R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

22CS930 ENTERPRISE CYBER SECURITY

Department: CSE(CS)

Batch/Year: 2022-2026/IV

Created by: Dr. Udhaya Sankar S M

Date: 15.5.2025

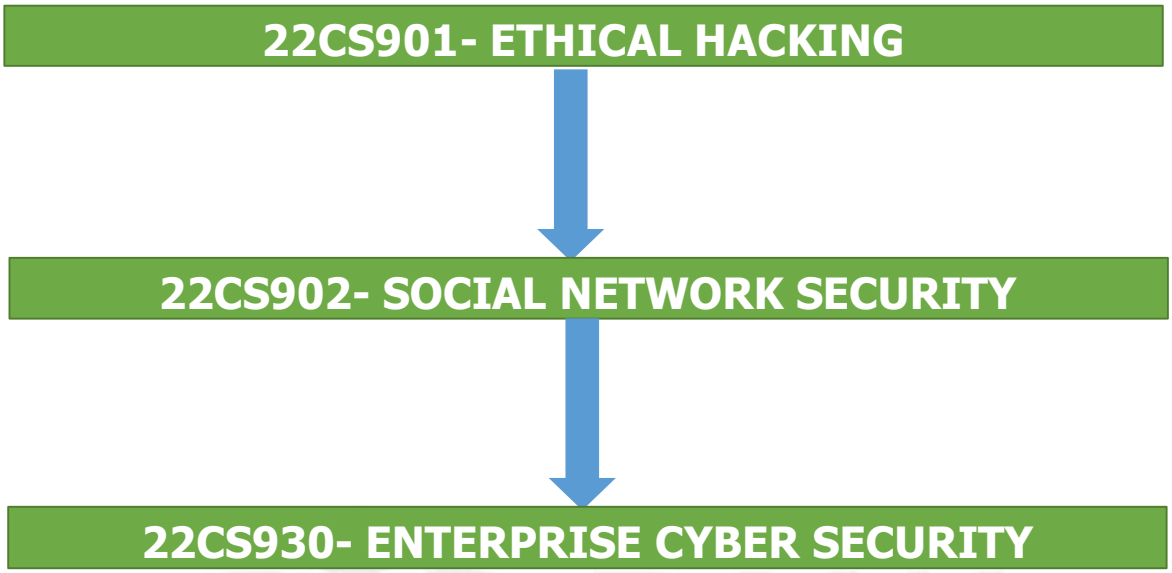
1.TABLE OF CONTENTS

2. COURSE OBJECTIVES

- Learn the fundamentals of cryptography.
- Learn the key management techniques and authentication approaches.
- Explore the network and transport layer security techniques.
- Understand the application layer security standards.
- Learn the real time security practices.

3. PRE REQUISITES

PRE-REQUISITE CHART



4.SYLLABUS

22CS930- ENTERPRISE CYBER SECURITY

L T P C
3 0 0 3

Unit-I INTRODUCTION TO CYBERSECURITY 9

Cyber Security – Need of Cybersecurity in Organizations – CIA Triad- Confidentiality, Integrity, Availability; Reason for Cyber Crime –Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes– A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

Unit II : NETWORK SECURITY BASICS

9

Network Security Concepts- Basics of Networks- Common Types of Network Attacks- Introduction to Firewalls- Types of Firewalls- IDS/IPS- Virtual Private Networks (VPN's)- Secure configuration and management of network devices. Case Study: Install Kali Linux on Virtual box.

Unit III : SECURE COMMUNICATION PROTOCOLS

9

Encryption Principles- Cryptography, Cryptanalysis, Feistel Cipher Structure. Block Encryption algorithms: DES, triple DES, and AES. Transport-Level Security: Secure Sockets Layer (SSL), Transport Layer Security TLS). Electronic Mail Security- Pretty Good Privacy (PGP), S/MIME. Securing wireless networks: WPA, WPA2, WPA3.

Unit IV : INTRUSION DETECTION AND PREVENTION SYSTEMS 9

IDPS- Need of Intrusion Detection Systems in Cyber Security- Types of IDPS: Network-based and Host-based. Configuring and Managing IDPS for threat detection using Honeypots. Case Study: Setup a honey pot and monitor the honey pot on network.

Unit V : WEB APPLICATION SECURITY 9

Introduction to Web Application Vulnerabilities – Cross Site Scripting (XSS) – SQL injection- Denial of Service (DoS)- Web Application Testing - Bypass of Penetration Tests- OWASP and OWASP Top.

5.COURSE OUTCOME

Course Code	Course Outcome Statement	Cognitive / Affective Level of the Course Outcome	Course Outcome
Course Outcome Statements in Cognitive Domain			
22CS930	Understanding the core concepts and importance of cybersecurity in organizational settings.	Understanding K2	CO1
22CS930	Acquire the knowledge common network attacks and deploy appropriate security measures.	Apply K3	CO2
22CS930	Implement encryption and secure communication protocols for data integrity and confidentiality.	Apply K3	CO3
22CS930	Deploy and manage Intrusion Detection and Prevention Systems for threat detection.	Analyse K4	CO4
22CS930	Identify and mitigate common web application vulnerabilities.	Analyse K4	CO5
22CS930	Conduct penetration tests to evaluate the security posture of web applications.	Evaluate K5	CO6

6.CO-PO/PSO MAPPING

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes.

Course Outcome COs	K-Levels	Program Outcomes(POs) , Program Specific Outcomes (PSO)												
		PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PSO2
22CS930.1	K2	3	2	-	-	-	-	-	-	-	2	-	-	3	-
22CS930.1	K3	3	3	2	-	-	-	-	-	-	2	-	1	3	2
22CS930.1	K3	3	3	3	2	2	-	-	-	-	2	-	2	3	3
22CS930.1	K4	3	3	3	2	2	-	-	-	-	2	-	2	3	3
22CS930.1	K4	3	3	3	-	-	-	-	-	-	2	-	2	3	3
22CS930.1	K5	3	3	3	2	2	-	-	-	-	2	-	2	3	3

UNIT III
NETWORK SECURITY BASICS

R.M.K GROUP OF INSTITUTIONS

7.LECTURE PLAN – UNIT III

UNIT III -SECURE COMMUNICATION MODELS

SNo	Topics	No. of Periods	Poposed Lecture period	Actual Lecture period	Pertaining COS	Taxonomy Level	Mode of Delivery
1	Encryption Principles-Cryptography , Cryptanalysis ,	1			CO1	K2	MD1, MD5
2	Feistel Cipher Structure	1			CO3	K3	MD1, MD5
3	Block Encryption algorithms: DES	1			CO3	K3	MD1, MD5
4	Triple DES, and AES.	1			CO3	K3	MD1, MD5
5	Transport-Level Security: Secure Sockets Layer (SSL)	1			CO3	K3	MD1, MD5
6	Transport Layer Security (TLS)	1			CO3	K3	MD1, MD5
7	Electronic Mail Security-Pretty Good Privacy (PGP)	1			CO3	K3	MD1, MD5
8	S/MIME	1			CO3	K3	MD1, MD5
9	Securing wireless networks: WPA, WPA2,	1			CO2	K3	MD1, MD5

7. LECTURE PLAN – UNIT III

ASSESSMENT COMPONENTS

- AC 1. Unit Test
- AC 2. Assignment
- AC 3. Course Seminar
- AC 4. Course Quiz
- AC 5. Case Study
- AC 6. Record Work
- AC 7. Lab / Mini Project
- AC 8. Lab Model Exam
- AC 9. Project Review

MODE OF DELEIVERY

MD 1. Oral presentation
MD 2. Tutorial
MD 3. Seminar
MD 4 Hands On
MD 5. Videos
MD 6. Field Visit

8 ACTIVITY BASED LEARNING : UNIT – III

ACTIVITY 1: Integrated Activity-Based Learning Plan

Objective:

Secure Communication Simulation Lab: From Encryption to Wireless Security

Activity Overview

- Students will be divided into teams. Each team will simulate a secure end-to-end communication system that includes:
- Encrypting messages using symmetric encryption (DES, 3DES, AES)
- Securely transmitting the message over a simulated network using TLS/SSL
- Sending secure emails using PGP or S/MIME
- Simulating secure wireless network transmission using WPA2/WPA3
- Attempting basic cryptanalysis on weakly encrypted messages
- Analyzing and documenting the role of the Feistel structure in block encryption

Activity Steps

Step	Description
1	**Design Phase**: Each team designs a communication flow that uses encryption and security layers.
2	**Encryption**: Students encrypt a sample message using AES or Triple DES.
3	**Transmission Simulation**: Set up a simple client-server using tools like OpenSSL to implement TLS.
4	**Email Security**: Send the encrypted message via email using PGP or S/MIME (with Thunderbird or GPG).
5	**Wireless Simulation**: Use Wireshark to observe packet encryption differences between WPA2 and WPA3.
6	**Cryptanalysis Challenge**: Teams exchange Caesar/Vigenère cipher messages and attempt decryption.
7	**Presentation & Report**: Each team presents their setup, encryption choices, and observations.

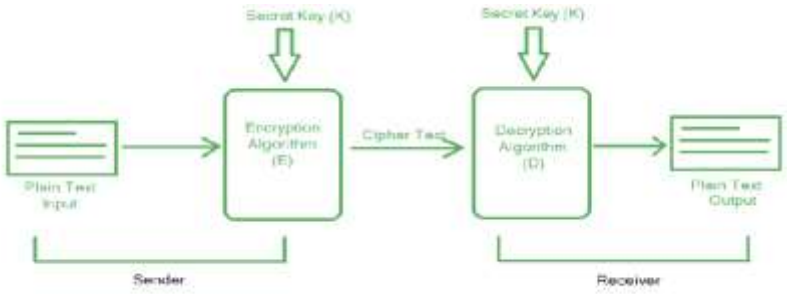
9 LECTURE NOTES : UNIT – III
Secure Communication Protocols

1. Encryption Principles:

Encryption is a fundamental technique in cryptography used to protect data by converting it into an unreadable format (ciphertext), which can only be decrypted back to readable form (plaintext) using a key.

Basic Terminology:

Plaintext: The original, readable data/message.
Ciphertext: The encrypted, unreadable version of the plaintext.
Encryption: The process of converting plaintext into ciphertext using an algorithm and a key.
Decryption: The process of converting ciphertext back to plaintext using a decryption key.
Key: A secret value used in encryption and decryption operaions.



Here's a breakdown of the key principles:
1. Confidentiality: This is the primary purpose of encryption, ensuring that only authorized individuals can access the information. It involves transforming the data into an unreadable format, making it unintelligible to anyone without the decryption key.
2. Integrity: Encryption helps ensure that the data hasn't been altered or tampered with during transmission or storage. By using cryptographic techniques like hash functions, any changes to the data can be detected.
3. Authentication: Encryption can verify the origin of the data, ensuring that it comes from the claimed sender. This can be achieved through digital signatures, which provide proof of the sender's identity.
4. Non-repudiation: Encryption can prevent the sender from denying that they sent the data. Digital signatures can also be used to provide evidence of the sender's action.

1.1 Cryptography:

Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. It involves using mathematical algorithms and keys to transform information into an unreadable format (encryption) and then back into its original readable form (decryption). This ensures confidentiality, integrity, and authentication of data, protecting it from unauthorized access and modification.

Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. It involves using mathematical algorithms and keys to transform information into an unreadable format (encryption) and then back into its original readable form (decryption). This ensures confidentiality, integrity, and authentication of data, protecting it from unauthorized access and modification.

How it works:

Cryptography relies on mathematical principles and algorithms to scramble data, making it incomprehensible to anyone without the correct key. For example, a sender might use an encryption algorithm and a secret key to encrypt a message. The encrypted message (ciphertext) is then sent to the recipient. The recipient uses the same algorithm and their corresponding secret key to decrypt the message and read the original information.

Examples of cryptography in use:

Secure websites (HTTPS):
Cryptography is used to encrypt communication between your browser and the website, protecting your sensitive information like passwords and credit card details.
Email encryption:
Cryptography can be used to encrypt emails so that only the intended recipient can read them.
Digital signatures:
Cryptography is used to create digital signatures, which verify the authenticity and integrity of digital documents.
Password protection:
Cryptography is used to store passwords securely, preventing them from being easily accessed if a system is compromised.

