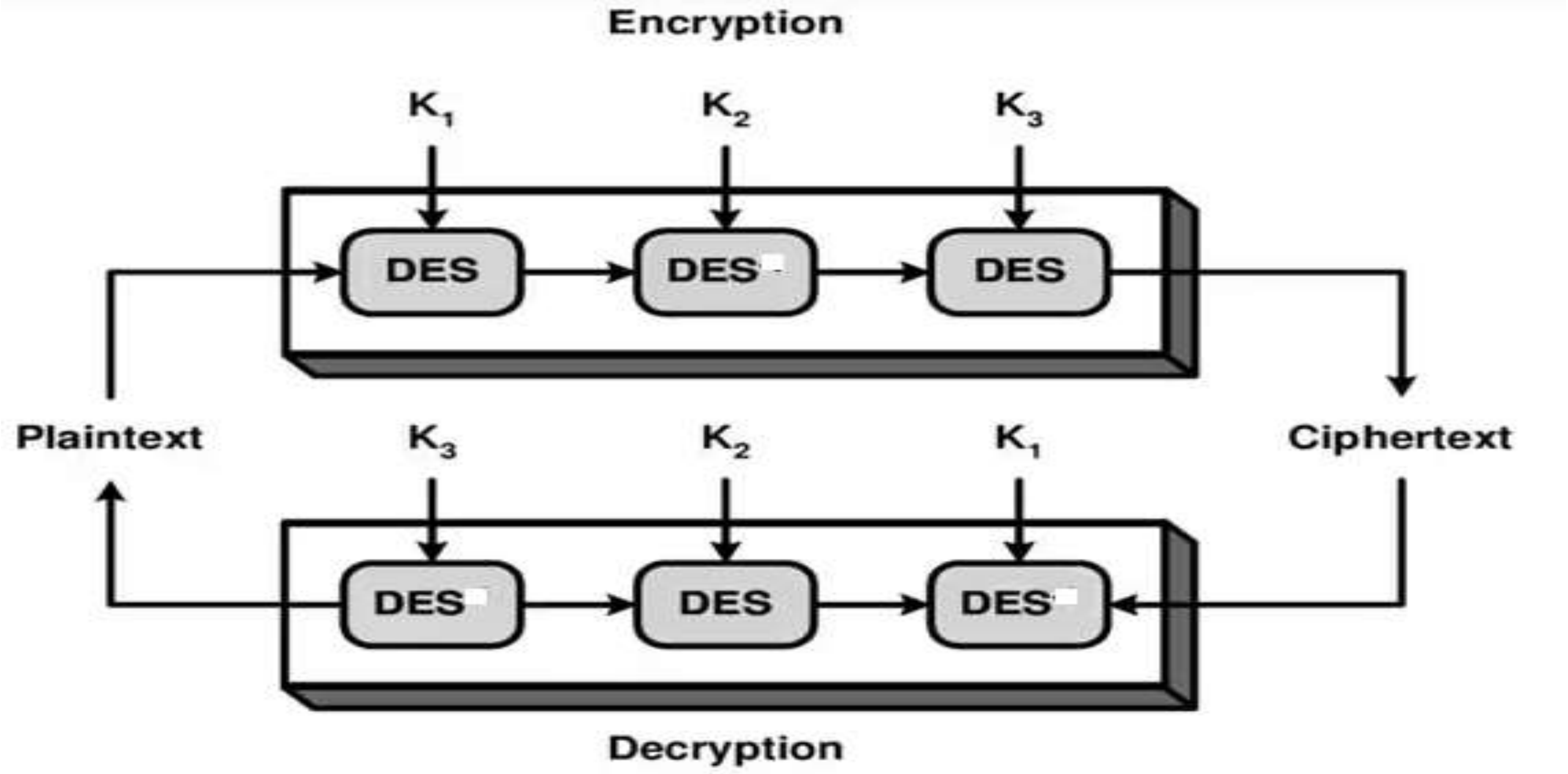
- Data encryption standard (DES) is the most widely used encryption standard.
- It was developed in the 1970s by the National Bureau of standards with the help of the national security agency
- Here the plain text is 64 bits in length and the key is 56 bits in length
  - First the 64 bit plain text passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 iterations of the same function
  - For every round we have different keys coming. Making keys by shifting procedure is of 16 rounds.

# Triple DES

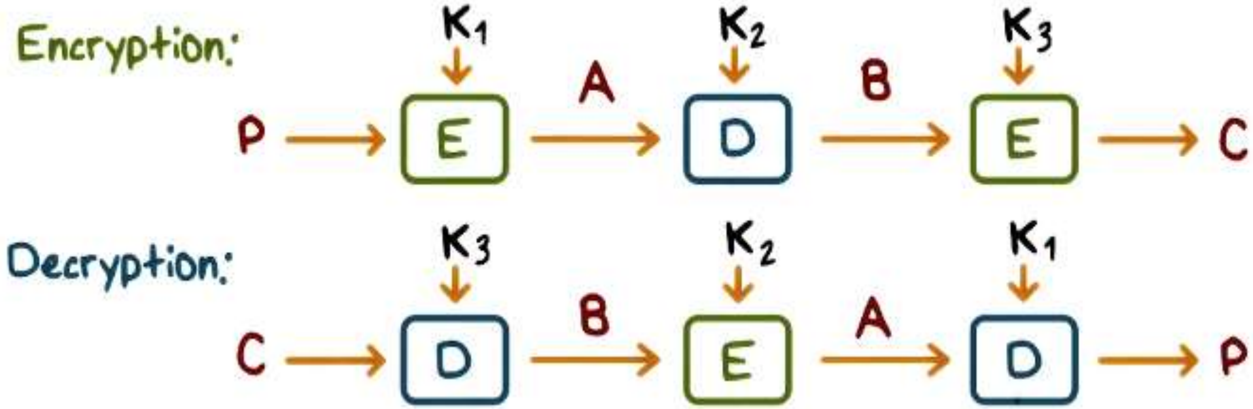

Key 1
Key 2
Key 3
64-bit
Plain Text
DES
Encryption
DES
Decryption
DES
Encryption
64-bit
Cipher Text

