ABHYASMITRA.IN
COMPREHENSIVE UNIVERSITY STUDY NOTES

NETWORK AND SECURITY

Unit V — Cryptography and Access Control Models

Topics Covered in this Unit

Introduction to Cryptography: Security Services (CIA & Non-Repudiation) & Attack Models
Symmetric Key Cryptography: Data Encryption Standard (DES Feistel & 3DES) & AES Architecture
Advanced Encryption Standard (AES): 128/192/256-bit SPN, State Matrix & Round Transformations
Asymmetric Key Cryptography: Mathematical Trapdoor Functions & The RSA Algorithm (Step-by-Step)
Cryptographic Hash Functions: Collision Resistance, MD5, SHA-256/SHA-3 & Digital Signatures
Access Control Models: Discretionary Access Control (DAC), Mandatory Access Control (MAC / MLS)
Role-Based Access Control (RBAC) & Dynamic Context-Aware Attribute-Based Access Control (ABAC)
Master Comparison Table of Access Control Models & Security Architecture Integration
High-Yield University Exam Question Bank with Numerical Solutions & Unit Summary

Compiled in a structured, easy-to-understand, textbook style format
Specially curated for B.Tech / B.E. / BCA / MCA / B.Sc Computer Science & IT Students

COURSE SYLLABUS & MAPPING

[UNIT V SYLLABUS — PRESCRIBED UNIVERSITY CURRICULUM]

This section contains the official syllabus for Unit V. Verify with your university curriculum mapping.

Unit V Syllabus Breakdown:

Introduction to Cryptography: Need for Cryptography in Network Security, Security services: Confidentiality, Integrity, Authentication, Non-repudiation, Basic terminology, Types of cryptographic attacks: Brute force, Cryptanalysis. Types: Symmetric Key Cryptography: DES, AES; Asymmetric Key Cryptography: RSA. Hash Functions and Digital Signatures. Access Control Models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC).

• Course Code: _____ • Semester / Year: _____

TABLE OF CONTENTS

5.1 Introduction to Cryptography

Definition: Cryptography & Cryptology

Cryptography (derived from Greek 'kryptos' meaning hidden, and 'graphein' meaning writing) is the scientific discipline of transforming plaintext information into unintelligible ciphertext using mathematical algorithms and cryptographic keys, ensuring data confidentiality, integrity, authenticity, and non-repudiation across insecure channels. Cryptology encompasses both Cryptography (creating ciphers) and Cryptanalysis (breaking ciphers).

Primary Security Services Provided by Cryptography

- **1. Confidentiality:** Prevents unauthorized parties from reading sensitive data by encrypting plaintext into ciphertext using strong mathematical ciphers (e.g., AES-256, RSA).
- **2. Data Integrity:** Ensures that data has not been altered, forged, or deleted in transit. Cryptographic hash functions (SHA-256) generate a unique digital fingerprint of the data; any single-bit alteration drastically alters the hash value.
- **3. Authentication:** Verifies the true identity of communicating entities and validates the origin of transmitted messages before granting access.
- **4. Non-Repudiation:** Guarantees that a sender cannot falsely deny having authored or sent a message, and the recipient cannot deny receiving it (enforced via asymmetric Digital Signatures).

Fundamental Cryptographic Terminology

- • **Plaintext (P):** The original, readable message or data in unencrypted cleartext format.
- • **Ciphertext (C):** The scrambled, unintelligible output produced after applying an encryption algorithm to plaintext.
- • **Encryption Algorithm (E):** The mathematical transformation that converts plaintext into ciphertext: C = E(K_e, P).
- • **Decryption Algorithm (D):** The mathematical inverse transformation that restores plaintext from ciphertext: P = D(K_d, C).
- • **Cryptographic Key (K):** A secret numerical parameter (bit string) that controls the operation of encryption and decryption algorithms.
- • **Kerckhoffs's Principle:** A foundational axiom of modern cryptography: 'A cryptographic system must remain secure even if everything about the system, including the algorithm itself, is public knowledge; security must depend solely on keeping the key secret.'