Types of Cryptography:

Symmetric-key cryptography: Uses the same key for both encryption and decryption.
Asymmetric-key cryptography: Uses a pair of keys: a public key for encryption and a private key for decryption.
Hashing: Creates a unique fingerprint of a piece of data, used for integrity checks and password storage.
Cryptography is a fundamental aspect of cybersecurity and plays a vital role in protecting sensitive information in various digital contexts.

Type	Description	Examples
Symmetric Key	Same key for encryption and decryption	AES, DES, 3DES
Asymmetric Key	Uses a key pair: public key for encryption, private for decryption	RSA, ECC
Hash Functions	One-way transformation, used for integrity checking	SHA-256, MD5

1.2 Cryptanalysis:

Cryptanalysis is the practice of breaking encrypted messages to reveal their hidden content, often without knowledge of the encryption key or the algorithm used. It involves analyzing cryptographic systems to identify vulnerabilities and weaknesses, ultimately aiming to decipher the original message

Cryptanalysis is essentially the art of "cracking" codes and ciphers. While cryptography focuses on creating secure encryption methods, cryptanalysis focuses on finding ways to bypass those methods.

Key Objectives:

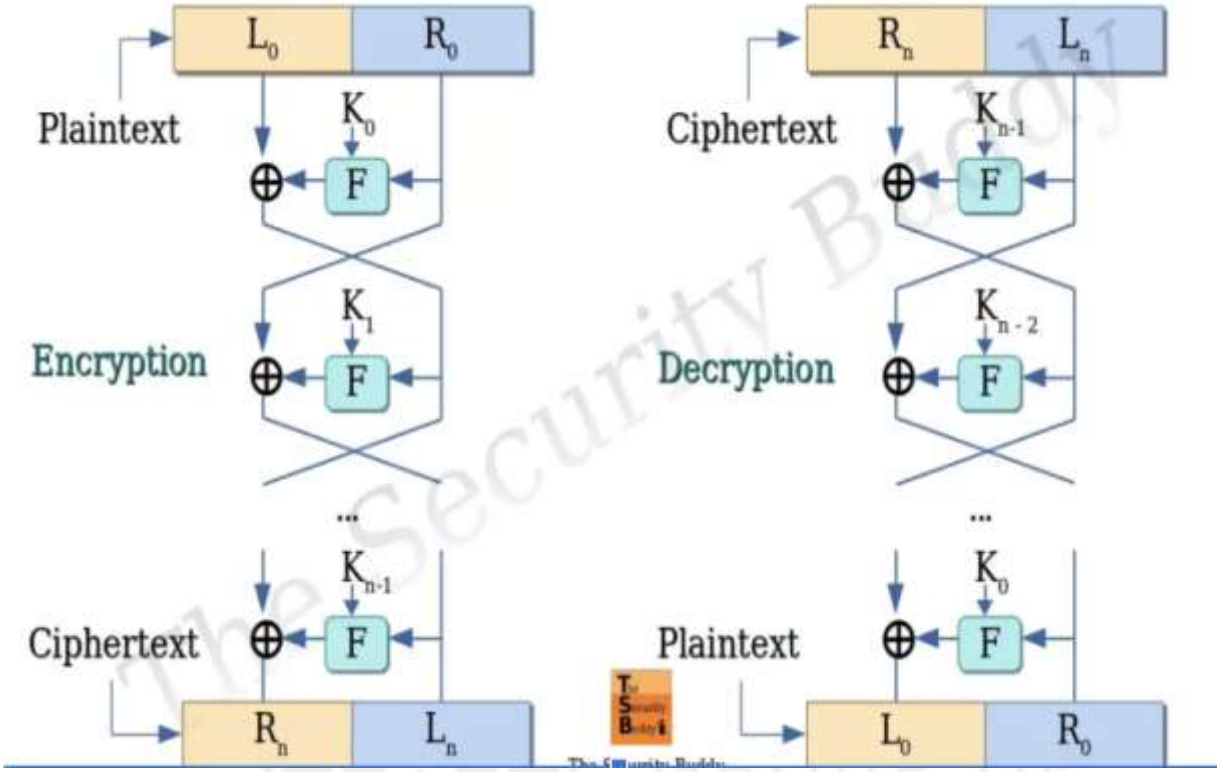
Breaking Encryption:
The primary goal is to decrypt ciphertext (encrypted text) without the decryption key.
Identifying Weaknesses:
Cryptanalysts examine cryptographic algorithms and systems to pinpoint vulnerabilities that can be exploited.
Improving Security:
By understanding how attacks work, cryptanalysts help developers create stronger, more secure encryption methods.

Methods Used:

Type of Attack	Description
Brute Force Attack	Trying all possible keys until the correct one is found.
Ciphertext-Only Attack (COA)	Attacker has access only to ciphertext and tries to deduce plaintext or key.
Known-Plaintext Attack (KPA)	Attacker knows some plaintext-ciphertext pairs and tries to find the key.
Chosen-Plaintext Attack (CPA)	Attacker can encrypt chosen plaintexts to gather information.
Chosen-Ciphertext Attack (CCA)	Attacker can decrypt chosen ciphertexts to gather information.
Side-Channel Attack	Exploits physical implementation (e.g., timing, power usage) of the algorithm.
Differential Cryptanalysis	Studies how differences in plaintext affect ciphertext to find the key.
Linear Cryptanalysis	Finds linear relationships between plaintext, ciphertext, and key bits.

1.3 Feistel cipher Structure

A Feistel cipher is a symmetric block cipher structure that uses the same algorithm for both encryption and decryption, but with a reversed key schedule. It divides the plaintext into two halves and processes them through multiple rounds, each involving a substitution and a permutation, to produce the ciphertext.



Here's a breakdown of the Feistel structure:

1. Block Division:
The plaintext is divided into two equal halves, typically denoted as the left (L) and right (R) halves.

2. Round Function:
Each round involves a round function that takes the right half (R) and a subkey derived from the main key as input.

3. Substitution and Permutation:
The round function's output is then XORed with the left half (L) to produce a new right half (R'). The original right half (R) becomes the new left half (L') for the next round.

4. Key Schedule:
A key schedule generates a series of subkeys, one for each round, from the main encryption key.

5. Encryption/Decryption:
The encryption and decryption processes are very similar. Decryption uses the same round function but applies the subkeys in reverse order.

6. Number of Rounds:
The number of rounds is a crucial design parameter. More rounds generally lead to greater security, but also affect performance.

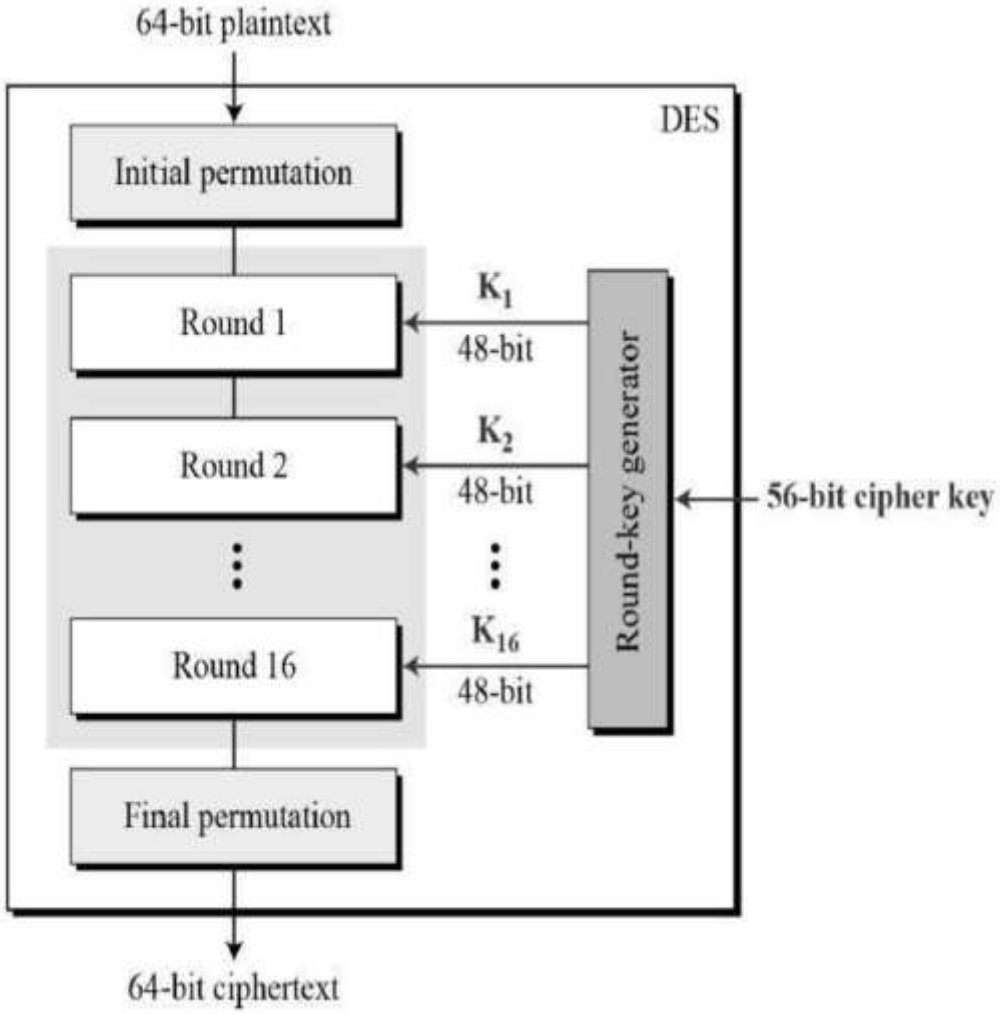
Key Features:

Iterative:
The Feistel structure is inherently iterative, with multiple rounds of processing.
Confusion and Diffusion:
The round function, with its substitution and permutation steps, aims to create confusion and diffusion, making the ciphertext difficult to decipher.
Flexibility:
Feistel ciphers can be adapted to different block sizes and key lengths.
Common Example:
The Data Encryption Standard (DES) is a well-known example of a Feistel cipher.

2. Block Encryption Algorithms

2.1 Data Encryption Standard (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 ch

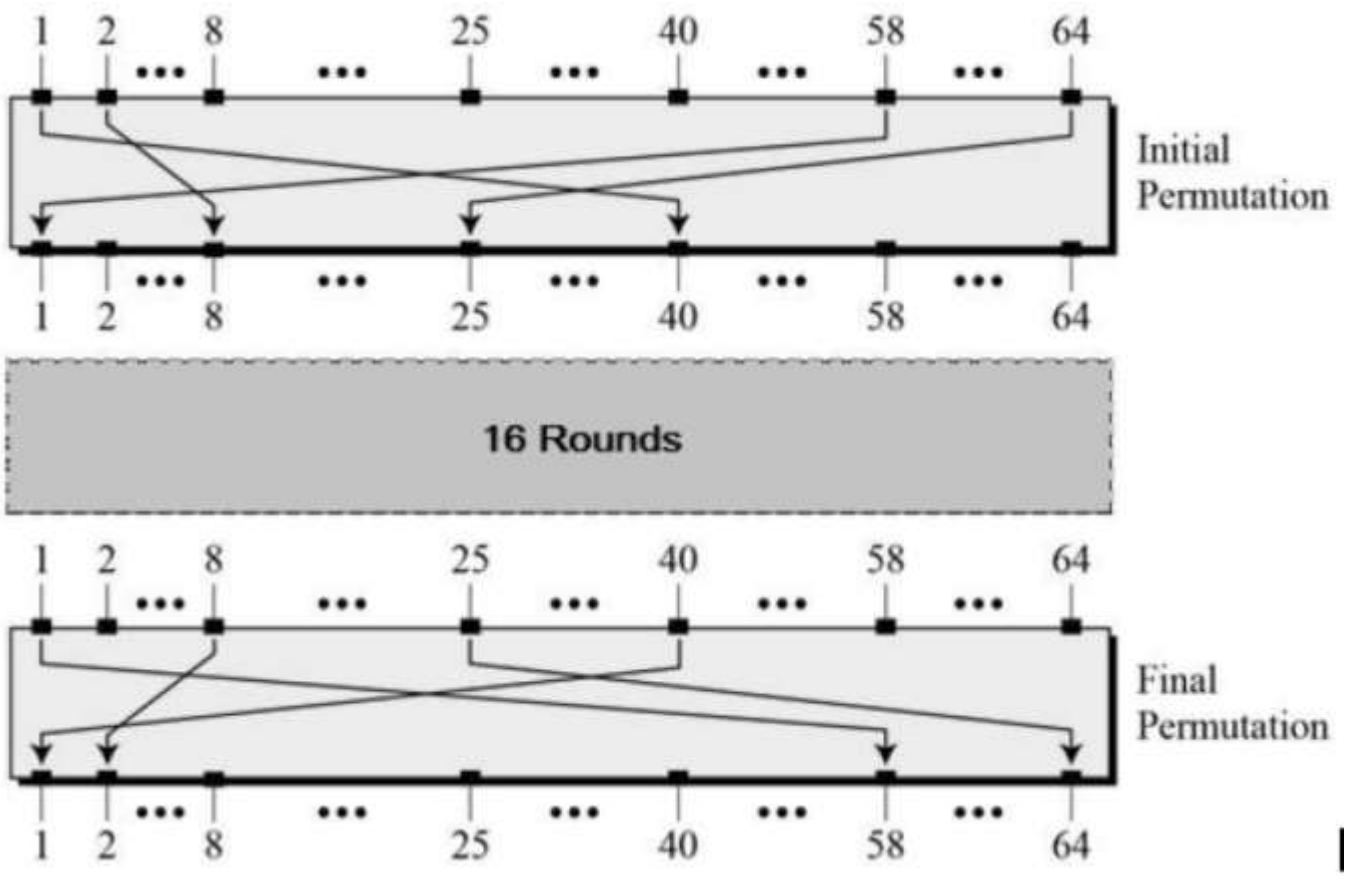


Since DES is based on the Feistel Cipher, all that is required to specify DES is –