# Triple DES

- 3 DES uses three keys ad three executions of the DES algorithm. The function follows an encrypt-decrypt-encrypt sequence



# Triple DES



The Encryption scheme can be denoted as:

C = E($K_3$,D($K_2$,E($K_1$,P)))

- Encrypt plaintext using the key K1; decrypt using key K2 and encrypt the resultant using K3.

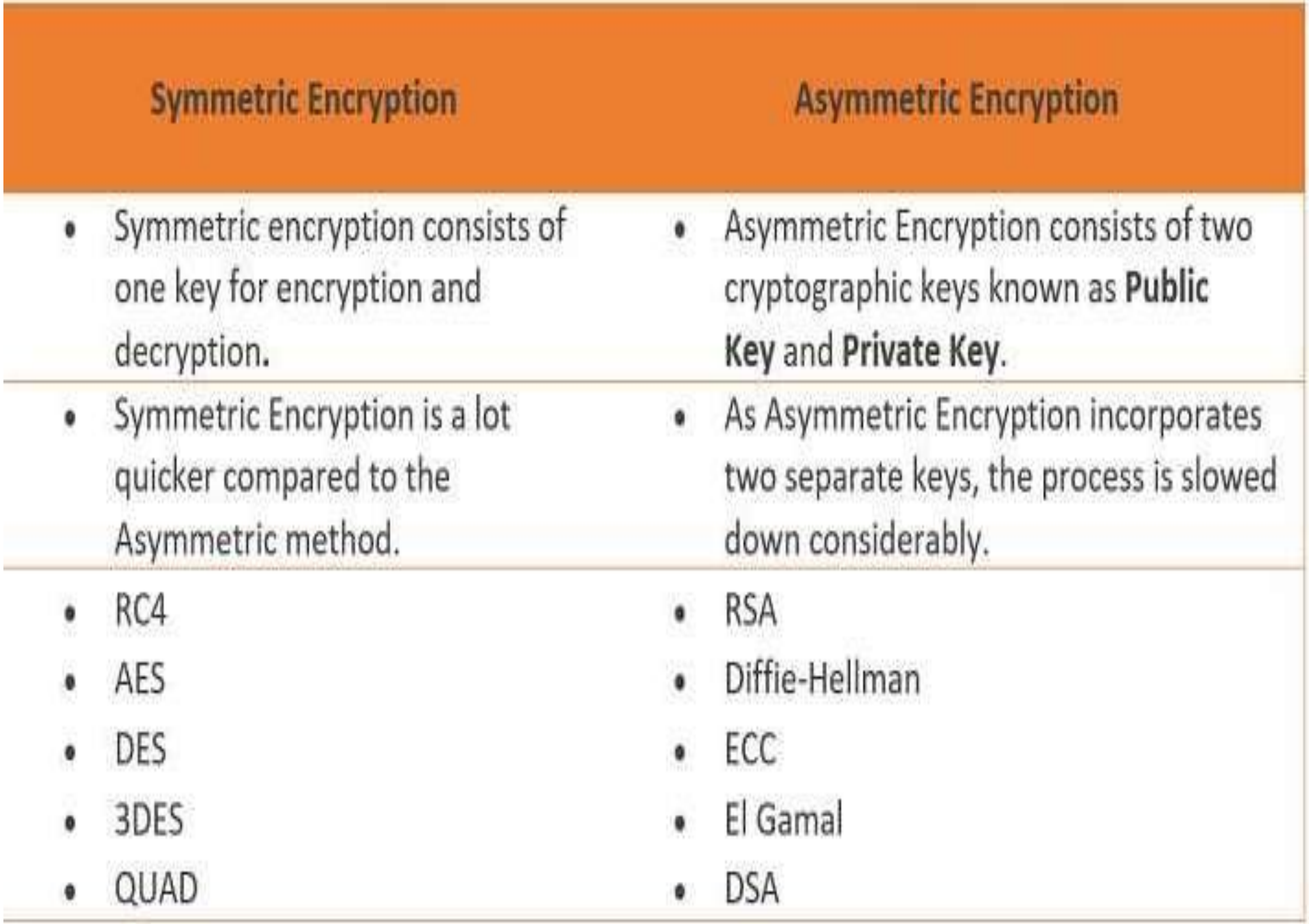
Similarly, the Decryption scheme can be denoted as:

P = E($K_1$,E($K_2$,D($K_3$,C)))

- Decrypt the plaintext using the key K3; encrypt using key K2 and decrypt the resultant using K1.

where:

P is the plaintext
C is the ciphertext
E[K,X] = encryption of X using key “K”
D[K,Y] = decryption of Y using key “K”



