ANNMACHARYA INSTITUTE OF TECHNOLOGY & SCIENCES,

RAJAMPET

(AUTONOMOUS)

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & DATASCIENCE

LECTURE NOTES

NAME OF THE FACULTY: P.RENUKA

CLASS: III B.TECH II SEM

NAME OF THECOURSE: NETWORK SECURITY & CRYPTOGRAPHY

SUBJECT CODE: 23A326AT

ACADEMIC YEAR:2025-2026

UNIT 1: INTRODUCTION TO COMPUTER SECURITY & CRYPTOGRAPHY

---

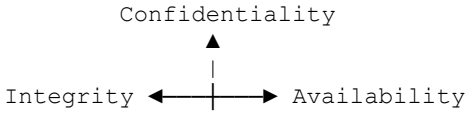
1. Introduction to Computer Security Concepts

Computer Security refers to the protection of computer systems, networks, and data from **unauthorized access, misuse, damage, or attacks**.

Objectives of Computer Security

- Protect information
- Ensure reliable system operation
- Prevent unauthorized access

CIA Triad (Core Security Goals)



- **Confidentiality** – Data is accessible only to authorized users
- **Integrity** – Data is accurate and not altered
- **Availability** – Systems and data are accessible when needed

Computer Security Concepts

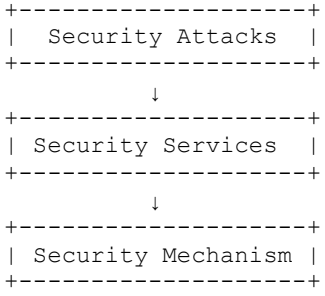
Key Concepts

- **Authentication** – Verifying identity (passwords, biometrics)
- **Authorization** – Granting access rights
- **Accountability** – Tracking user actions
- **Non-repudiation** – Sender cannot deny sending data

3. OSI Security Architecture

The OSI Security Architecture defines **security attacks, services, and mechanisms**.

OSI Security Architecture Diagram



---

4. Security Attacks

A **security attack** is any action that compromises system security.

Types of Attacks

Passive Attacks

- Eavesdropping
- Traffic analysis

Active Attacks

- Masquerade
- Replay attacks
- Modification of messages
- Denial of Service (DoS)

5. Security Services

Security services protect systems against attacks.

Major Security Services

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation
- Availability

6. Security Mechanisms

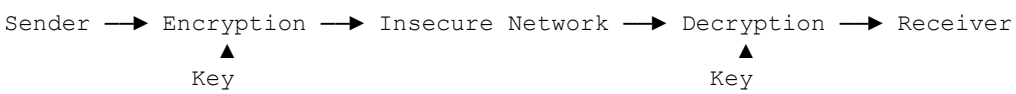
Security mechanisms implement security services.

Examples

- Encryption
- Digital signatures
- Firewalls
- Intrusion detection systems
- Access control mechanisms

7. Model for Network Security

Network Security Model Diagram



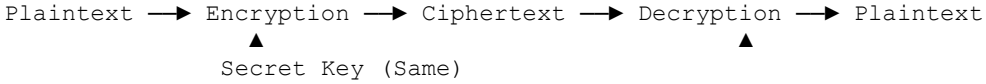
- Message is encrypted before transmission

- Secure keys ensure confidentiality

8. Symmetric Cipher Model

In symmetric encryption, **the same key** is used for encryption and decryption.

Symmetric Cipher Diagram



Advantages

- Fast
- Suitable for large data

Disadvantages

- Key distribution problem

9. Substitution Techniques

Substitution ciphers replace plaintext characters with other characters.

Examples

- Caesar Cipher
- Monoalphabetic Cipher
- Playfair Cipher

Caesar Cipher Example

```
Plaintext : HELLO
Key shift : +3
Ciphertext: KHOOR
```

10. Transposition Techniques

Transposition ciphers rearrange the positions of characters.

Example

```
Plaintext : ATTACK
Key       : 3
Ciphertext: TAACTK
```

Characteristics

- No character substitution
- Changes order only

11. Steganography

Steganography hides **the existence of a message**.