Round function
Key schedule
Any additional processing – Initial and final permutation

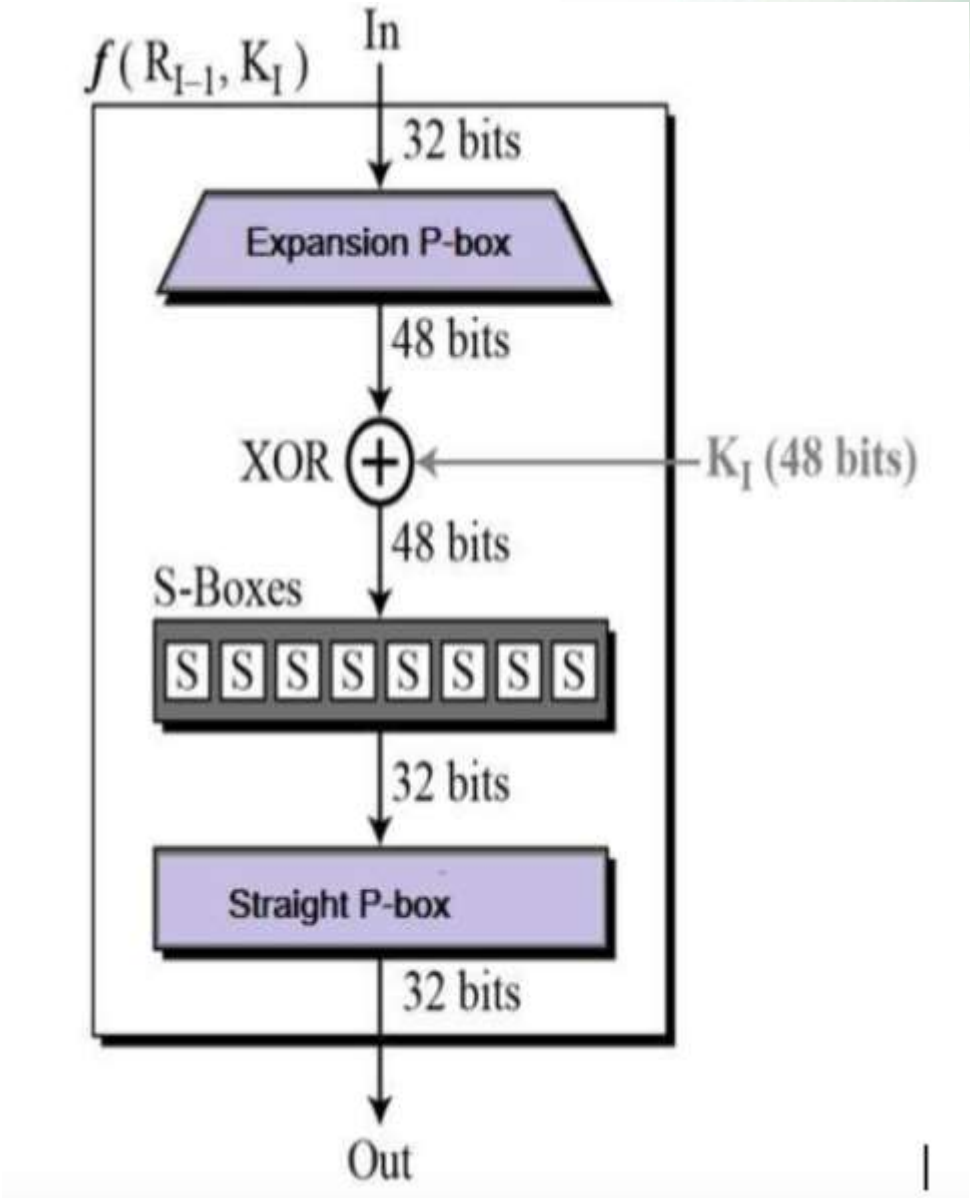
Initial and Final Permutation

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

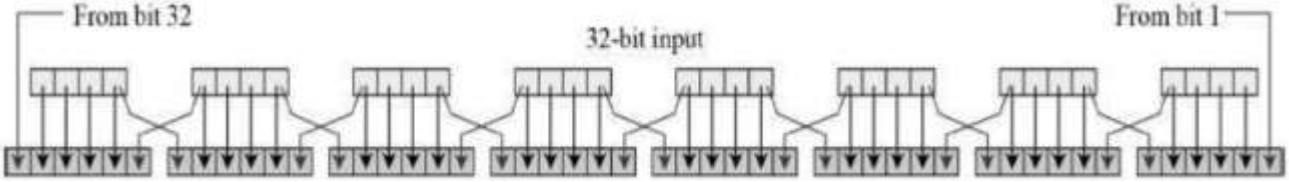


Round Function

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



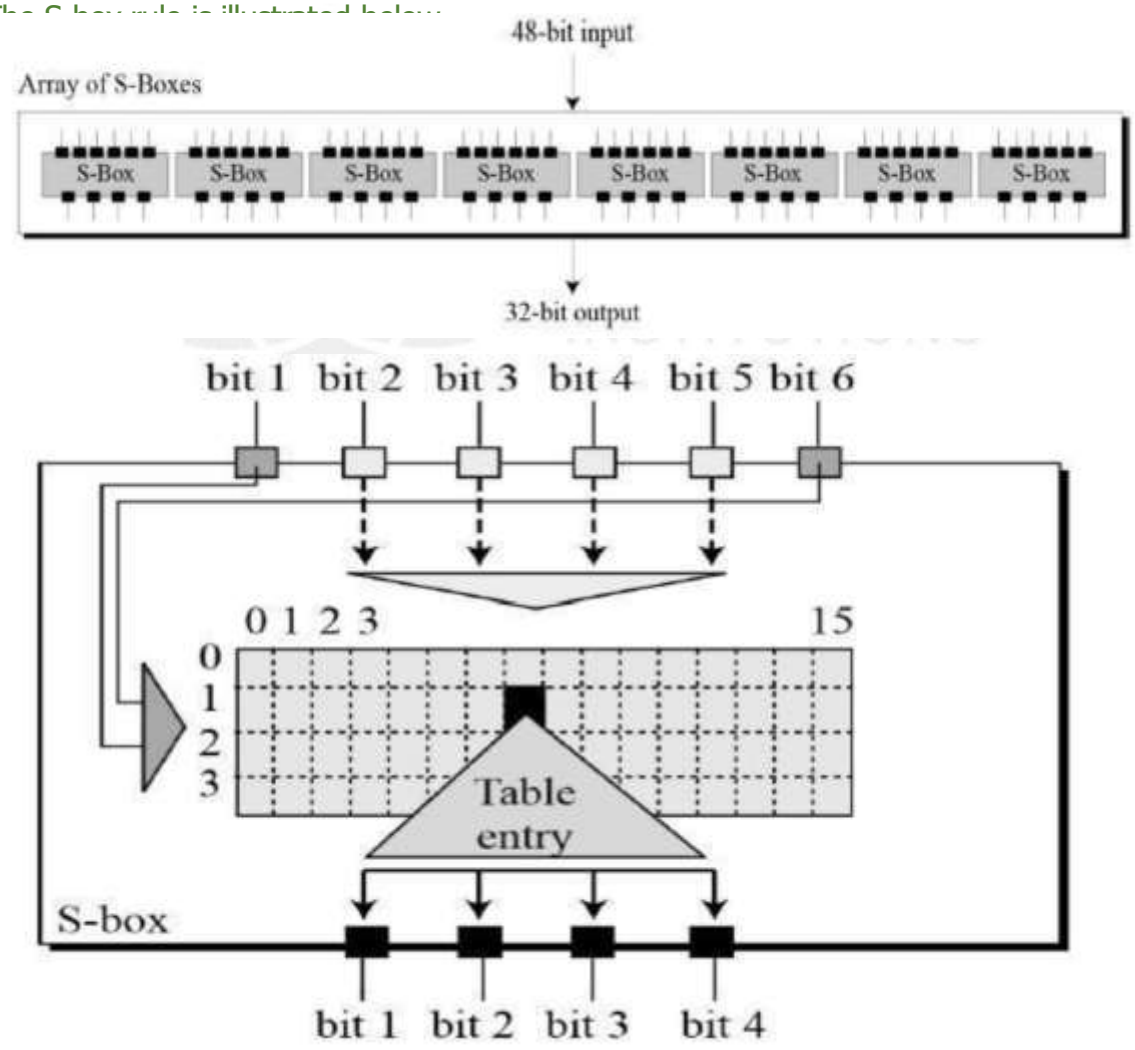
The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

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

The S-box rule is illustrated below



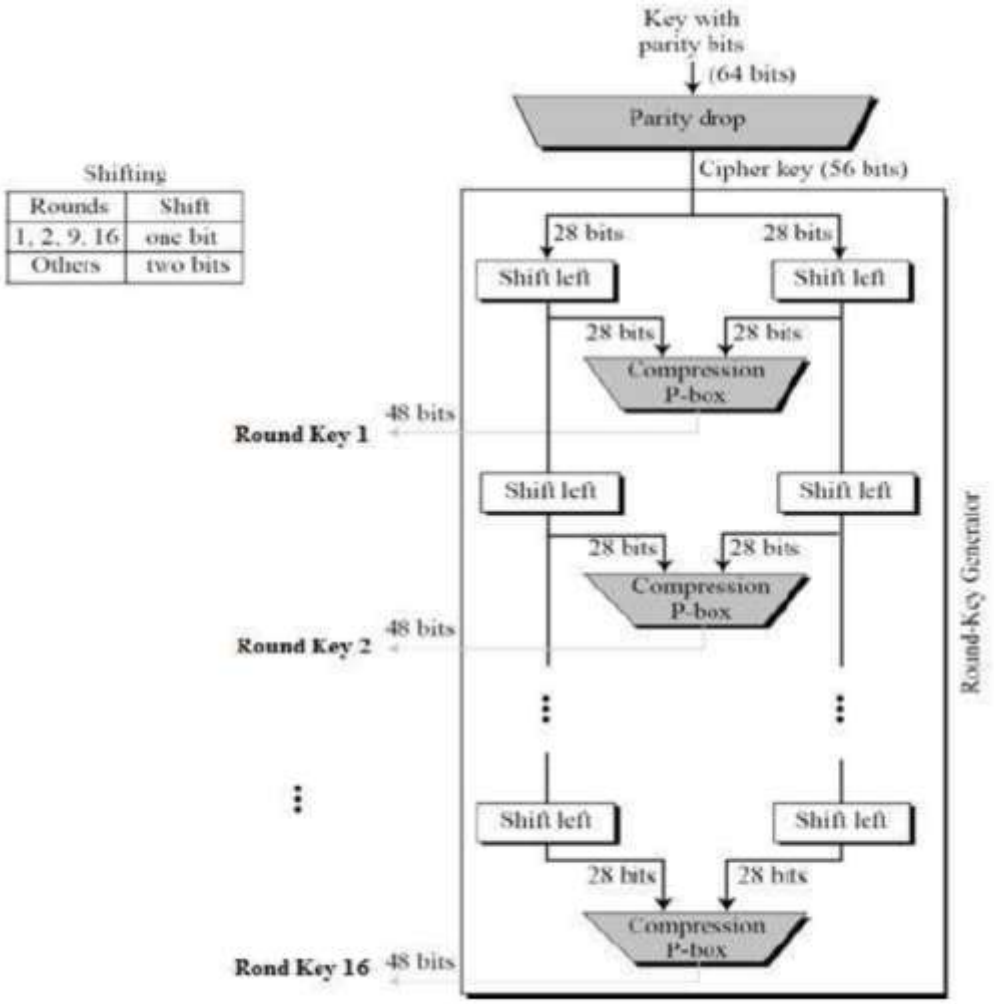
There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