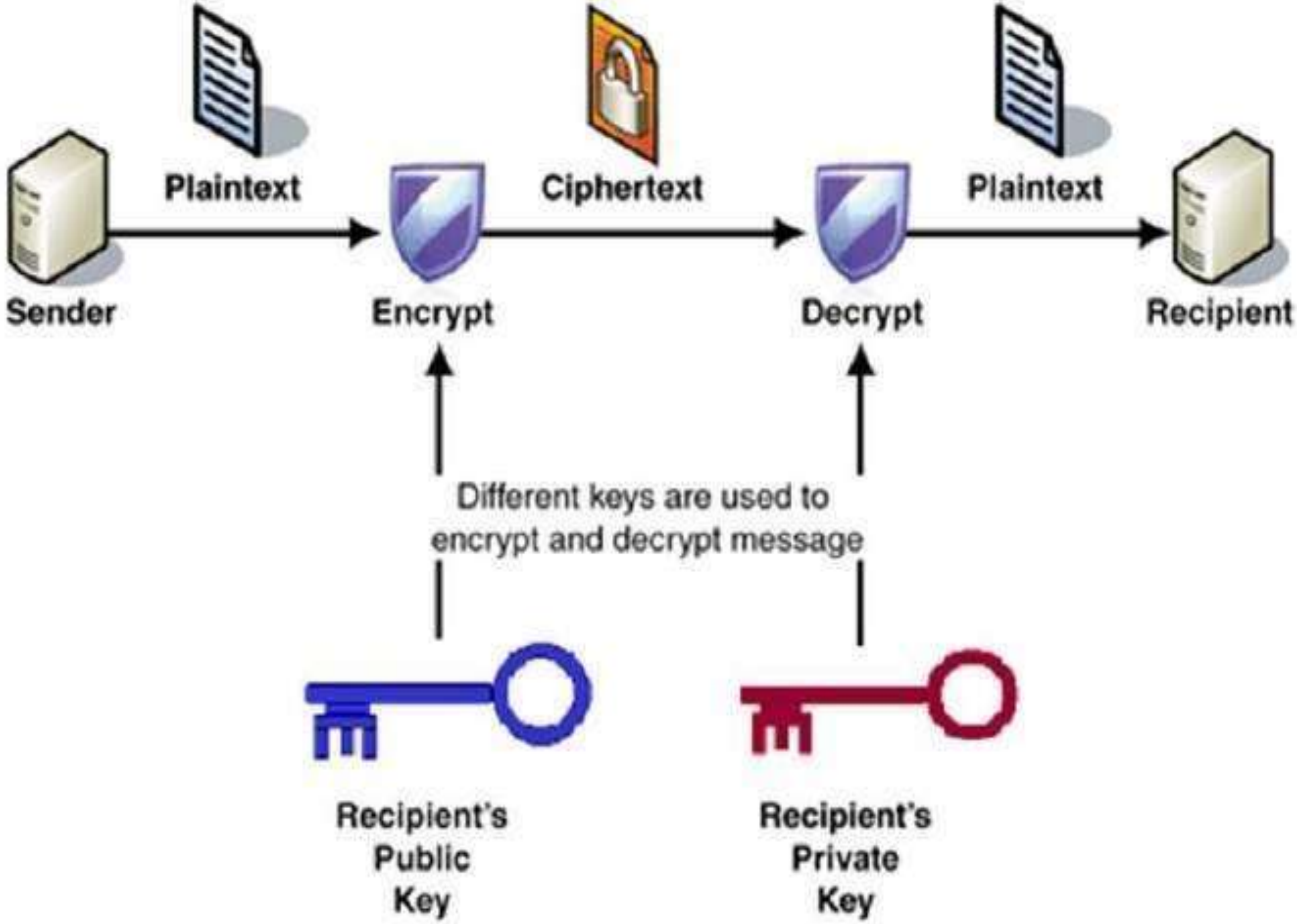
| Symmetric Encryption | Asymmetric Encryption |
|---|---|
| - Symmetric encryption consists of one key for encryption and decryption. | - Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**. |
| - Symmetric Encryption is a lot quicker compared to the Asymmetric method. | - As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably. |
| - RC4<br>- AES<br>- DES<br>- 3DES<br>- QUAD | - RSA<br>- Diffie-Hellman<br>- ECC<br>- El Gamal<br>- DSA |

# RSA

- **RSA (Rivest–Shamir–Adleman)** is a public-key cryptosystem that is widely used for secure data transmission.
- In a public-key cryptosystem, the **encryption key is public** and **distinct from the decryption key, which is kept secret (private).**
- RSA algorithm is **asymmetric cryptography** algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that **the Public Key is given to everyone and Private key is kept private.**

Example :

- A client (for example browser) sends its public key to the server and requests for some data.
- The server encrypts the data using client’s public key and sends the encrypted data.
- Client receives this data and decrypts it.



