

## UNIT-II

### 1. Introduction to Symmetric Key Cryptography

#### Definition

Symmetric key cryptography is a method of encryption where the same secret key is used for both encryption and decryption.

#### Basic Process

- Sender encrypts plaintext using a secret key.
- Ciphertext is transmitted through a communication channel.
- Receiver decrypts ciphertext using the same key.

#### Features

- Fast encryption and decryption.
- Suitable for large amounts of data.
- Requires secure key distribution.

#### Advantages

- High speed.
- Efficient for bulk data encryption.
- Less computational complexity.

#### Disadvantages

- Key distribution problem.
- Difficult key management for large networks.
- Lack of non-repudiation.

#### Applications

- Secure communication.
- Banking systems.
- VPNs.
- Wireless security.
- File encryption.

### 2. Block Cipher Principles

#### Definition

A block cipher encrypts data in fixed-size blocks using a symmetric key.

#### Characteristics

- Operates on fixed-size blocks.
- Uses substitution and permutation techniques.
- Same plaintext block with same key produces same ciphertext.

# CRYPTOGRAPHY AND NETWORK SECURITY

## Important Concepts

### Plaintext

Original readable message.

### Ciphertext

Encrypted unreadable message.

### Encryption Algorithm

Procedure used to convert plaintext into ciphertext.

### Secret Key

Shared key used for encryption and decryption.

### Decryption Algorithm

Converts ciphertext back into plaintext.

### Confusion and Diffusion

#### Confusion

- Hides relationship between key and ciphertext.
- Achieved using substitution.

#### Diffusion

- Spreads influence of one plaintext bit across many ciphertext bits.
- Achieved using permutation.

### Product Cipher

#### Combination of:

- Substitution
- Permutation
- Transposition

### Feistel Structure

Many block ciphers use Feistel architecture.

#### Working Steps

1. Divide plaintext into two halves.
2. Apply round function on one half.
3. XOR result with other half.
4. Swap halves.
5. Repeat for multiple rounds.

# CRYPTOGRAPHY AND NETWORK SECURITY

## Advantages of Block Ciphers

- Strong security.
- Efficient for digital communication.
- Suitable for hardware and software implementation.

## 3. Data Encryption Standard (DES)

### Introduction

DES is a symmetric block cipher developed by IBM and adopted by NIST in 1977.

### Features

- Block size: 64 bits
- Key size: 56 bits
- Number of rounds: 16
- Based on Feistel structure

### DES Architecture

#### Main Components

1. Initial Permutation (IP)
2. 16 Feistel rounds
3. Final Permutation (FP)

#### DES Working Procedure

##### Step 1: Initial Permutation

- Rearranges bits of plaintext.

##### Step 2: Splitting

- Plaintext divided into Left Half (L) and Right Half (R).

##### Step 3: Round Operations

##### For each round:

- Expansion permutation
- XOR with round key
- Substitution using S-boxes
- Permutation
- XOR with left half
- Swap halves

##### Step 4: Final Permutation

- Produces ciphertext.



your roots for success...

NARSIMHA REDDY  
ENGINEERING COLLEGE

# CRYPTOGRAPHY AND NETWORK SECURITY

## DES Round Function

Contains:

- Expansion box
- XOR operation
- S-box substitution
- Permutation box

Advantages

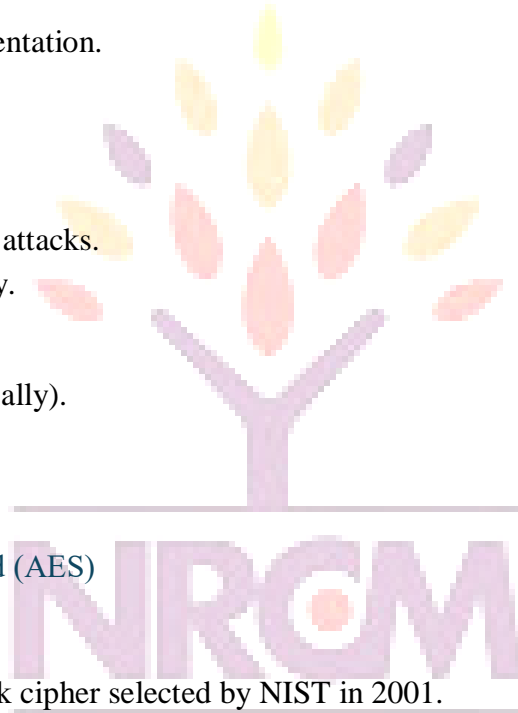
- Simple hardware implementation.
- Widely used historically.