Straight Permutation – The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

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



The logic for Parity drop, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

Avalanche effect – A small change in plaintext results in the very great change in the ciphertext.
Completeness – Each bit of ciphertext depends on many bits of plaintext.
During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

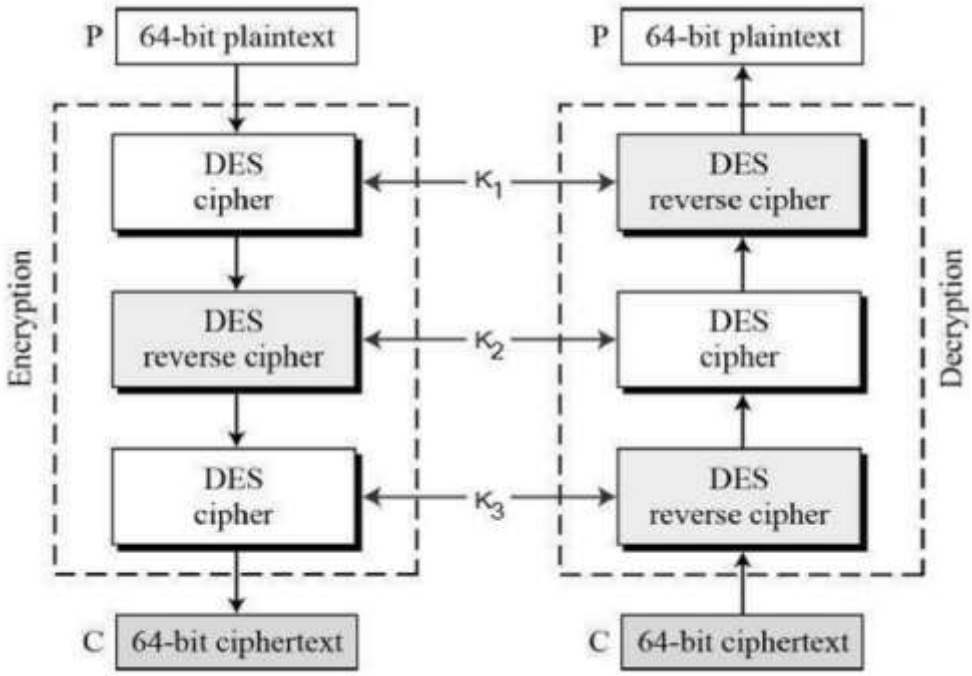
2.1 Triple DES

The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 356 = 168 bits. The encryption scheme is illustrated as follows



https://youtu.be/S918rR4VdqQ

The encryption-decryption process is as follows

- Encrypt the plaintext blocks using single DES with key K1.
- Now decrypt the output of step 1 using single DES with key K2.
- Finally, encrypt the output of step 2 using single DES with key K3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

Due to this design of Triple DES as an encryptdecryptencrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

2.3 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a highly trusted encryption algorithm used to secure data by converting it into an unreadable format without the proper key. It is developed by the National Institute of Standards and Technology (NIST) in 2001.

It is is widely used today as it is much stronger than DES and triple DES despite being harder to implement. AES encryption uses various key lengths (128, 192, or 256 bits) to provide strong protection against unauthorized access.

This data security measure is efficient and widely implemented in securing internet communication, protecting sensitive data, and encrypting files. AES, a cornerstone of modern cryptography, is recognized globally for its ability to keep information safe from cyber threats.

- AES is a Block Cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text. AES relies on the substitution-permutation network principle, which is performed using a series of linked operations that involve replacing and shuffling the input data.

Working of The Cipher

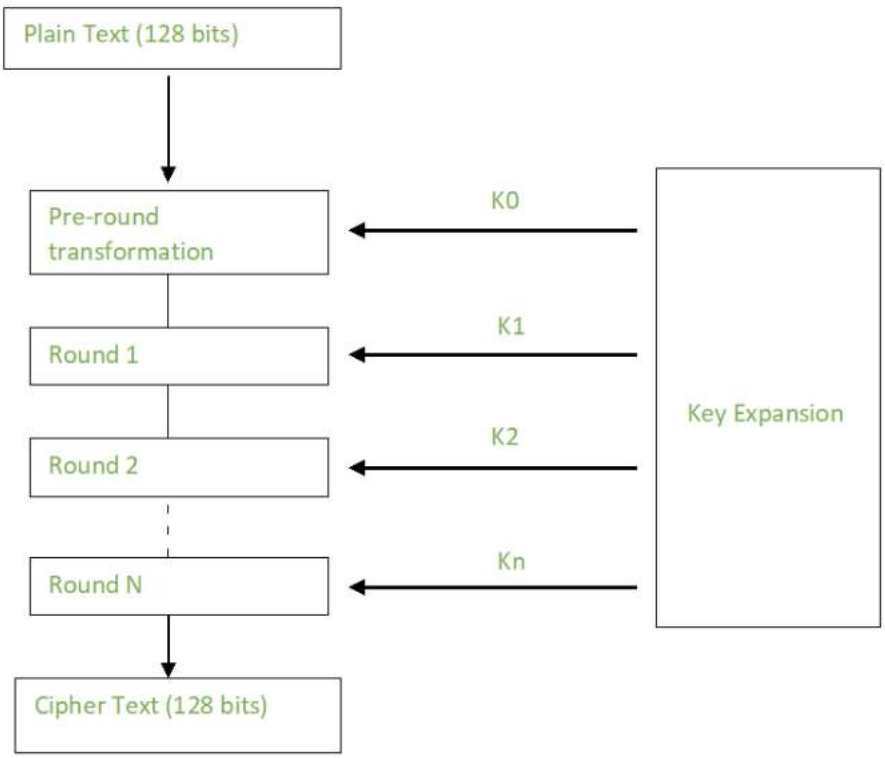
- AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

- The number of rounds depends on the key length as follows :

N (Number of Rounds)	Key Size (in bits)
10	128
12	192
14	256

Creation of Round Keys

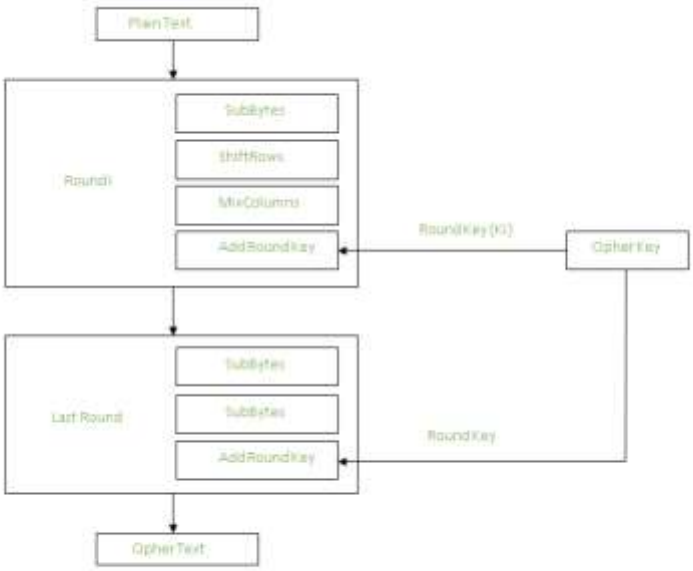
A Key Schedule algorithm calculates all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



Creation of Round Keys (AES)

Encryption
AES considers each block as a 16-byte (4 byte x 4 byte = 128) grid in a column-major arrangement.

[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]



Added Round Keys (AES)

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

Step1. Sub Bytes

This step implements the substitution.

In this step, each byte is substituted by another byte. It is performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16-byte (4 x 4) matrix like before.

The next two steps implement the permutation.

Step2. Shift Rows

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

```
[ b0  | b1  | b2  | b3  ]          [ b0  | b1  | b2  | b3  ]
| b4  | b5  | b6  | b7  |    ->    | b5  | b6  | b7  | b4  |
| b8  | b9  | b10 | b11 |          | b10 | b11 | b8  | b9  |
[ b12 | b13 | b14 | b15 ]          [ b15 | b12 | b13 | b14 ]
```

Step 3: Mix Columns

This step is a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.

```
[ c0 ]       [ 2  3  1  1 ] [ b0 ]
| c1 |  =     | 1  2  3  1 |    | b1 |
| c2 |      | 1  1  2  3 |     | b2 |
[ c3 ]     [ 3  1  1  2 ]     [ b3 ]
```

Step 4: Add Round Keys

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes are not considered as a grid but just as 128 bits of data.

After all these rounds 128 bits of encrypted data are given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round of decryption are as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse. The steps with notable differences.

Inverse MixColumns

This step is similar to the Mix Columns step in encryption but differs in the matrix used to carry out the operation.
Mix Columns Operation each column is mixed independent of the other.
Matrix multiplication is used. The output of this step is the matrix multiplication of the old values and a
constant matrix

[b0] = [14 11 13 9] [c0]
[b1]=[9 14 11 13] [c1]
[b2] =[13 9 14 11] [c2]
[b3]=[11 13 9 14] [c3]

Inverse SubBytes

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

Function Substitute performs a byte substitution on each byte of the input word. For this purpose, it uses an S-box.

Applications of AES

AES is widely used in many applications which require secure data storage and transmission. Some common use cases include:

- **Wireless security:** AES is used in securing wireless networks, such as Wi-Fi networks, to ensure data confidentiality and prevent unauthorized access.

- **Database Encryption:** AES can be applied to encrypt sensitive data stored in databases. This helps protect personal information, financial records, and other confidential data from unauthorized access in case of a data breach.

- **Secure communications:** AES is widely used in protocols such as internet communications, email, instant messaging, and voice/video calls. It ensures that the data remains confidential

- **Data storage:** AES is used to encrypt sensitive data stored on hard drives, USB drives, and other storage media, protecting it from unauthorized access in case of loss or theft.

- **Virtual Private Networks (VPNs):** AES is commonly used in VPN protocols to secure the communication between a user's device and a remote server. It ensures that data sent and received through the VPN remains private and cannot be deciphered by eavesdroppers.

- **Secure Storage of Passwords:** AES encryption is commonly employed to store passwords securely. Instead of storing plaintext passwords, the encrypted version is stored. This adds an extra layer of security and protects user credentials in case of unauthorized access to the storage.

- **File and Disk Encryption:** AES is used to encrypt files and folders on computers, external storage devices, and cloud storage. It protects sensitive data stored on devices or during data transfer to prevent unauthorized access.

3 Transport Layer Security (TLS)

Transport layer security protocol is one of the security protocols which are designed to facilitate privacy and data security for communications over the Internet. The main use of TLS is to encrypt the communication between web applications and servers, like web browsers loading a website.

TLS is used to encrypt other communications like email, messaging, and voice over IP (VoIP). TLS was proposed by the Internet Engineering Task Force (IETF), which is an international standards organization.