Plaintext

Ciphertext

Plaintext

Sender

Encrypt

Decrypt

Recipient

Different keys are used to
encrypt and decrypt message

Recipient's
Public
Key

Recipient's
Private
Key

# RSA Algorithm

## The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: **private key and public key.**

# RSA algorithm: Key Generation

- Generate two large prime numbers, p and q
- Let n=p*q
- Let m=(p-1)(q-1)
- Choose a small number e(1<e<m), such that GCD(e , m)=1
- Find d, such that d.e%m=1, where, d = (1+m*i)/e

(Go through the values of i until integer solution is found)

# RSA algorithm: Key Generation

- Publish e and n as the public key, i.e. (n , e)
- Publish d and n as the private key, i.e. (n , d)

**For encryption algorithm**

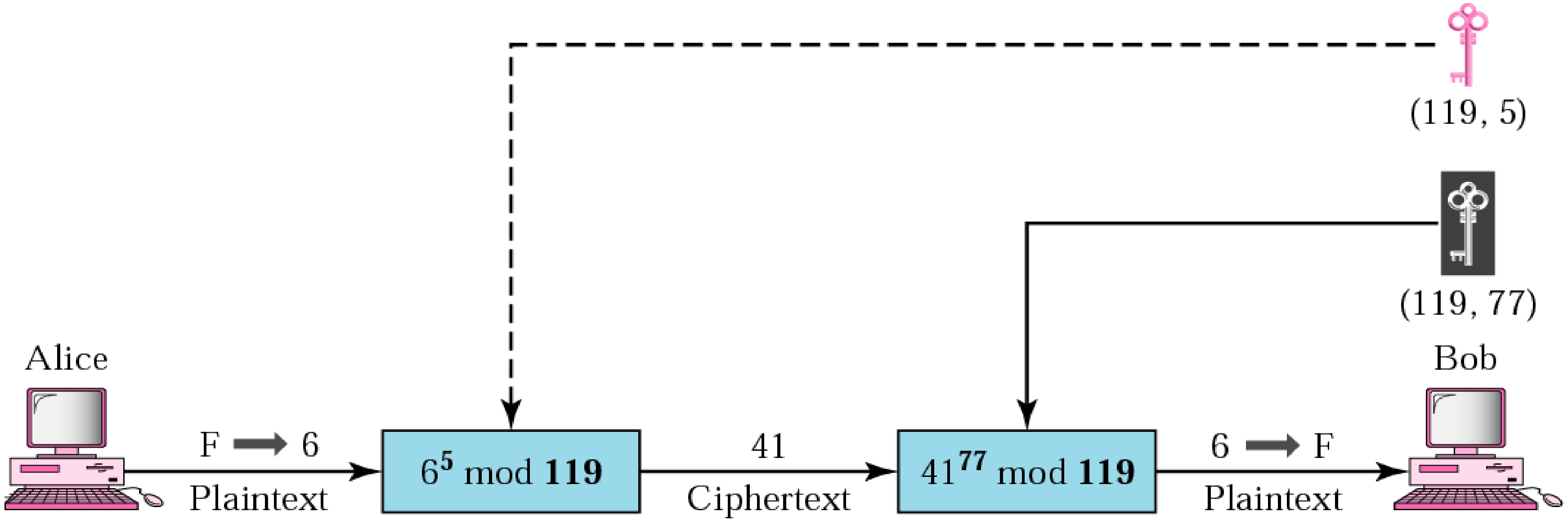
$C = P^{e}$ mod n

**For encryption algorithm**

P $= C^{d}$ mod n

# Public-Key Cryptography : RSA (Rivest, Shamir, Adleman)

Consider
public key pair➔ ( n, e ) ➔ (119,5)
private key pair➔ ( n, d ) ➔ (119,77)



# Public-Key Cryptography : RSA (Rivest, Shamir, Adleman)

- RSA encryption is intended primarily to provide confidentiality
- RSA cannot provide integrity
- It is highly required to maintain secrecy and integrity

# Diffie Hellman key exchange protocol

- The purpose of the algorithm is to enable two users to exchange a secret key securely
- The algorithm itself is limited to the exchange of the keys

# Diffie Hellman key exchange protocol

| Alice | | |
|---|---|---|
| Shared Key | Secret Key | Calculation |
| (g , p) = (5, 23) | | |
| | x = 6 | $g^x$ mod P = result1<br>$5^6$ mod 23 = 8 |
| | | result2 = 19 |
| | | $(result2)^x$ mod P<br>$19^6$ mod 23<br>= 2 |

| Bob | | |
|---|---|---|
| Shared Key | Secret Key | Calculation |
| (g , p) = (5, 23) | | |
| | x = 15 | $g^x$ mod P = result2<br>$5^{15}$ mod 23 = 19 |
| | | result1 = 8 |
| | | $(result1)^x$ mod P<br>$8^{15}$ mod 23<br>= 2 |

# Diffie Hellman (DH) key exchange protocol

- Alice and Bob agree to use the same two numbers.

  For e.g.,

  the base number, g = 5 and

  prime number, p= 23

- Alice now chooses a secret number, x = 6
- Alice performs the DH algorithm: $g^x$ mod P = $5^6$ mod 23 = 8 and sends the new result1 to Bob
- Meanwhile, Bob has also chosen a secret number x = 15, performed the DH algorithm: $g^x$ mod P = $5^{15}$ mod 23 = 19 and sends the new result2 to Alice
- Alice now computes $(result2)^x$ mod P = $(19)^6$ mod 23 = 2
- Bob now computes $(result1)^x$ mod P = $(8)^{15}$ mod 23 = 2