Difference from Cryptography

- Cryptography hides content
- Steganography hides message itself

Steganography Diagram

```
Secret Message + Image → Stego Image → Receiver extracts message
```

Applications

- Secure communication
- Digital watermarking

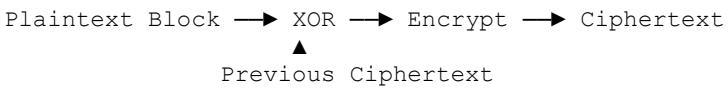
12. Cipher Block Modes of Operation

Block ciphers encrypt fixed-size blocks.

Common Modes

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining)
- CFB
- OFB
- CTR

CBC Mode Diagram



13. Data Encryption Standard (DES)

DES is a **symmetric block cipher**.

Features

- Block size: 64 bits
- Key size: 56 bits
- 16 rounds of encryption

Limitations

- Short key length
- Vulnerable to brute-force attacks

14. Advanced Encryption Standard (AES)

AES is a modern replacement for DES.

Features

- Block size: 128 bits
- Key sizes: 128, 192, 256 bits
- Strong security

AES Structure Diagram

```
Input Block
   ↓
SubBytes
   ↓
ShiftRows
   ↓
MixColumns
   ↓
AddRoundKey
```

Advantages

- Fast
- Highly secure
- Widely used

UNIT 2: NUMBER THEORY & PUBLIC KEY CRYPTOGRAPHY

1. Number Theory (Basics)

Number theory is the **mathematical foundation of cryptography**. It deals with properties of integers.

Key Concepts

- Prime numbers
- Divisibility
- Greatest Common Divisor (GCD)
- Modular arithmetic

2. Euclidean Algorithm

The **Euclidean Algorithm** is used to find the **Greatest Common Divisor (GCD)** of two integers.

Algorithm

If `a > b`:

```
a = bq + r
```

Repeat until `r = 0`.

Example

Find GCD(48, 18):

```
48 = 18 × 2 + 12
18 = 12 × 1 + 6
12 = 6 × 2 + 0
```

✔GCD = 6

Importance in Cryptography

- Used in RSA for key generation
- Helps find modular inverses

3. Modular Arithmetic

Modular arithmetic deals with **remainders**.

Notation

```
a ≡ b (mod n)
```

Means `a` and `b` leave the same remainder when divided by `n`.

Example

```
17 mod 5 = 2
```

Properties

- Addition: (a + b) mod n
- Multiplication: (a × b) mod n
- Subtraction: (a − b) mod n

4. Fermat's Little Theorem

Statement

If `p` is prime and `a` is not divisible by `p`:

```
a^(p-1) ≡ 1 (mod p)
```

Use

- Simplifies large exponent calculations
- Used in primality testing

5. Euler's Totient Theorem

Euler's Totient Function (φ(n))

Counts numbers less than `n` that are **coprime** to `n`.

Theorem

If `gcd(a, n) = 1`:

```
a^φ(n) ≡ 1 (mod n)
```

Application

- Core principle behind **RSA encryption**

6. Chinese Remainder Theorem (CRT)

CRT solves **simultaneous congruences**.

Statement

If moduli are pairwise coprime, a **unique solution** exists.

Example

```
x ≡ 2 (mod 3)
x ≡ 3 (mod 5)
```

✔Unique solution exists modulo 15.

Use in Cryptography

- Improves RSA efficiency
- Used in modular computations

7. Discrete Logarithm Problem

Definition

Given:

```
a^x ≡ b (mod p)
```

Find `x`.

Importance

- Computationally hard
- Security basis for Diffie-Hellman and ECC

8. Finite Fields

A **finite field** is a set with finite elements where addition, subtraction, multiplication, and division are defined.

8.1 Finite Field GF(p)

- `p` is a prime number
- Elements: `{0, 1, 2, ..., p-1}`

Example

GF(7) = {0,1,2,3,4,5,6}

8.2 Finite Field GF(2^n)

- Used in **binary systems**
- Elements are binary polynomials

Application

- AES encryption
- Error-correcting codes

9. Public Key Cryptography

Public key cryptography uses **two keys**.

Keys

- Public Key – shared openly
- Private Key – kept secret

Diagram

```
Sender → Encrypt (Public Key) → Ciphertext → Decrypt (Private Key) → Receiver
```

Advantages

- Secure key exchange
- Digital signatures

10. RSA Algorithm

RSA is the **most widely used public key algorithm**.