Disadvantages

- Small key size.
- Vulnerable to brute-force attacks.
- Considered insecure today.

Applications

- Banking systems (historically).
- Legacy security systems.



## 4. Advanced Encryption Standard (AES)

Introduction

AES is a modern symmetric block cipher selected by NIST in 2001.

Features

- Block size: 128 bits
- Key sizes: 128, 192, 256 bits
- Faster and more secure than DES

AES Structure

AES uses substitution-permutation network instead of Feistel structure.

Number of Rounds

- AES-128 → 10 rounds
- AES-192 → 12 rounds
- AES-256 → 14 rounds

AES Working Procedure

Step 1: Add Round Key

Plaintext XORed with initial key.

# CRYPTOGRAPHY AND NETWORK SECURITY

## Step 2: SubBytes

- Byte substitution using S-box.

## Step 3: ShiftRows

- Rows shifted cyclically.

## Step 4: MixColumns

- Columns mixed mathematically.

## Step 5: AddRoundKey

- XOR with round key.

## Final Round

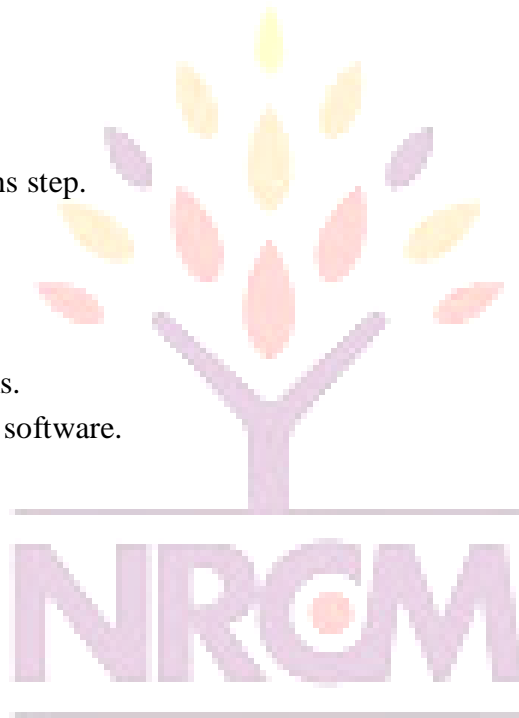
Final round excludes MixColumns step.

## Advantages

- Strong security.
- Fast performance.
- Resistant to known attacks.
- Efficient in hardware and software.

## Applications

- Wi-Fi security.
- SSL/TLS.
- Government security.
- Cloud security.
- Mobile applications.



your roots for success...

## 5. Blowfish Algorithm

### Introduction

Blowfish is a symmetric block cipher designed by Bruce Schneier.

### Features

- Block size: 64 bits
- Key size: 32 to 448 bits
- Feistel network
- 16 rounds

### Structure

- Uses large key-dependent S-boxes.
- Fast encryption.

# CRYPTOGRAPHY AND NETWORK SECURITY

## Blowfish Working

### Step 1

Split plaintext into two 32-bit halves.

### Step 2

Apply Feistel function for 16 rounds.

### Step 3

Use P-array and S-boxes.

### Step 4

Combine halves to produce ciphertext.

### Advantages

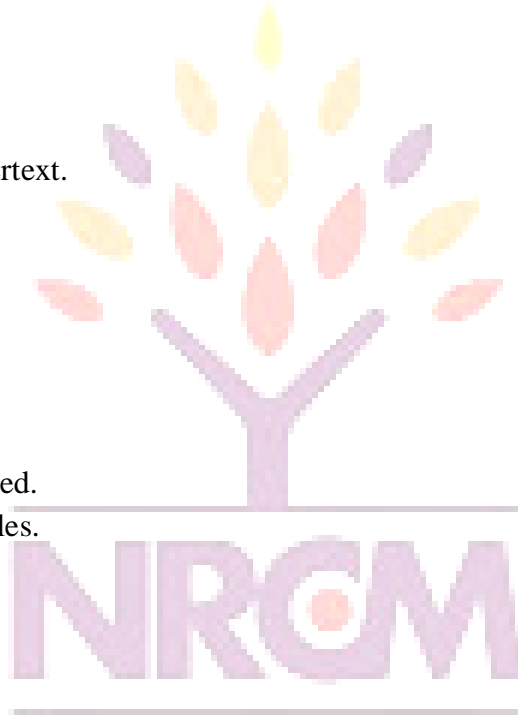
- Free and open algorithm.
- Flexible key size.
- Good performance.