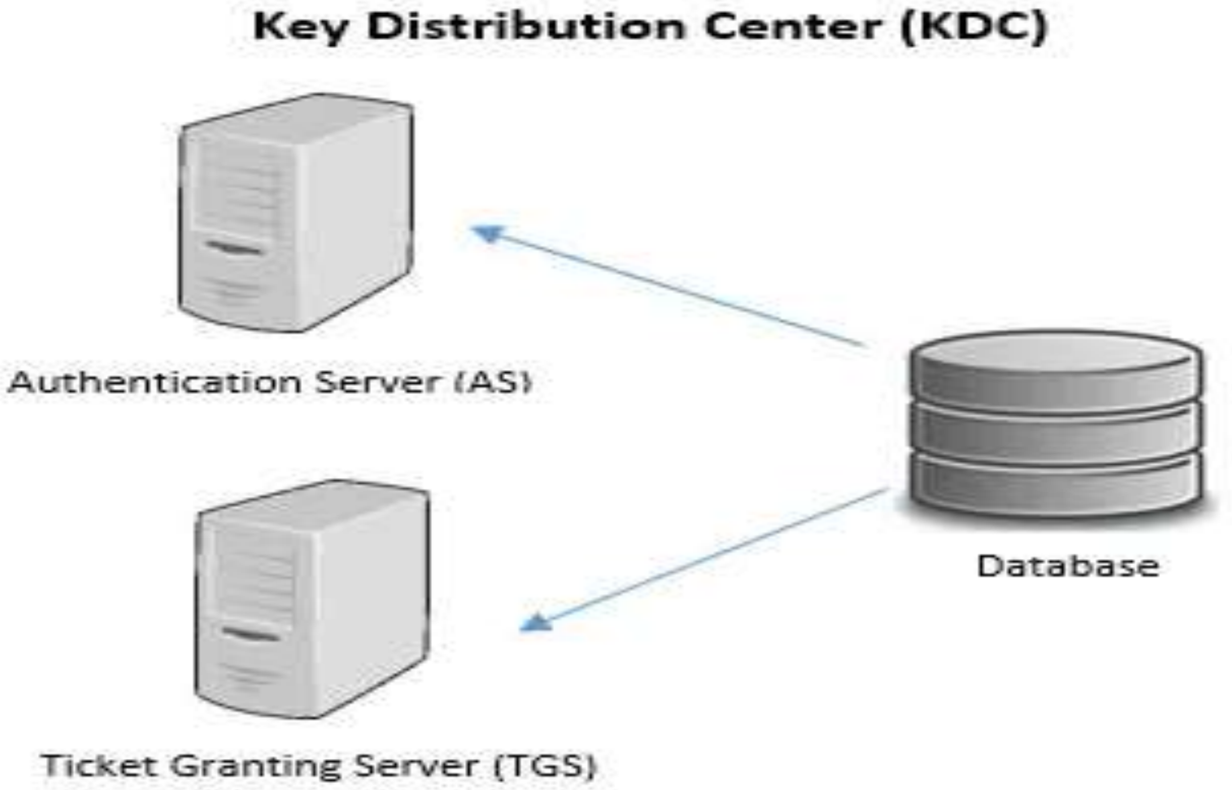
**“The obtained value i.e. 2 is same for both Alice and Bob. Hereby this number can be used as a shared secret key by the encryption algorithm”**

# Diffie Hellman (DH) key exchange protocol

- Authentication = it is the identification of assurance of origin of information
- The main limitation of DH key exchange protocol is that it doesn’t authenticate the participants. So this key exchange protocol is vulnerable to attack
- This vulnerability can be overcome with the use of digital signatures and digital certificates

# Kerberos: The Computer Network Authentication Protocol

- Kerberos is a network authentication protocol that uses a Key Distribution Center (KDC) to authenticate clients and servers in a distributed computing environment.
- The KDC is a trusted third-party system that issues tickets to prove the identity of clients and servers. This allows for secure communication and prevents unauthorized access.


Key Distribution Center (KDC)
Authentication Server (AS)
Database
Ticket Granting Server (TGS)

# Kerberos: The Computer Network Authentication Protocol

***Here are some details about how Kerberos works:***

**Mutual authentication**

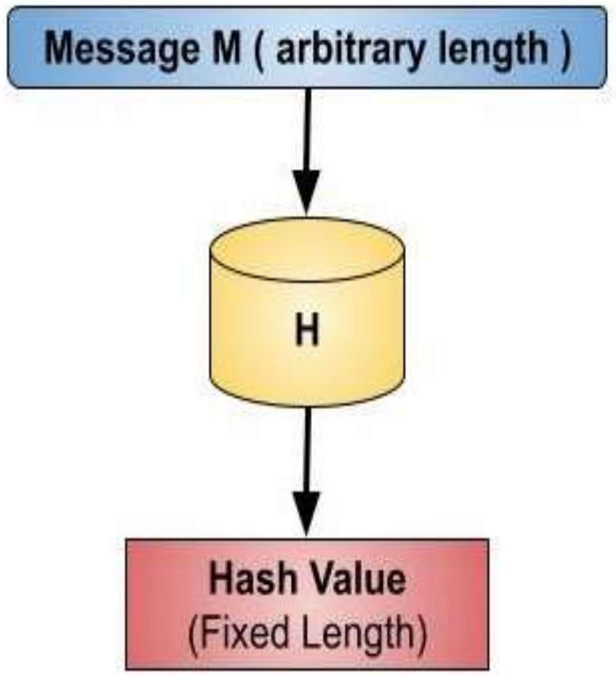
- Kerberos uses a shared secret key to authenticate both the client and server before any data is transferred.

- **Client authentication**
  - The client sends a user ID to the Authentication Server (AS) to request services. The AS checks to see if the client is in its database.
- **Ticket-granting service (TGS)**
  - The KDC uses the log-on session key to decrypt the user's authenticator message. If the authenticator passes, the KDC creates a session key for the user to share with the targeted server.