Components

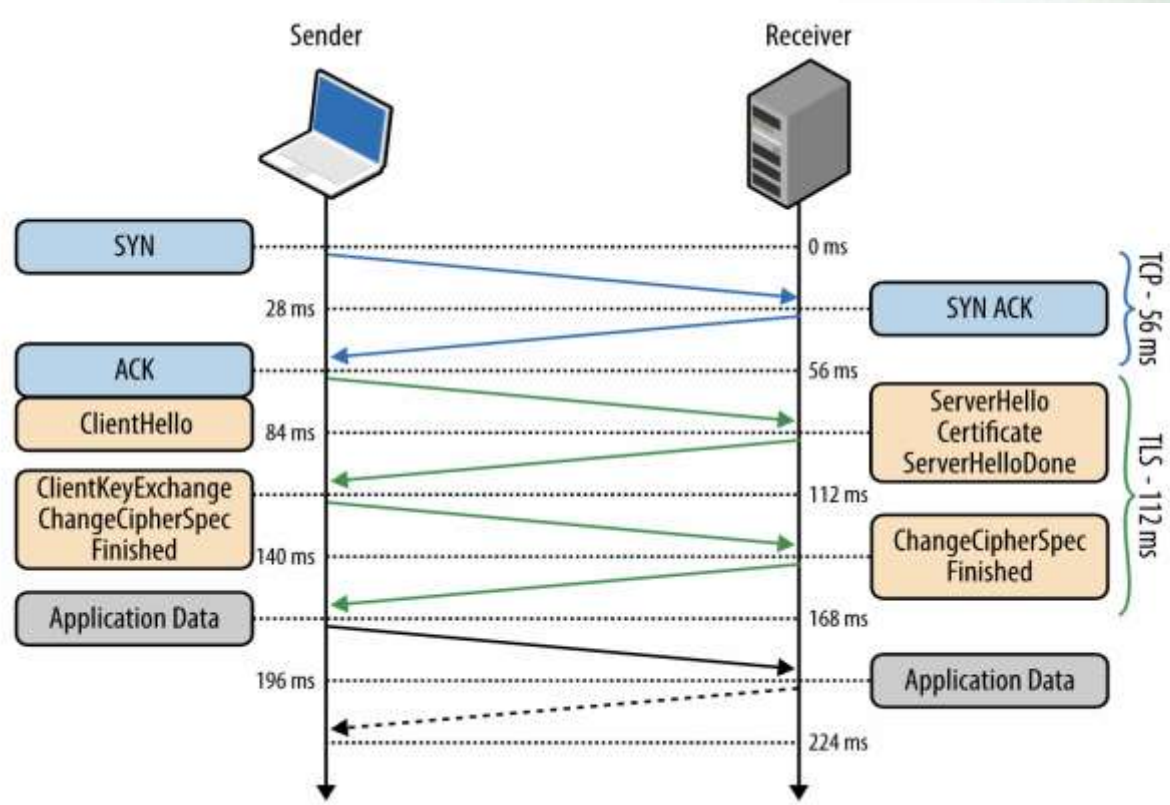
The three main components that TLS accomplishes are as follows

- **Encryption:** It is used to hide the data being transferred from third parties.

- **Authentication:** It always ensures that the parties exchanging information are who they claim to be.

- **Integrity:** verifies that the data has not been tampered with.

Given below is the pictorial representation of the Transport layer security protocol (TLS)



Advantages:

The advantages of TLS are as follows

- Encryption
- Interoperability
- Flexibility
- Easy of deployment
- Easy to use.

3.1 Secure Sockets Layer (SSL)

SSL or Secure Sockets Layer, is an Internet security protocol that encrypts data to keep it safe. It was created by Netscape in 1995 to ensure privacy, authentication, and data integrity in online communications. SSL is the older version of what we now call TLS (Transport Layer Security).

Websites using SSL/TLS have "HTTPS" in their URL instead of "HTTP."

Working of SSL

- **Encryption:** SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.

- **Authentication**: SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.

- **Data Integrity:** SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data received is exactly what was sent by the sender.

Importance of SSL

Originally, data on the web was transmitted in plaintext, making it easy for anyone who intercepted the message to read it. For example, if someone logged into their email account, their username and password would travel across the Internet unprotected. SSL was created to solve this problem and protect user privacy. By encrypting data between a user and a web server, SSL ensures that anyone who intercepts the data sees only a scrambled mess of characters. This keeps the user's login credentials safe, visible only to the email service.

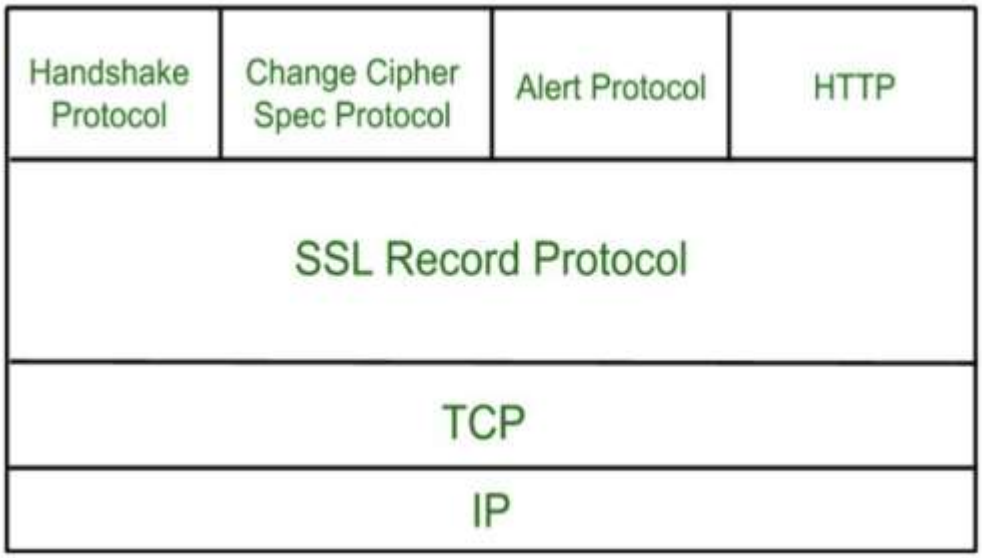
Additionally, SSL helps prevent cyber attacks by:

Authenticating Web Servers: Ensuring that users are connecting to the legitimate website, not a fake one set up by attackers.

Preventing Data Tampering: Acting like a tamper-proof seal, SSL ensures that the data sent and received hasn't been altered during transit.

Secure Socket Layer Protocols

1. SSL Record Protocol
2. Handshake Protocol
3. Change-Cipher Spec Protocol
4. Alert Protocol

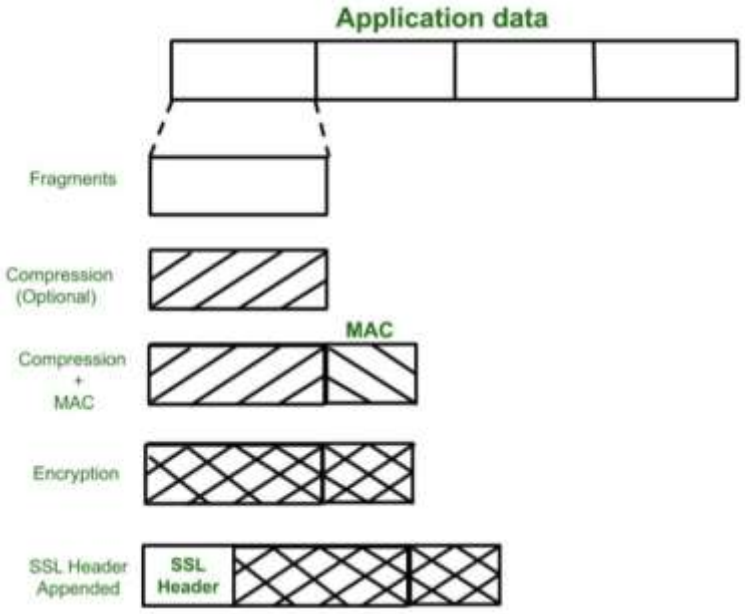


SSL Record Protocol

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



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 it 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 it certificate and Client-exchange-key.

Phase-4: In Phase-4 Change Cipher Spec occurs and after this the Handshake Protocol ends.

Change-Cipher Protocol

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state.

Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol

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

The level is further classified into two parts:

Warning (level = 1)
This Alert has no impact on the connection between sender and receiver. Some of them are:

- **Bad Certificate:** When the received certificate is corrupt.
- **No Certificate:** When an appropriate certificate is not available.
- **Certificate Expired:** When a certificate has expired.
- **Certificate Unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
- **Close Notify:** It notifies that the sender will no longer send any messages in the connection.
- **Unsupported Certificate:** The type of certificate received is not supported.
- **Certificate Revoked**: The certificate received is in revocation list.

Fatal Error (level = 2):

This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are :

- **Handshake Failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available.
- **Decompression Failure:** When the decompression function receives improper input.
- **Illegal Parameters:** When a field is out of range or inconsistent with other fields.
- **Bad Record MAC:** When an incorrect MAC was received.
- **Unexpected Message:** When an inappropriate message is received.
- The second byte in the Alert protocol describes the error.

Salient Features of Secure Socket Layer

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Versions of SSL

SSL 1 - Never released due to high insecurity
SSL 2 - Released in 1995
SSL 3 - Released in 1996
TLS 1.0 - Released in 1999
TLS 1.1 - Released in 2006
TLS 1.2 - Released in 2008
TLS 1.3 - Released in 2018

SSL Certificate:

SSL (Secure Sockets Layer) certificate is a digital certificate used to secure and verify the identity of a website or an online service. The certificate is issued by a trusted third-party called a Certificate Authority (CA), who verifies the identity of the website or service before issuing the certificate.

The SSL certificate has several important characteristics that make it a reliable solution for securing online transactions :

Encryption: The SSL certificate uses encryption algorithms to secure the communication between the website or service and its users. This ensures that the sensitive information, such as login credentials and credit card information, is protected from being intercepted and read by unauthorized parties.

Authentication: The SSL certificate verifies the identity of the website or service, ensuring that users are communicating with the intended party and not with an impostor. This provides assurance to users that their information is being transmitted to a trusted entity.

Integrity: The SSL certificate uses message authentication codes (MACs) to detect any tampering with the data during transmission. This ensures that the data being transmitted is not modified in any way, preserving its integrity.

Non-repudiation: SSL certificates provide non-repudiation of data, meaning that the recipient of the data cannot deny having received it. This is important in situations where the authenticity of the information needs to be established, such as in e-commerce transactions.
Public-key cryptography: SSL certificates use public-key cryptography for secure key exchange between the client and server. This allows the client and server to securely exchange encryption keys, ensuring that the encrypted information can only be decrypted by the intended recipient.

Session management: SSL certificates allow for the management of secure sessions, allowing for the resumption of secure sessions after interruption. This helps to reduce the overhead of establishing a new secure connection each time a user accesses a website or service.
Certificates issued by trusted CAs: SSL certificates are issued by trusted CAs, who are responsible for verifying the identity of the website or service before issuing the certificate. This provides a high level of trust and assurance to users that the website or service they are communicating with is authentic and trustworthy.

Certificates issued by trusted CAs: SSL certificates are issued by trusted CAs, who are responsible for verifying the identity of the website or service before issuing the certificate. This provides a high level of trust and assurance to users that the website or service they are communicating with is authentic and trustworthy.

Types of SSL Certificates:

There are different types of SSL certificates, each suited for different needs:

- **Single-Domain SSL Certificate:** This type covers only one specific domain. A domain is the name of a website, like www.geeksforgeeks.org. For instance, if you have a single-domain SSL certificate for www.geeksforgeeks.org, it won't cover any other domains or subdomains.

- **Wildcard SSL Certificate:** Similar to a single-domain certificate, but it also covers all subdomains of a single domain. For example, if you have a wildcard certificate for *.geeksforgeeks.org, it would cover www.geeksforgeeks.org, blog.www.geeksforgeeks.org, and any other subdomain under example.com.

- **Multi-Domain SSL Certificate:** This type can secure multiple unrelated domains within a single certificate.

These certificates vary in scope and flexibility, allowing website owners to choose the appropriate level of security coverage based on their needs.

SSL certificates have **different validation levels,** which determine how thoroughly a business or organization is vetted:

- **Domain Validation (DV):** This is the simplest and least expensive level. To get a DV certificate, a business just needs to prove it owns the domain (like www.geeksforgeeks.org).

- **Organization Validation (OV):** This involves a more hands-on verification process. The Certificate Authority (CA) directly contacts the organization to confirm its identity before issuing the certificate. OV certificates provide more assurance to users about the legitimacy of the organization.

- **Extended Validation (EV):** This is the most rigorous level of validation. It requires a comprehensive background check of the organization to ensure it's legitimate and trustworthy. EV certificates are recognized by the green address bar in web browsers, indicating the highest level of security and trustworthiness.

4 Electronic Mail Security:

Email security refers to the methods and processes used to safeguard email accounts, information, and communications from unauthorized access, data loss, and other hostile threats.