Key Generation Steps

1. Choose two primes `p` and `q`
2. Compute `n = p × q`
3. Compute `φ(n)`
4. Choose public key `e`
5. Compute private key `d`

Encryption

```
C = M^e mod n
```

Decryption

```
M = C^d mod n
```

Security Basis

- Difficulty of **factorizing large numbers**

11. Diffie–Hellman Key Exchange

Allows two parties to **securely share a secret key** over an insecure channel.

Steps

1. Agree on public values `p` and `g`
2. Exchange computed values
3. Generate common secret key

Diagram

```
Alice → A = g^a mod p → Bob
Bob   → B = g^b mod p → Alice
Shared Key = g^(ab) mod p
```

Security

- Based on discrete logarithm problem

12. Elliptic Curve Cryptography (ECC)

ECC uses **elliptic curves over finite fields**.

Elliptic Curve Equation

$$y^2 = x^3 + ax + b$$

ECC Diagram (Conceptual)

```
Point P + Point Q = Point R (on curve)
```

Advantages

- Smaller key size
- Faster computation
- High security

Applications

- Secure messaging
- Digital certificates
- Blockchain systems

UNIT 3 – Cryptographic Hash Functions & PKI

---

1. Cryptographic Hash Functions

A **cryptographic hash function** converts input data of any length into a **fixed-length hash value (message digest)**.

Characteristics

- One-way function
- Fixed output size
- Fast computation
- Deterministic

Hash Function Diagram

```
Message ⟶ Hash Function ⟶ Hash Value (Digest)
```

2. Applications of Hash Functions

- Data integrity verification
- Password storage
- Digital signatures
- Message authentication
- File fingerprinting

3. Requirements and Security of Hash Functions

Security Requirements

1. **Preimage resistance** – Hard to find input from hash
2. **Second preimage resistance** – Hard to find another input with same hash
3. **Collision resistance** – Hard to find two inputs with same hash

Avalanche Effect

- Small change in input → large change in output

4. Secure Hash Algorithm (SHA)

SHA is a family of cryptographic hash functions developed by **NIST**.

SHA Family

- SHA-1 (obsolete)

- SHA-2 (SHA-256, SHA-512)
- SHA-3

SHA Working Model

```
Message → Padding → Block Processing → Hash Output
```

Features

- High security
- Widely used
- Resistant to attacks

5. Message Authentication Functions

Message Authentication ensures:

- Message integrity
- Data origin authentication

Message Authentication Model

```
Sender ⟶ MAC Generation ⟶ Message + MAC ⟶ Receiver
```

6. Message Authentication Codes (MAC)

MAC uses a **secret key** with a message.

Types

- Hash-based MAC (HMAC)
- Cipher-based MAC (CMAC)

7. HMAC (Hash-Based Message Authentication Code)

HMAC uses a **hash function + secret key**.

HMAC Structure

```
Key + Message ⟶ Hash ⟶ MAC
```

Advantages

- Strong security
- Resistant to collision attacks
- Works with SHA-256, SHA-512

8. CMAC (Cipher-Based Message Authentication Code)

CMAC uses a **block cipher (AES)**.

Features

- Uses symmetric encryption
- Fixed-length output
- Strong integrity protection

Comparison: HMAC vs CMAC

Feature	HMAC	CMAC
Based On	Hash	Block Cipher
Speed	Fast	Moderate
Usage	Widely used	Secure environments

9. NIST Digital Signature Algorithms

Digital signatures provide:

- Authentication
- Integrity
- Non-repudiation

NIST Approved Algorithms

- **DSA** (Digital Signature Algorithm)
- **RSA Signatures**
- **ECDSA** (Elliptic Curve DSA)

Digital Signature Model

```
Sender ⟶ Hash ⟶ Sign (Private Key) ⟶ Signature
Receiver ⟶ Verify (Public Key)
```

10. Distribution of Public Keys

Public key distribution is a major challenge.

Methods

- Public announcement
- Public directories
- Public key authority
- Certificates

11. X.509 Certificates

X.509 defines the **standard format for public key certificates**.