**Kerberos was originally developed in the 1980s by computer scientists at MIT. The goal of Kerberos is to authenticate users without sending passwords over the internet.**

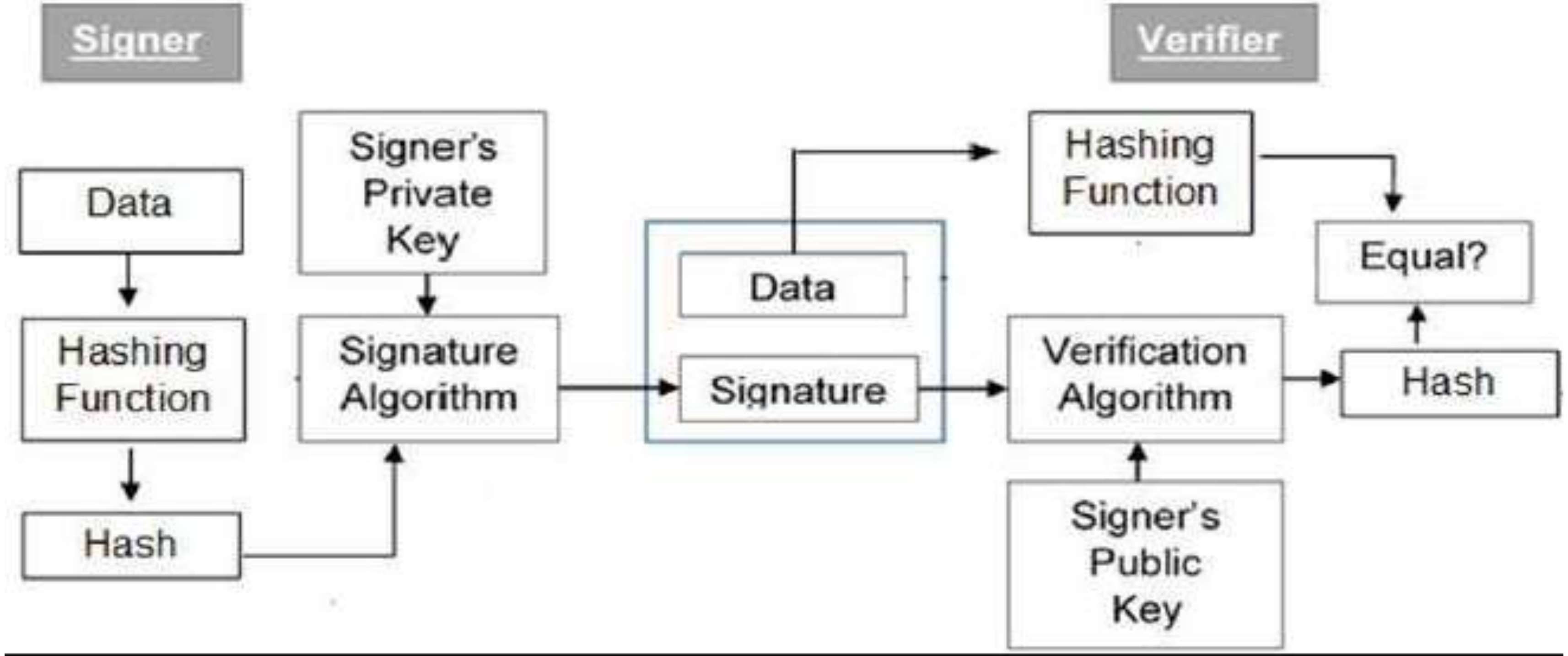
# Hash Function

- It is also known as message digest or fingerprint
- Hash function is irreversible
- One way  transformation
- One way function
- Length of H(m) is much shorter than length of m
- Usually fixed lengths: 128 or 160 bits
- Hash creates an identifiable signature of data
- It is possible to verify the integrity of data

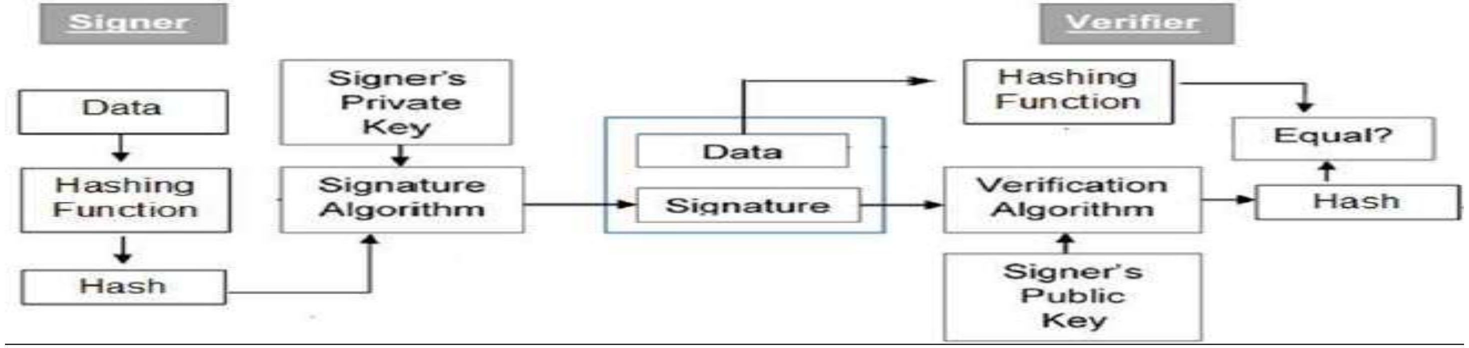


# Hash Function Application -  Digital signature

- Digital signature is an electric analogue of a written signature.
- It can be used to provide assurance that the claimed signatory signed the information
- It validates the integrity of signed data



# Digital Signature



- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by ‘private’ key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

# Digital Certificate

- Digital certificate can be obtained from a locally trusted 3$^{rd}$ party
- Or you can set up a locally trusted certification authority (CA) server within your own organization to provide digital certificates
- It is a kind of identification document that you can use to prove your identity in message or electronic transaction over the internet

# Firewall : What it is ??

- □ A Firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

- □ The use of single choke point simplifies security management because security capabilities are consolidate on a single system.