Significance of Email Security Practices

Hackers and cybercriminals use email as a means to disseminate malware, spam, and phishing assaults. It's also one of the common ways to get into a business network and steal sensitive data.

Approximately 92 percent of all malware is distributed via email. Every day, 15 billion spam emails are sent, accounting for around 45 percent of all emails. Furthermore, 96% of corporate email hack damages ranged from 250to 984,855.

Threats to Email Marketing

Spam – Spam is defined as unsolicited emails sent in large numbers. Vector spam can contain links that download malware files in some situations.

Phishing – Phishing is when hackers use false emails, adverts, links, or messages to steal personal information or gain access to internet accounts. Phishing is involved in 36% of breaches, according to Verizon.

Malware – Malware is when cybercriminals use harmful code distributed in email communications to infect one or more machines. Email virus infections will increase by 600 percent in 2020.

Spoofing – Spoofing is a spam and phishing assault tactic used by hackers. It is meant to deceive consumers into believing that the communication comes from someone or something they know or can trust.

Botnet Messages – A botnet is a network of computers that have been infected with malware. It commands the 'bot-header,' a single assaulting party. It's used to hack into devices, steal data, send spam, and get access to the device and its network.

BEC (Business Email Compromise) – The tracker uses this approach to acquire access to a business email account and impersonate the owner. The attacker usually targets organizations that use wire transfers to send money to overseas vendors.

How Can You Identify an Email as a Threat?

Dangerous emails have some common features. Look out for the following attributes to identify emails that have been sent with a malicious intent

Untrustworthy Email Address

Look for emails that utilize display name spoofing to hide the sender's true identity. These emails look like to have been sent by respectable organizations or trustworthy persons. Examine the sender's email address in the header for any small variations, such as extra characters or letters.

A Sense of Immediacy

In addition to verifying the email's header, you should also check the email's body. If you receive an unusual request that makes you feel compelled to act, it's likely that it includes malware. As a result, examine the email's wording for any feeling of urgency. Check for grammar and spelling issues, as most spam emails are poorly written.

Requests for Information Verification

Any email that requests you to verify, evaluate, check, or confirm any information is most likely a virus email. As a result, double-check the sender's email address before responding.

Email Security Best Practices
Following are some of the best practices in email security that work –

Email marketing should be encrypted. Customer-sensitive information is sometimes included in emails, making them susceptible. As a result, it's critical to protect these communications by encrypting all emails sent to and from your customers.

Email security software should be used. Additionally, employ high-quality email and security solutions that aren't easily manipulated or hacked. Invest in password management software, as well as anti-phishing and anti-spoofing software.

Use two-factor authentication. It's a common habit as well as an efficient security precaution. Before logging in, a user must submit two pieces of identifying information, making it far more difficult for hackers to get access to an account, even if they know the password.

Make sure the devices you use to log in are up to date. With the rise of remote work, many workers are encouraged to work from home and use personal devices to access company email accounts. Personal gadgets, on the other hand, are far more difficult for an organization to track, posing a serious security concern.

Only connect to secure Wi-Fi networks. If your firm doesn't utilize Wi-Fi or work from home, make sure you're always connected to the internet over a secure connection.

4.1 Pretty Good Privacy:

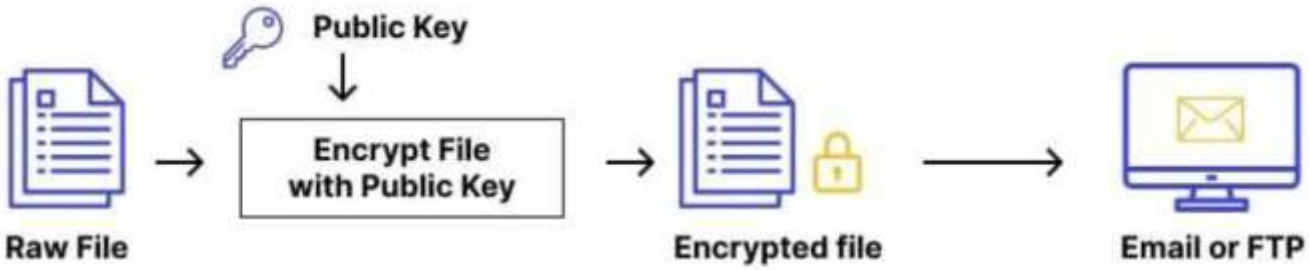
Pretty Good Privacy, or PGP, was a popular program used to encrypt and decrypt email over the Internet, authenticate messages with digital signatures and store encrypted files. PGP now commonly refers to any encryption program or application that implements the OpenPGP public key cryptography standard.

How does PGP encryption work?

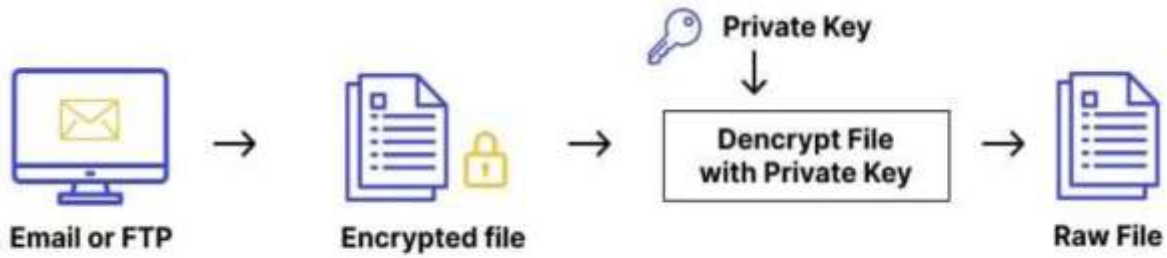
Pretty Good Privacy uses a variation of the public key system. In this system, each user has an encryption key that is publicly known and a secret, private key that is known only to that user. Users encrypt a message they send to someone else using that person's public PGP key. When the recipient receives the message, they decrypt it using their private key.

Encrypting an entire message using public key encryption can consume excessive resources. As a result, PGP uses a symmetric key encryption algorithm to encrypt the message and then uses the public key to encrypt that symmetric encryption key. Both the encrypted message and the encrypted symmetric encryption key are sent to the recipient, who first uses their private key to decrypt the short key and then uses that key to decrypt the message.

Encryption Process



Decryption Process



Email encryption is a wide usage of PGP. Primarily, users seeking exchange of sensitive information used it. With time, it became a mainstream solution for government organizations and agencies.

These entities are using this kind of encryption to protect sensitive information.

Send and receive encrypted emails

Defining the ID of encrypted messages

Encrypt files stored on your devices or in the cloud

The original PGP program was offered in two versions: one using the Rivest-Shamir-Adleman (RSA) algorithm for key exchange and one using the Diffie-Hellman algorithm for key exchange. PGP was required to pay RSA a license fee for the RSA version. That version used the International Data Encryption Algorithm to generate a short key for the entire message and RSA to encrypt the short key. The Diffie-Hellman version used the CAST algorithm for the short key to encrypt the message and the Diffie-Hellman algorithm to encrypt the short key.

When sending digital signatures, PGP uses an efficient algorithm that generates a hash (a mathematical summary) from the user's name and other signature information. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, the receiver is sure that the message has arrived securely from the stated sender. PGP's RSA version used the MD5 algorithm to generate the hash code. PGP's Diffie-Hellman version used the SHA-1 algorithm to generate the hash code; neither of those hashing algorithms is considered secure today.

More modern implementations use more secure algorithms like AES, AES-256 and 3DES.

What is PGP used for?

There are two main reasons for using PGP.

Encryption. PGP enables the encryption of sensitive information or data, whether it is a file, email or message. A PGP user can secure data through encryption in a format that is easily transmitted but that can only be decrypted with the recipient's secret key.

Authentication. PGP enables the digital signing of a message, file or email -- whether encrypted or not. The recipient uses the signer's public key to authenticate the digital signature.
More specifically, PGP software enables users to do all basic PGP transactions, including the following functions:

Creating a PGP public key pair.

Revoking a PGP public key pair so that others will no longer use it.
Key server functions, like specifying a default key server and registering key pairs.

1. Encrypt files and messages.
2. Decrypting a message or file.
3. Digitally signing a message or file.
4. Authenticating a digital signature.
5. Signing a public key.
6. Key management.

Different OpenPGP implementations have different -- but similar -- processes for each of these functions.

PGP is used mostly to encrypt or digitally sign emails, though it can also be used to do the following:

Encrypt and digitally sign transmissions in messaging applications. PGP has been implemented as an applet or an add-on to messaging applications. The basic GPG implementation operates at the command line, but numerous projects and some products act as a graphical user interface (GUI) front end for GPG.

Encrypt and digitally sign disk drives. Depending on the operating system (OS), PGP-based applications are available to encrypt disk volumes.

Scripts and application programming interfaces (APIs) for programming with PGP. Although it is less commonly used in modern settings, developers can still use scripts of cryptographic processes. Many of these common but complicated scripts are available online. Users can also develop their own scripts or use APIs to integrate PGP support into their customized applications.

PGP is used mostly to encrypt or digitally sign emails, though it can also be used to do the following:

Encrypt and digitally sign transmissions in messaging applications. PGP has been implemented as an applet or an add-on to messaging applications. The basic GPG implementation operates at the command line, but numerous projects and some products act as a graphical user interface (GUI) front end for GPG.

Encrypt and digitally sign disk drives. Depending on the operating system (OS), PGP-based applications are available to encrypt disk volumes.

Scripts and application programming interfaces (APIs) for programming with PGP. Although it is less commonly used in modern settings, developers can still use scripts of cryptographic processes. Many of these common but complicated scripts are available online. Users can also develop their own scripts or use APIs to integrate PGP support into their customized applications.

PGP concepts

PGP depends on some concepts that enable users to easily access and share public keys, and to transmit cryptographic information across networks and systems. Important terms include the following:

Alice and Bob. These are names assigned to generic actors in cryptographic processes. Alice, Bob and other generic actor names are often used when illustrating cryptographic exchanges, such as those used by PGP.

Web of trust. This is a concept used to describe how trust is established in public keys. A PGP user can try to establish trust directly with every key holder they interact with. In those cases where trust is established, they might also be willing to sign those keys to signify that they have authenticated the key pair and its holder.

The PGP user can also accept trust in key holders that certain other PGP users have already signed to indicate they are trustworthy. Suppose Alice accepts that Bob is sufficiently trustworthy in how carefully he vets the public keys he accepts as authenticated. In that case, Alice can also trust those other public keys that Bob trusts.

Implicit trust. One of the two types of trust that can be established through the web of trust, implicit trust is used when Alice signs Bob's public key pair. This indicates that Alice has vetted Bob -- and his private and public keys and his email address -- and is willing to assert (through her own signature) that she found Bob to be who he says he is and that the email and key pair are under Bob's control.

Explicit trust. The other type of trust established through the web of trust, explicit trust, occurs when Carlos -- a third generic user -- trusts Alice's judgment about others whose keys she has signed. Carlos can use explicit trust in Alice to accept that Bob's public key pair is also valid.

Key signing. This PGP function enables one person to announce that they have verified the person who claims to own the public key pair. PGP creator Zimmermann stresses verifying the following:

The key you are signing should be verified as controlled by the person who claims it.

The identity of the key holder should be verified with at least one form of photo ID. Even friends or coworkers should be formally identified if you have never previously seen that person's ID.

Email and private key ownership should be verified. The email address in the signed key should be verified as the correct one for the person claiming the key pair.

American Standard Code for Information Interchange (ASCII) armor, also known as Radix-64 encoding, is a way of formatting encrypted data in a printable format. PGP uses ASCII armor to format data in a way that resists the introduction of errors through different computer formats as the data transits the internet. ASCII armor uses only ASCII characters and header and footer blocks to identify the start and finish of the armored data.

The session key is a symmetric encryption key used for just one encryption session.

Benefits of PGP encryption

Although PGP has fallen in relevance, the encryption technology still does have some benefits:

PGP is hard to break. PGP's security depends on key strength and algorithms used. Adding to security, PGP uses both asymmetric and symmetric encryption, it has end-to-end encryption and modern implementations have stronger modern algorithms.

Versatility. PGP is flexible because it can encrypt data such as emails, files and other documents.

Offline security. PGP can be used to encrypt data in cold storage or data that is not connected to the internet.

Open source. Modern and free PGP implementations are still available.