### Disadvantages

- 64-bit block size is outdated.
- Not ideal for very large files.

### Applications

- Password protection.
- File encryption.
- Secure software tools.



## 6. RC5 Algorithm

### Introduction

RC5 is a symmetric block cipher designed by Ronald Rivest.

### Features

- Variable block size.
- Variable key size.
- Variable number of rounds.
- Simple operations.

### RC5 Parameters

- Word size ( $w$ )
- Number of rounds ( $r$ )
- Key length ( $b$ )

# CRYPTOGRAPHY AND NETWORK SECURITY

## Operations Used

- XOR
- Addition modulo  $2^w$
- Circular shifts

## RC5 Working Procedure

### Step 1

Plaintext divided into two words.

### Step 2

Initial key addition.

### Step 3

Repeated rounds involving:

- XOR
- Circular shifts
- Addition

### Step 4

Generate ciphertext.

## Advantages

- Simplicity.
- Fast implementation.
- Flexible design.

## Disadvantages

- Patent restrictions existed earlier.
- Less popular today.

## Applications

- Embedded systems.
- Secure communication.

## 7. IDEA (International Data Encryption Algorithm)

### Introduction

IDEA is a symmetric block cipher developed in Switzerland.

### Features

- Block size: 64 bits
- Key size: 128 bits
- 8 rounds + output transformation



your roots for success...

NARSIMHA REDDY  
ENGINEERING COLLEGE

# CRYPTOGRAPHY AND NETWORK SECURITY

## Operations Used

- XOR
- Addition modulo  $2^{16}$
- Multiplication modulo  $(2^{16} + 1)$

## IDEA Working

### Step 1

Plaintext divided into four 16-bit blocks.

### Step 2

Apply mathematical operations in rounds.

### Step 3

Generate subkeys from main key.

### Step 4

Final transformation produces ciphertext.

## Advantages

- Strong security.
- Resistant to differential cryptanalysis.

## Disadvantages

- Complex mathematical operations.
- Slower compared to AES.

## Applications

- PGP encryption.
- Secure email systems.

## 8. Block Cipher Modes of Operation

### Definition

Modes of operation define how block ciphers process data larger than one block.

### Need for Modes

- Encrypt large data.
- Improve security.
- Handle repeated plaintext patterns.

### 8.1 Electronic Code Book (ECB)

#### Working

Each plaintext block encrypted independently.

# CRYPTOGRAPHY AND NETWORK SECURITY

## Advantages

- Simple implementation.
- Parallel processing possible.

## Disadvantages

- Repeated plaintext produces repeated ciphertext.
- Weak security.

## Applications

- Small random data.

## 8.2 Cipher Block Chaining (CBC)

### Working

- Each plaintext block XORed with previous ciphertext block.
- Uses Initialization Vector (IV).

### Advantages

- Better security than ECB.
- Hides plaintext patterns.

### Disadvantages

- Encryption cannot be parallelized.

### Applications

- File encryption.
- SSL protocols.

## 8.3 Cipher Feedback Mode (CFB)

### Working

- Converts block cipher into stream cipher.
- Uses previous ciphertext as input.

### Advantages

- Suitable for stream data.
- No padding required.

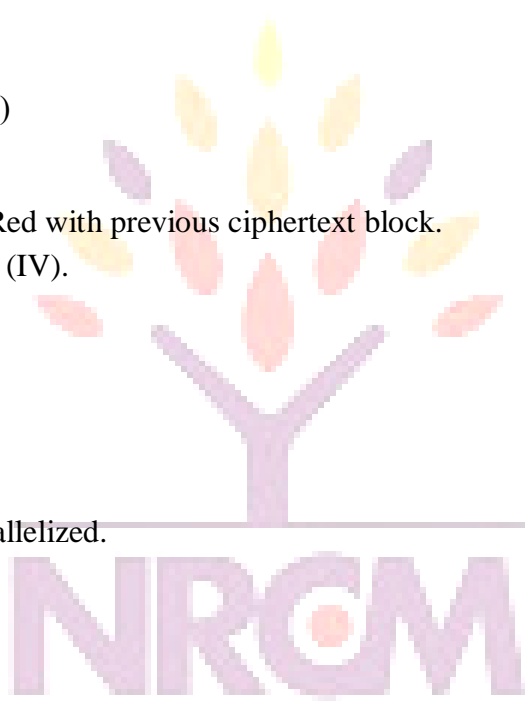
### Disadvantages

- Error propagation occurs.