- □ A Firewall provides a location for monitoring security-related events.

- □ Audits and Alarms can be implemented on the Firewall system.

**Basically, firewalls is used to prevent network intrusion to the private network. So we can say firewall is a dedicated appliance or software running on another computer which inspects network traffic passing through it.**

# Firewall : Design goals ??

- All Traffic from inside to outside and vice versa must pass through the Firewall.
- It is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The Firewall itself is immune to penetration. => Trusted System with secure Operating Systems.

# Firewall : Control Access Methods?

1. Service Control

- □ Filter traffic on the basis of IP address or TCP Port Address.
- □ Example : Block Port 80, Allow Port 23

2. Direction Control

- □ Determine the direction => Inbound/outbound.

3. User Control

- □ Internal or External Users.

4. Behavior Control

- □ Filter e-mail to eliminate Spam.

# Firewall : Types of Firewall

## 1. Packet Filtering Router

- □ It applies a set of rules to each incoming IP Packet.
- □ The router is configured to filter packets going in both directions.
- □ Filtering rules are based on IP and Transport header.

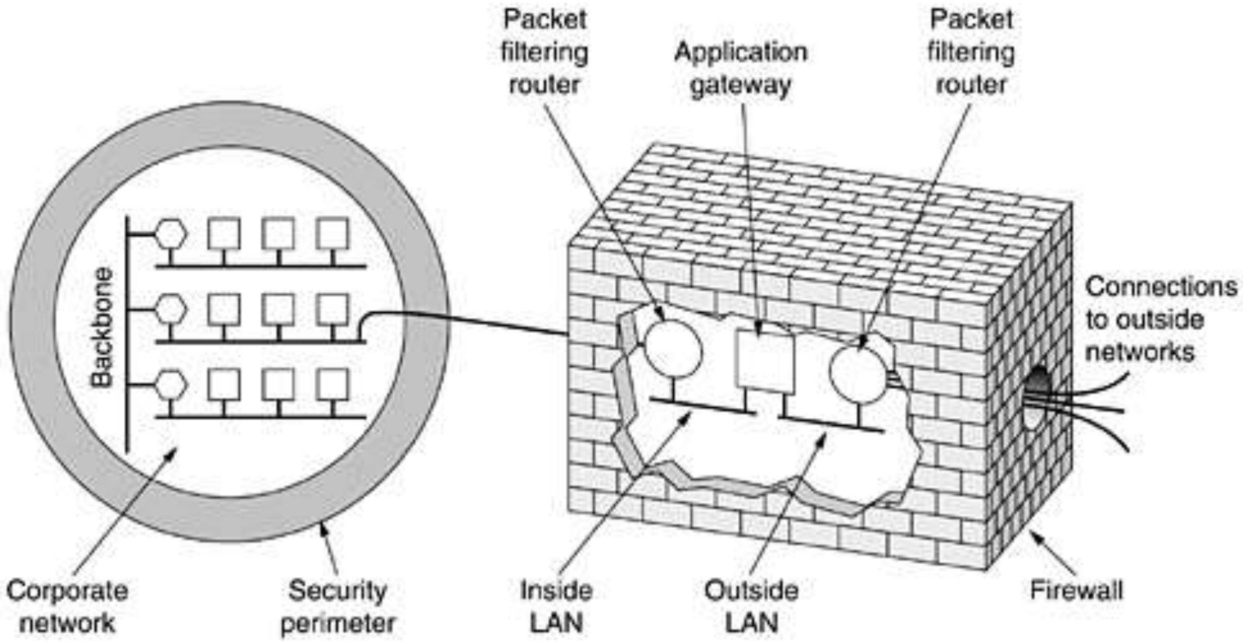
## 2. Application Level Gateway

- □ They are called Proxy Servers and acts as a relay of application level traffic.

## 3. Circuit Level Gateway

- □ It does not permit an end to end TCP Connection directly.
- □ The gateway setups two TCP Connections (IN and OUT).
- □ Once two connections are established => Gateway Relays

# Firewall : Types of Firewall



# Virtual Private Network (VPN)

- A VPN is one of the best tool for ensuring the network privacy. A VPN encrypts our connection and keeps us hidden while surfing, shopping and backing online.
- It is a service that helps us stay private online by establishing a secure, encrypted connection between our computer and the internet, providing a private tunnel for our data and communication s while we use public networks

# What does a VPN hide?

- VPN works on the operating system level, so they re-route all the traffic through other servers
- Instead of sending your internet traffic (e.g. your online searches, uploads and downloads) directly to your ISP, a PN first routes your traffic through a VPN server.
- That way, when your data is finally transmitted to the internet, it appears to come form the VPN server, not your personal device

# Types of VPN

- A remote access VPN
  - Allows users to connect to another network, be it the internet or their company's internal system, through a private encryption tunnel
- Site to site VPN or, (router to router VPN)
  - Mostly used within corporate environments specifically when an enterprise has headquarters in several different locations

# VPN : Virtual Private Networks

- Both Private and Hybrid Networks are Expensive.