Certificate Contents

- Subject name
- Public key
- Issuer name
- Validity period
- Digital signature

Certificate Structure

```
Certificate = { User Info + Public Key + CA Signature }
```

12. Public Key Infrastructure (PKI)

PKI is a **framework** that manages public key encryption.

Components of PKI

- Certificate Authority (CA)
- Registration Authority (RA)
- Digital Certificates
- Certificate Revocation List (CRL)

PKI Model Diagram

```
User → RA → CA → Certificate
          ↓
        Repository
```

13. Applications of PKI

- Secure web browsing (HTTPS)
- Secure email
- VPNs
- Digital signatures
- Authentication systems

14. Advantages of PKI

- Strong authentication
- Secure key management
- Trust establishment
- Scalable security

UNIT 4: AUTHENTICATION, E-MAIL SECURITY & IP SECURITY

---

1. Remote User Authentication – Principles

Remote user authentication verifies the **identity of a user accessing a system over a network**.

Goals

- Verify user identity
- Prevent impersonation
- Protect credentials
- Ensure secure communication

Authentication Factors

1. **Something you know** – Password, PIN
2. **Something you have** – Smart card, token
3. **Something you are** – Biometrics

Remote Authentication Model

```
User ⟶ Credentials ⟶ Authentication Server ⟶ Access Granted/Denied
```

Challenges

- Password sniffing
- Replay attacks
- Man-in-the-middle attacks

2. Kerberos Authentication System

Kerberos is a **trusted third-party authentication protocol** developed by MIT.

Key Concepts

- Uses **tickets** instead of passwords
- Based on **symmetric key cryptography**
- Prevents password transmission over network

Main Components

- Client
- Authentication Server (AS)
- Ticket Granting Server (TGS)
- Application Server

Kerberos Working

```
Client → AS → Ticket Granting Ticket (TGT)
Client → TGS → Service Ticket
Client → Server → Secure Access
```

Advantages

- Strong authentication
- Mutual authentication
- Password never sent in plaintext

Limitations

- Time synchronization required
- Single point of failure (KDC)

3. E-Mail Security

E-mail security protects messages from:

- Unauthorized access
- Modification
- Forgery

Security Requirements

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

4. Pretty Good Privacy (PGP)

PGP is a **widely used e-mail security system**.

Services Provided by PGP

- Encryption (confidentiality)
- Digital signatures
- Compression
- Key management

PGP Operation

```
Message → Hash → Sign → Encrypt → Send
Receive → Decrypt → Verify → Read
```

Algorithms Used

- RSA
- AES
- SHA

5. S/MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME is a **standard for secure e-mail** using X.509 certificates.

Features

- Encryption
- Digital signatures
- Certificate-based authentication

Comparison: PGP vs S/MIME

Feature	PGP	S/MIME
Key Management	User-based	Certificate-based
Standardization	Less	Highly standardized
Usage	Personal	Enterprise

6. IP Security (IPsec) – Overview

IPsec secures data at the **IP layer**.

Services Provided

- Data confidentiality
- Data integrity
- Authentication
- Replay protection

IPsec Modes

- **Transport Mode** – Protects payload
- **Tunnel Mode** – Protects entire packet

7. IP Security Architecture

IPsec Components

- Security Associations (SA)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)

8. IP Security Policy

An IPsec policy defines:

- Which traffic to protect
- What security services to use
- Which algorithms to apply

Policy Elements

- Source and destination IP
- Protocol type
- Security mechanism

9. Encapsulating Security Payload (ESP)

ESP provides:

- Confidentiality
- Integrity
- Authentication

ESP Packet Format

```
IP Header | ESP Header | Encrypted Data | ESP Trailer | Auth Data
```

Advantages

- Strong encryption
- Protects data payload

10. Security Associations (SA)

A **Security Association** is a **set of parameters** defining how two systems communicate securely.

SA Parameters

- Encryption algorithm
- Keys
- Mode (transport/tunnel)

SA Identification

- SPI (Security Parameter Index)
- IP address
- Security protocol

11. Combining Security Associations

Multiple SAs can be combined for enhanced security.