PGP's challenges

PGP's success was primarily due to offering early users access to strong cryptography with little or no investment in software licenses. However, implementing and using PGP can be challenging for the following reasons:

Usability. PGP implementations tend to be challenging to use, whether at the command line or in a GUI.
Conceptual complexity. New users often have difficulty understanding key PGP concepts and processes. Users should know how it works so that they do not accidentally create security holes.
Decentralized infrastructure. Using a web of trust can pose a problem when there are not enough participants in the larger general population. Likewise, PGP does not anonymize users. Although the main data is encrypted, senders and recipients of emails sent through a PGP tool are still traceable.
Using older algorithms. Any PGP system using older algorithms will still be vulnerable. While most users do not use PGP, there is still enough of a user base to fuel the continued development of OpenPGP-compliant implementations and related applications.

4.2 Secure/ Multipurpose Internet Mail Extensions (S/MIME)

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and digital signing of MIME data (commonly email). It provides end-to-end security features for email communication

Key Features of S/MIME:

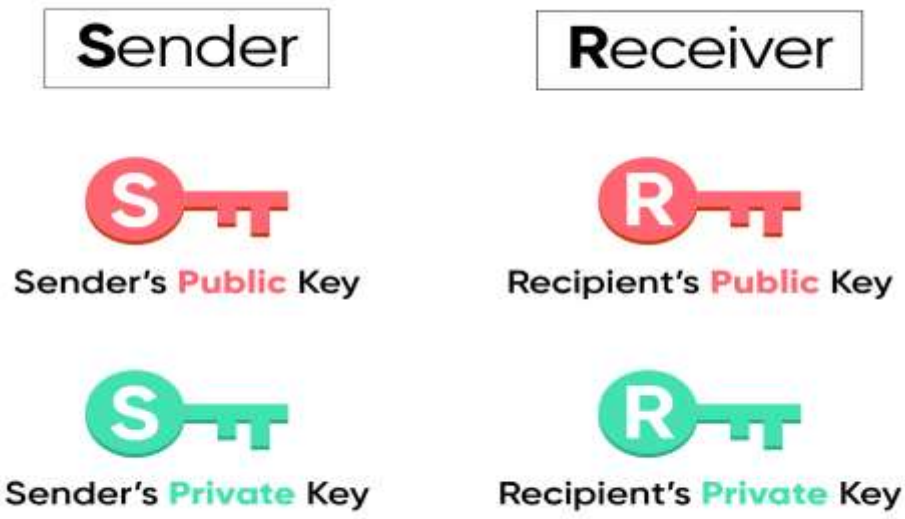
- **Authentication:** Ensures the email is from a verified sender using digital signatures.
- **Message Integrity:** Detects if the email has been altered during transit.
- **Confidentiality:** Encrypts the email contents so only the intended recipient can read them.
- **Non-repudiation:** The sender cannot deny sending the email, thanks to digital signatures.

S/MIME includes two security features:

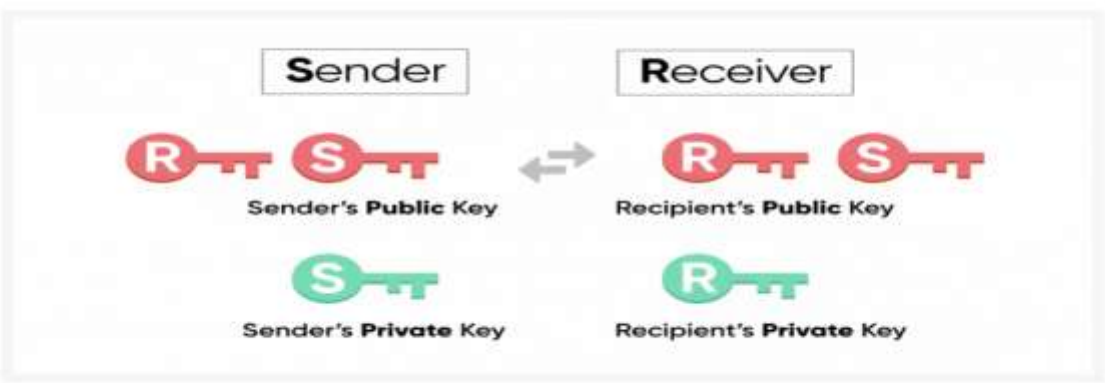
- **Email Encryption** - It encrypts the content of the email sent between two S/MIME enabled users to make it unreadable to anyone other than the intended recipient.
- **Digital Signature** - It digitally signs the emails sent between two S/MIME enabled users to eliminate any risk of spoofing.

Pre-requisites for S/MIME

You need to have a valid S/MIME certificate. This certificate would include a public key



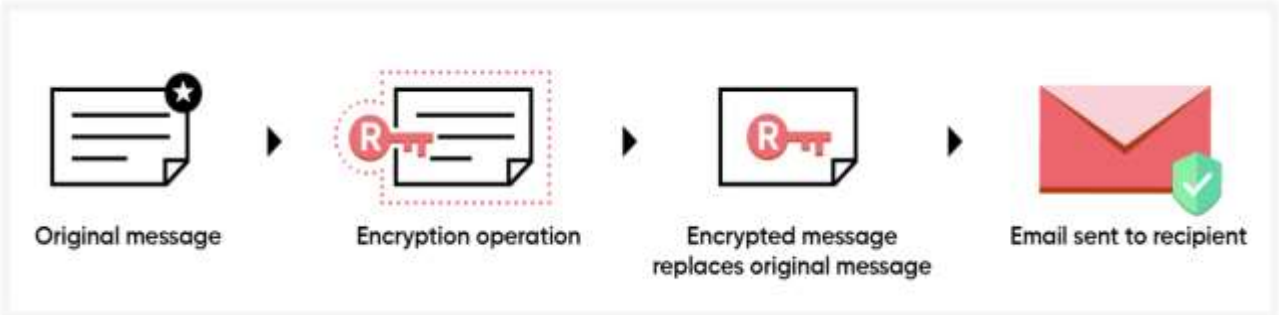
The sender and the receiver have to exchange their public key with each other. This process happens automatically when the sender and recipient exchange emails for the first time.



How does it work?

The process starts with the sender and receiver possessing each other's public key. The steps in Email encryption is as follows:

Encryption process



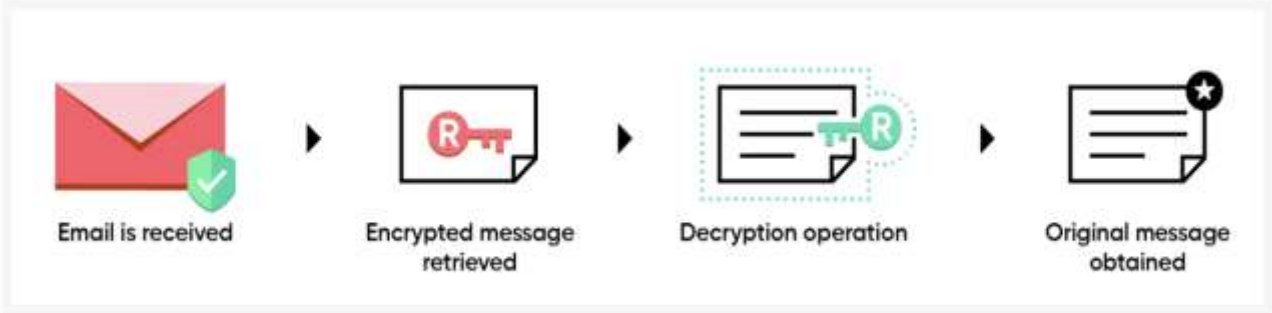
Once the sender clicks on Send, the original unencrypted message is captured.

The recipient's public key is used to encrypt the original message. At the end of the process, an encrypted version of the original message is produced.

The encryption message replaces the original message.

The email is sent to the recipient.

Decryption process

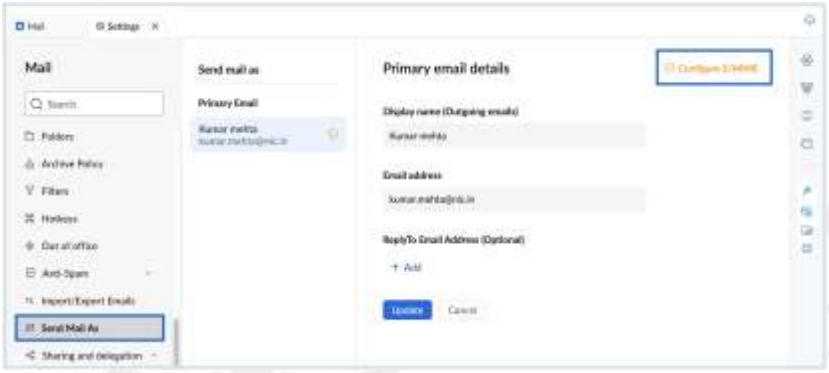


The recipient receives the email.
The encrypted message is retrieved.
The recipient's private key is used to decrypt the encrypted message.
The original message is obtained and displayed to the recipient.

Configuring S/MIME

You can configure S/MIME for your email address from the Send Mail As settings.
To begin configuring S/MIME, you are required to possess a valid certificate mapped to the email account issued by an authenticated certifier.

1.Login to https://mail.gov.in/.
2.Click the Settings icon.
3.Go to Send Mail As setting.
4.Choose the Configure S/MIME option next to the email address for which you want to configure S/MIME. The S/MIME encryption popup opens.



5.Click on the Add certificate button and select the certificate to upload the S/MIME certificate of the relevant email account.
6.Enter the certificate password and click Save to complete the uploading process.

Once uploaded, select the certificate. Click the OK button on the S/MIME certificate popup that appears to enable the certificate.

The emails that are further sent using the associated email address will be encrypted using the selected certificate. You will be able to disable the certificate if you click on the selected certificate and click OK in the pop up that appears.

Sending S/MIME encrypted emails

While composing an email, you are notified if the email you are about to send is S/MIME encrypted.

The icon displayed next to the recipient's name in the TO field indicates that the recipient has enabled S/MIME.

The icon next to the From address denotes that the email you send from this address will be digitally signed.

Receiving S/MIME encrypted emails

When you receive an email, the Encryption level indicator denotes the encryption status of the email. S/MIME encrypted emails are marked with S/MIME Encryption level indicator.

The icon next to the sender's name in the email preview indicates that the email has been digitally signed by the sender using S/MIME.

Feature	S/MIME	PGP
Trust Model	Based on Certificate Authority	Web of Trust
Integration	Built into many mail clients	Requires plugins
Key Management	Centralized	Decentralized

5. Securing Wireless Networks: WPA, WPA2, WPA3

Wireless networks are vulnerable to unauthorized access and eavesdropping. To protect data transmitted over Wi-Fi, security protocols like WPA, WPA2, and WPA3 were developed by the Wi-Fi Alliance.

5.1. WPA (Wi-Fi Protected Access)

Introduced: 2003 (as a temporary solution to replace WEP)

Technical Features:
Uses TKIP (Temporal Key Integrity Protocol) for encryption.
Per-packet key mixing: Creates a new encryption key for each data packet, making key reuse harder.
Message Integrity Check (MIC): Protects against data tampering.
Supports 802.1X authentication for enterprise use and Pre-Shared Key (PSK) for personal/home use.

Limitations:
TKIP is outdated and vulnerable to several attacks (e.g., replay attacks).
Not compliant with modern encryption standards like AES.
Slower due to legacy encryption and less efficient key handling.

Current Status:
Deprecated and not recommended for use today.
Most modern devices have dropped support for WPA.

2. WPA2 (Wi-Fi Protected Access 2)

Introduced: 2004 (mandatory for Wi-Fi certification by 2006)

Technical Features:

Encryption: Uses AES (Advanced Encryption Standard), providing stronger and faster encryption than TKIP.

Two modes:

WPA2-Personal (PSK): Requires a shared password for all users.
WPA2-Enterprise: Uses 802.1X with a RADIUS server for unique user credentials.
CCMP (Counter Mode CBC-MAC Protocol): Ensures data confidentiality and integrity.

Strengths:

Strong security when used with AES and a complex password.
Suitable for both home and enterprise networks.

Weaknesses:

Vulnerable to the KRACK (Key Reinstallation Attack), which exploits the 4-way handshake (patched in newer systems).

Shared passwords (in WPA2-PSK) can be guessed with offline dictionary attacks.

Current Status:

Still widely used, but being phased out in favor of WPA3. Regularly updated firmware and strong passwords can help mitigate known issues.