- Solution to use global Internet for both Private and Public Communication => VPN

- VPN Creates a Network that is Private but Virtual.

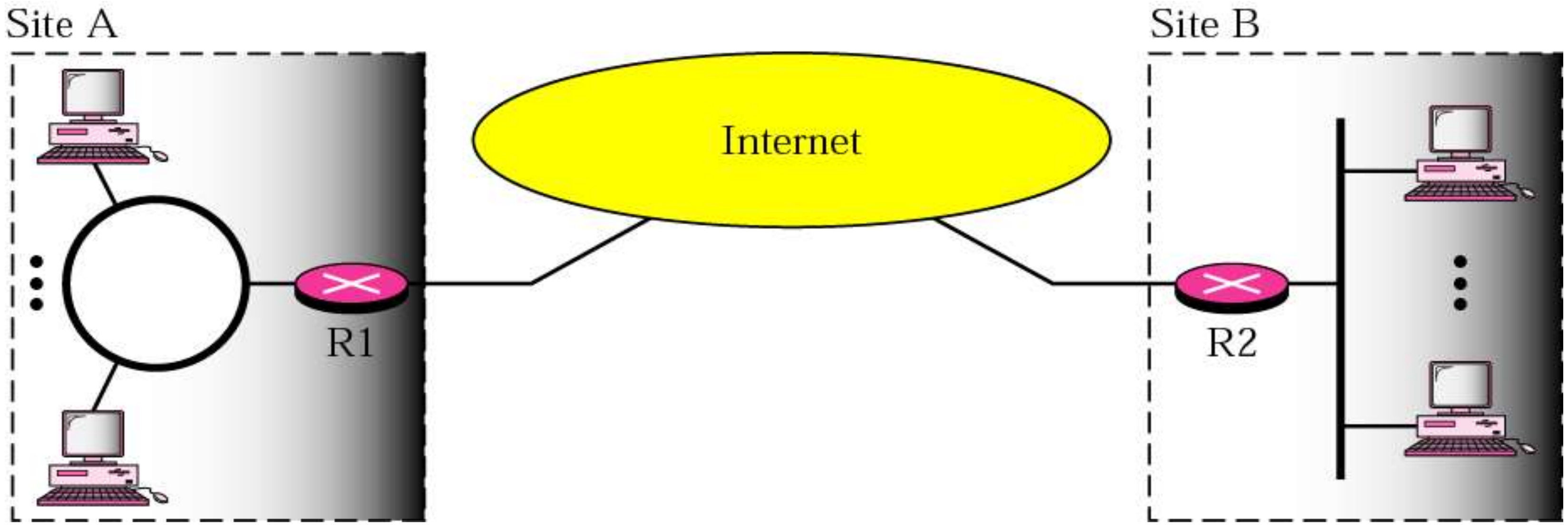
- It is Private because it guarantees Privacy inside the Organization.

- It is Virtual because it does not use Real Private WANs.

- The Network is Physically Public but Virtually Private.

- VPN Use IPSec in the Tunnel Mode to Provide Authentication, Integrity and Privacy.

# VPN : Virtual Private Networks



# Overview of Internet Protocol Security (IPsec)

- The Internet was not created with security in mind.
- Communications can be altered, examined and exploited.
- There is a growing need to protect private information crossing the public networks that make up the Internet infrastructure.
- IPSec is a set of protocols and methodologies to create secure IP connections.
- The IP security (IPsec) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authenticity, integrity and confidentiality.

# Overview of IP security

- It defines the encrypted, decrypted and authenticated packets.
- The protocols needed for secure key exchange and key management are defined in it.

**Uses of IP security:**

- To encrypt application larger data
- To provide security for routers sending routing data across the public internet
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two end points is encrypted, as with a virtual private network (VPN) connection
- The oldest VPN protocol which is till in use today tis PPTP (pint to point tunneling protocol)
- OpenVPN is amongst the most secure because any vulnerabilities in tis programming will quickly be notice and patched

# Next Generation Network (NGN)

- A next-generation network (NGN) is a network that uses new technologies to improve the performance, security, and scalability of existing networks. NGNs are designed to be flexible, secure, and easier to manage than traditional networks.

<u>Characteristics of NGNs:</u>

- **Packet-based**
  - NGNs use multiple broadband transport technologies that enable quality of service (QoS).
- **Heterogeneous**
  - NGNs can handle a wide range of devices, technologies, services, and verticals.
- **Secure**
  - NGNs use the latest advancements in cybersecurity to protect the network and services.
- **Scalable**
  - NGNs are designed to be scalable and meet the demands of modern businesses.
- **Converged**
  - NGNs are based on IP and converge fixed and mobile network infrastructures into a single network.

# Tutorial

1. What is cryptography? Show how Diffie-Hellman works with a suitable example
2. What is firewall? Explain types of firewall.
3. What do you mean by asymmetric cryptography? Explain RSA algorithm.
4. What do you mean by encryption and decryption? Explain DES function with suitable diagram.
5. What do you mean by network security? Explain Kerberos with suitable diagram.
6. Write short notes on
   a) VPN
   b) NGN
   c) Digital certificate
   d) Internet Protocol Security (IP Sec)