## 8.4 Output Feedback Mode (OFB)

### Working

- Generates keystream independent of plaintext.



your tools for success...

NARSIMHA REDDY  
ENGINEERING COLLEGE

# CRYPTOGRAPHY AND NETWORK SECURITY

## Advantages

- No error propagation.
- Suitable for noisy channels.

## Disadvantages

- IV reuse dangerous.

## 8.5 Counter Mode (CTR)

### Working

- Encrypts counter values.
- XOR result with plaintext.

### Advantages

- High speed.
- Parallel processing.
- Random access possible.

### Disadvantages

- Counter reuse causes security risks.

### Applications

- High-speed network encryption.

## 9. Stream Ciphers

### Definition

A stream cipher encrypts data one bit or byte at a time.

### Characteristics

- Continuous encryption process.
- Uses keystream generator.
- Faster than block ciphers.

### Working

Ciphertext = Plaintext XOR Keystream

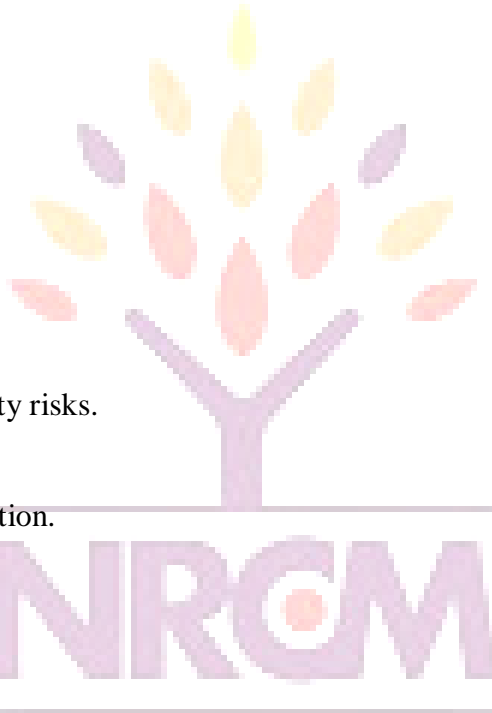
### Types

#### Synchronous Stream Cipher

Keystream independent of plaintext and ciphertext.

#### Self-Synchronizing Stream Cipher

Keystream depends on previous ciphertext.



# CRYPTOGRAPHY AND NETWORK SECURITY

## Advantages

- Fast processing.
- Low memory usage.
- Suitable for real-time communication.

## Disadvantages

- Key reuse dangerous.
- Sensitive to synchronization errors.

## Applications

- Wireless communication.
- Audio/video streaming.
- Mobile communication.

## 10. RC4 Stream Cipher

### Introduction

RC4 is a widely known stream cipher developed by Ronald Rivest.

### Features

- Variable key size.
- Byte-oriented stream cipher.
- Simple and fast.

### Main Components

1. Key Scheduling Algorithm (KSA)
2. Pseudo Random Generation Algorithm (PRGA)

### RC4 Working Procedure

#### Step 1: Initialization

- Initialize state array S with values 0–255.

#### Step 2: Key Scheduling Algorithm (KSA)

- Rearranges array using secret key.

#### Step 3: Pseudo Random Generation Algorithm (PRGA)

- Generates keystream bytes.

#### Step 4: Encryption

Ciphertext = Plaintext XOR Keystream

## Advantages

- Very fast.
- Easy implementation.
- Low memory requirement.

# CRYPTOGRAPHY AND NETWORK SECURITY

## Disadvantages

- Weak security.
- Vulnerable to several attacks.
- No longer recommended.

## Applications

- Earlier versions of SSL/TLS.
- WEP wireless security.

## 11. Comparison of Symmetric Algorithms

Algorithm	Block Size	Key Size	Structure	Security Level
DES	64 bits	56 bits	Feistel	Low
AES	128 bits	128/192/256 bits	SP Network	Very High
Blowfish	64 bits	32–448 bits	Feistel	High
RC5	Variable	Variable	Feistel-like	High
IDEA	64 bits	128 bits	Substitution-Mixing	High
RC4	Stream Cipher	Variable	Stream Cipher	Low

## 12. Difference Between Block Cipher and Stream Cipher

Feature	Block Cipher	Stream Cipher
Data Processing	Block-by-block	Bit/Byte-by-byte
Speed	Moderate	Faster
Memory Requirement	Higher	Lower
Error Propagation	More	Less
Examples	AES, DES	RC4

NARSIMHA REDDY  
ENGINEERING COLLEGE



your roots for success...

# NARSIMHA REDDY ENGINEERING COLLEGE