WPA3 (Wi-Fi Protected Access 3):

Introduced: 2018 (modern security standard)
Technical Features:
Replaces PSK with SAE (Simultaneous Authentication of Equals):
A more secure handshake protocol that prevents offline dictionary attacks.
Ensures each session has a unique encryption key.

Forward Secrecy:
Even if a password is compromised later, previous data remains secure.

Protected Management Frames (PMF):
Enhances protection against deauthentication and disassociation attacks.

Individualized data encryption in public networks:
Even in open Wi-Fi hotspots, user data is encrypted independently.

WPA3-Enterprise:

Offers 192-bit minimum encryption for sensitive environments like governments and finance.

Strengths:
Much more resistant to brute-force attacks.
Improved protection on public Wi-Fi (e.g., in cafes, airports).
Simplifies secure device setup with Wi-Fi Easy Connect™ (uses QR codes or NFC).

Limitations:
Not all devices support WPA3 yet.
May cause compatibility issues with older hardware.
Some routers offer WPA2/WPA3 mixed mode, which could lower security to WPA2 level.

Current Status:
Strongly recommended for new networks and devices.
Becoming the default in modern routers and IoT devices.

Comparison Table

Feature	WPA (2003)	WPA2 (2004)	WPA3 (2018)
Encryption Algorithm	TKIP	AES (via CCMP)	AES (CCMP) + SAE
Authentication Method	PSK / 802.1X	PSK / 802.1X	SAE / 802.1X
Offline Attack Resistance	Weak	Moderate	Strong (Prevents offline attacks)
Key Management	Basic	Robust (4-way handshake)	Enhanced (Simultaneous Authentication)
Public Network Protection	None	Minimal	Yes (Individual data encryption)
Deauthentication Protection	No	Partial	Full (via PMF)
Recommended Use	Not recommended	Acceptable (patched devices)	Recommended

10. ASSIGNMENT UNIT III

SET 1: Explain the principles of cryptography and cryptanalysis. Illustrate how the Feistel cipher structure is used in block encryption algorithms like DES.

SET 2: Compare and contrast DES, Triple DES, and AES in terms of architecture, key size, rounds, and security level. Which one is most suitable for modern applications and why?

SET 3: Discuss how SSL and TLS protocols ensure secure communication over the internet. Include the handshake process and real-time applications in daily life and industry.

SET 4: What are PGP and S/MIME? How do they secure electronic mail communication? Discuss their differences with appropriate examples.

SET 5: With respect to securing wireless networks, explain the evolution from WPA to WPA3. Highlight the key improvements in WPA3 and how it addresses the vulnerabilities of its predecessors.

11. PART A Q & A (WITH K LEVEL AND CO) UNIT 3

1. What are the main objectives of cryptography?K1,CO1

Confidentiality, Integrity, Authentication, and Non-repudiation: ensuring data privacy, correctness, sender/receiver verification, and denial prevention.

2. Define cryptanalysis?K1,CO1

Cryptanalysis is the process of analyzing encrypted data to uncover the original plaintext without knowing the secret key. It exposes algorithm vulnerabilities

3.What is the structure of a Feistel cipher?

Feistel cipher divides plaintext into two halves and processes them using multiple rounds with XOR and permutation functions, allowing reversible encryption.

4.Compare DES and AES. K3,CO2

DES has a small 56-bit key making it vulnerable to brute-force attacks and is outdated for modern security standards.

5.State any two drawbacks of DES. K2, CO2

The OSI model is a 7-layer framework that standardizes communication functions, helping troubleshoot, design, and implement interoperable network systems and protocols.

6.What is Triple DES and why was it introduced? K2, CO2

A DoS attack overwhelms a system or network with traffic or requests, making it unavailable to legitimate users, often disrupting services significantly.

7. What is the function of SSL in secure communication? K2, CO3

SSL secures communication over networks by encrypting data, ensuring confidentiality, integrity, and authentication. It has been replaced by TLS.

8. Differentiate between SSL and TLS? K3,CO3

SSL is an older protocol, now deprecated. TLS is its successor, offering stronger encryption, better performance, and security.

9.What are the security services provided by S/MIME ? K4,CO2

S/MIME ensures confidentiality, integrity, authentication, and non-repudiation for email by using encryption and digital signatures.

10.How does PGP ensure secure email transmission? K3,CO4

PGP uses a symmetric key to encrypt messages and encrypts that key with the recipient's public key. It adds a digital signature for authenticity.

11.Define WPA and its role in wireless security?K1, CO5

WPA3 includes Simultaneous Authentication of Equals (SAE) for secure key exchange and 192-bit encryption for better security.

12.List two enhancements introduced in WPA3 ? K2,CO5

A firewall filters network traffic, while antivirus software detects and removes malware. Both are crucial but operate on different aspects of cybersecurity.

13.Explain the avalanche effect in block ciphers.? K1,CO2

A small change in input (one bit) leads to a significant and unpredictable change in the ciphertext, enhancing security.

14.What is the key length of AES-256?K1,CO2

AES-256 uses a 256-bit key, providing high security and resistance to brute-force attacks.

15.Define symmetric and asymmetric encryption with examples.K2,CO1

Symmetric uses one key (e.g., AES), while asymmetric uses public-private key pairs (e.g., RSA) for encryption and decryption.

16. What is the purpose of Initialization Vector (IV) in encryption?K2,CO2

IV ensures that identical plaintexts produce different ciphertexts by introducing randomness, enhancing security.

17.Mention two key exchange algorithms used in SSL/TLS.?K2,CO3

RSA and Diffie-Hellman are commonly used to securely share encryption keys over insecure networks.

18.How does TLS provide data integrity?K2,CO3

TLS uses HMAC (Hash-based Message Authentication Code) to ensure the data hasn't been modified in transit.

18. What are the types of IDS? K4,CO1

IDS can be classified as Host-based (HIDS) or Network-based (NIDS). HIDS monitors activities on a single host, while NIDS scans network traffic for threats.

19.What is a digital certificate and who issues it?K2,C03?

A digital certificate is issued by a Certificate Authority (CA) and verifies the identity of the entity holding a public key.

20.What is MIME and how is it extended by S/MIME? K3,CO4

MIME supports multimedia content in email. S/MIME adds encryption and digital signatures to provide secure communication.

21. Why is AES preferred over DES in modern systems?K2,CO2

AES is faster, supports larger key sizes (128-256 bits), and provides stronger encryption than DES.

22.State the role of digital signatures in email security ? K2,C04

Digital signatures ensure message integrity and verify sender identity, preventing tampering and impersonation.

23. Differentiate between WPA2-Personal and WPA2-Enterprise?K3,CO5

Best practices include disabling unused ports, changing default credentials, applying firmware updates, logging activities, and using secure management protocols like SSH.

24.What is SAE in WPA3 and its advantage? K2,CO5

SAE (Simultaneous Authentication of Equals) is a secure password-authentication protocol in WPA3, resistant to offline attacks.

12. PART B Q s (WITH K LEVEL AND CO) UNIT III

1. Explain the principles of cryptography and cryptanalysis with suitable examples?(13) **K2,CO1**
2. Describe the Feistel cipher structure. How is it used in DES? Illustrate with an example?(13) **K4,CO2**
3. Compare DES, Triple DES, and AES in terms of architecture, key size, number of rounds, and security.(13) **K4,CO2**
4. Explain the architecture and protocol flow of Secure Sockets Layer (SSL) with a diagram.? (13) **K2,CO3**
5. Compare and contrast SSL and TLS. Highlight the protocol improvements in TLS?(13) **K4,CO3**
6. Describe the working of Pretty Good Privacy (PGP) for securing email communication?(13) **K2,CO4**
7. Explain S/MIME architecture and how it provides security services for email communication?(13)**K3,CO**
8. Explain the evolution of wireless security standards: WPA, WPA2, and WPA3. Highlight the improvements(13)?**K5,CO5**
9. Compare WPA, WPA2, and WPA3 in terms of encryption, authentication, and security features(13)?**K4,CO5**

13. Supportive online Certification courses

1. **UDEMY: SSL/TLS Fundamentals**

   https://www.udemy.com/course/ssl-tls-intro/

2. **COURSERA: Cryptography I**

   https://www.coursera.org/learn/crypto

3. **NPTEL : Cybersecurity and Privacy**

   https://onlinecourses.nptel.ac.in/noc25_cs116/preview

14. Real time applications in day to day life and to Industry

Real-Time Application in Day-to-Day Life

Question:

How do common users experience the principles of encryption, secure communication protocols, and wireless security in their everyday digital activities such as messaging, online shopping, banking, and using Wi-Fi at home?

Expected Answer (Key Points):

Encryption Principles: Messaging apps like WhatsApp use end-to-end encryption (AES-based).

Cryptanalysis awareness: Secure password practices avoid easy-to-crack passwords.

Feistel Cipher: Not visible, but used internally in legacy encryption methods in older banking systems.

Block Encryption (AES/DES): Used when compressing files with passwords (7-Zip with AES), mobile data encryption.

SSL/TLS: Accessing any HTTPS website (e.g., online shopping, banking).

PGP/S-MIME: Not common but used in secure email clients like ProtonMail or Thunderbird with PGP.

WPA/WPA2/WPA3: Home Wi-Fi routers use WPA2/WPA3 to protect network from neighbors/hackers.

Real-Time Application in Industry

Question:

How are encryption algorithms, secure communication protocols, and wireless network security standards applied in modern industry to protect sensitive data and maintain regulatory compliance?

Expected Answer (Key Points):

Encryption Principles: Used to encrypt databases, logs, and data at rest (e.g., BitLocker, AES-256).

Cryptanalysis: Used by cybersecurity teams during penetration testing to assess vulnerabilities.

Feistel Cipher: Used in older industrial control systems relying on DES-based protocols.

Block Encryption (AES, 3DES): Protects data during storage and secure file transmission in sectors like finance and healthcare.

SSL/TLS: Ensures secure data exchange between client and server (HTTPS, APIs, remote access).

PGP/S-MIME: Used in legal, government, and corporate sectors for encrypted and signed email communication.

WPA2/WPA3: Enterprise networks use WPA3-Enterprise with RADIUS for secure and authenticated access.

15. ASSESSMENT SCHEDULE

Tentative schedule for the Assessment During 2024-2025 ODD semester

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	Unit Test 1			UNIT 1
2	IAT 1			UNIT 1 & 2
3	Unit Test 2			UNIT 3
4	IAT 2			UNIT 3 & 4
5	Revision 1			UNIT 5 , 1 & 2
6	Revision 2			UNIT 3 & 4
7	Model			ALL 5 UNITS

16. PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXT BOOKS:

1. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021.
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, 2018.

REFERENCES:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Ravi Das and Greg Johnson, "Testing and Securing Web Applications", 2021.
3. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly Media, Inc, 2020.

17 MINI PROJECTS SUGGESTIONS

TLS-Based Secure Chat Application

Secure File Transfer with AES and TLS

SSL/TLS Certificate Validation Browser Extension

S/MIME-Based Email Integrity Checker

Cryptanalysis Tool for Classical and Block Ciphers

IoT Communication Security Using TLS and AES

18. GATE QUESTIONS

1.Q1: DES uses a Feistel network structure. How many rounds does DES perform?
A. 8
B. 16
C. 32
D. 64
Answer: B. 16
Explanation: DES uses a 16-round Feistel structure

2. Which of the following statements is false?
A. DES block size is 64 bits
B. AES supports 128/192/256-bit keys
C. 3DES applies DES encryption three times
D. AES is slower than 3DES
Answer: D
Explanation: AES is significantly faster than 3DES

3.During a TLS handshake, which protocol step updates cipher modes and encryption keys?
A. Alert Protocol
B. Handshake Protocol
C. ChangeCipherSpec Protocol
D. Record Protocol
Answer: C
Explanation: The ChangeCipherSpec message switches to negotiated cipher suite

4.Which is not a secure email transfer mechanism?
A. POP3
B. SSMTP
C. PGP
D. S/MIME
Answer: A
Explanation: POP3 is plaintext only; the others provide encryption/authentication

5. Compared to WPA2, WPA3 offers all of the following except:
A. Improved handshake protection
B. Individualized data encryption
C. Simpler password-based authentication
D. Uses 40-bit encryption
Answer: D
Explanation: WPA3 increases key sizes, not decreases – it does not use 40-bit encryption.

Thank you