Combination Types

- Transport adjacency
- Iterated tunneling

Example

```
Encryption + Authentication → Higher Security
```

12. Internet Key Exchange (IKE)

IKE is a protocol used to **establish Security Associations**.

Functions

- Key generation
- Authentication
- SA negotiation

IKE Phases

Phase 1

- Establish secure channel

Phase 2

- Establish IPsec SAs

IKE Diagram

```
Host A ⇄ IKE ⇄ Host B
     ↓          ↓
   Secure Keys & SA
```

13. Advantages of IPsec

- Network-level security
- Transparent to applications
- Strong cryptographic protection

UNIT V – WEB SECURITY & FIREWALLS

---

1. Web Security Requirements

Web security focuses on protecting **web applications, services, and data** from threats while using the internet.

Key Web Security Requirements

1. **Confidentiality**
   - Prevent unauthorized access to data
   - Achieved using encryption (TLS/HTTPS)
2. **Integrity**
   - Ensure data is not altered during transmission
   - Achieved using hashes and MACs
3. **Authentication**
   - Verify identity of users and servers
   - Achieved using certificates, passwords, tokens
4. **Non-repudiation**
   - Sender cannot deny sending data
   - Achieved using digital signatures
5. **Availability**
   - Services should be accessible when required
   - Protection against DoS attacks

2. Transport Layer Security (TLS)

TLS is a **cryptographic protocol** that provides secure communication over a network.

Objectives of TLS

- Privacy (encryption)
- Data integrity
- Authentication

TLS Working Model

```
Client ⟶ TLS Handshake ⟶ Secure Channel ⟶ Server
```

TLS Handshake Steps

1. Client sends supported algorithms
2. Server sends certificate
3. Key exchange
4. Secure session established

Advantages

- Strong encryption
- Widely used
- Protects against eavesdropping

3. HTTPS (HyperText Transfer Protocol Secure)

HTTPS is **HTTP over TLS/SSL**.

Difference Between HTTP and HTTPS

Feature	HTTP	HTTPS
Encryption	No	Yes
Security	Weak	Strong
Port	80	443

HTTPS Communication Diagram

```
Browser ⟶ HTTPS Request ⟶ Secure Web Server
        ⟵ Encrypted Response ⟵
```

Benefits

- Secure online transactions
- Prevents data interception
- Ensures website authenticity

4. Secure Shell (SSH)

SSH is a **secure protocol for remote login and command execution**.

Features

- Encrypted communication
- Secure authentication
- Data integrity

SSH Model

```
User ⟶ SSH Client ⟶ Encrypted Channel ⟶ SSH Server
```

Applications

- Remote system administration
- Secure file transfer (SCP, SFTP)

5. Firewalls

A firewall is a **security device or software** that monitors and controls network traffic.

Functions of a Firewall

- Allow authorized traffic
- Block unauthorized access
- Protect internal networks

6. Characteristics of a Firewall

- All traffic must pass through the firewall
- Only authorized traffic is allowed
- Firewall itself must be secure
- Enforces security policy

7. Types of Firewalls

1. Packet Filtering Firewall

- Filters packets based on IP, port, protocol
- Fast but limited security

2. Stateful Inspection Firewall

- Tracks connection states
- More secure than packet filtering

3. Application-Level Gateway (Proxy Firewall)

- Filters at application layer
- High security but slower

4. Next-Generation Firewall (NGFW)

- Deep packet inspection
- Intrusion prevention
- Application awareness

8. Firewall Location

Network Firewall Placement

```
Internet ⟶ Firewall ⟶ Internal Network
```

DMZ (Demilitarized Zone) Configuration

```
Internet
   |
Firewall
   |
  DMZ (Web Server)
   |
Internal Network
```

9. Firewall Configuration

Firewall configuration defines **rules and policies**.

Configuration Rules

- Source and destination IP
- Port numbers
- Protocol type
- Action (allow/deny)

Best Practices

- Default deny policy
- Least privilege principle
- Regular rule updates
- Log monitoring

10. Advantages of Firewalls

- Prevent unauthorized access
- Protect sensitive data
- Enforce security policies
- Reduce attack surface

11. Limitations of Firewalls

- Cannot protect against internal threats
- Cannot stop attacks through allowed traffic
- Requires proper configuration