Types of Cryptographic Attacks

- **1. Brute-Force Attack (Exhaustive Key Search):** The attacker systematically tries every possible key in the key space until the correct decryption key is discovered. For an n-bit key, there are 2^n possible keys. With AES-128 (2^128 keys) or AES-256 (2^256 keys), brute-force attacks are computationally infeasible, requiring billions of years even on supercomputer clusters.
- **2. Cryptanalysis Attacks (Mathematical Weakness Exploitation):**
  - • **Ciphertext-Only Attack:** The cryptanalyst possesses only intercepted ciphertext strings and attempts to deduce plaintext or key based on statistical properties.
  - • **Known-Plaintext Attack:** The attacker possesses several known pairs of plaintext and corresponding ciphertext, using them to deduce the secret key.
  - • **Chosen-Plaintext Attack:** The attacker can submit arbitrary plaintext messages of their choice to the encryption machine and analyze the resulting ciphertexts (differential cryptanalysis).
  - • **Chosen-Ciphertext Attack:** The attacker can submit chosen ciphertexts to a decryption oracle and analyze the decrypted plaintext outputs.

5.2 Symmetric Key Cryptography: DES and AES

Definition: Symmetric Key Cryptography (Secret-Key / Private-Key)
Symmetric Key Cryptography is a cryptographic paradigm where the exact same shared secret key (K) is used for both plaintext encryption and ciphertext decryption: P = D(K, E(K, P)).

1. Data Encryption Standard (DES)

Adopted by NIST in 1977, DES is a classic Symmetric Block Cipher based on the Feistel Cipher Network structure.

- **Key Parameters of DES:**
  - Block Size: 64 bits (processes 64-bit plaintext blocks into 64-bit ciphertext blocks).
  - Key Length: 64 bits total, but only 56 bits are effective key bits (every 8th bit is a parity check bit).
  - Number of Rounds: Strictly 16 identical Feistel rounds.
- **Round Mechanics:** Each 64-bit block is split into Left (L) and Right (R) 32-bit halves. For round i: L_i = R_(i-1), and R_i = L_(i-1) XOR F(R_(i-1), K_i). The round function F expands R from 32 to 48 bits, XORs with 48-bit subkey K_i, passes through 8 non-linear S-Boxes (Substitution Boxes: compressing 6 bits to 4 bits), and permutes via a P-Box.

- **Weakness & Obsolescence:** The 56-bit key space (2^56 = 7.2 x 10^16 keys) is too small. In 1999, distributed computing cracked DES in 22 hours.
- **Triple DES (3DES):** Applies DES three times with two or three distinct keys (Key Size: 112 or 168 bits): C = E(K3, D(K2, E(K1, P))). Secure but slow.

2. Advanced Encryption Standard (AES - Rijndael)

Adopted by NIST in 2001 to replace DES, AES is a modern symmetric block cipher based on a Substitution-Permutation Network (SPN). It processes data blocks as a 4x4 State Matrix of 16 bytes.

AES Variant	Block Size	Key Length	Number of Transformation Rounds	Round Subkeys Generated
AES-128	128 bits (16 bytes)	128 bits (16 bytes / 4 words)	10 Rounds	11 Subkeys (44 words)
AES-192	128 bits (16 bytes)	192 bits (24 bytes / 6 words)	12 Rounds	13 Subkeys (52 words)
AES-256	128 bits (16 bytes)	256 bits (32 bytes / 8 words)	14 Rounds	15 Subkeys (60 words)

Four Core Transformations in Each AES Round

- **1. SubBytes (Byte Substitution):** A non-linear byte-by-byte substitution where each state byte is replaced with another byte from a predefined 256-byte S-Box based on multiplicative inverse over Galois Field GF(2^8), providing non-linear confusion.
- **2. ShiftRows (Permutation):** A cyclic left byte shift applied to each row of the 4x4 State Matrix: Row 0 shifted 0 bytes, Row 1 shifted 1 byte left, Row 2 shifted 2 bytes left, Row 3 shifted 3 bytes left, providing horizontal diffusion.
- **3. MixColumns (Column Diffusion):** Each 4-byte column is transformed by multiplying it with a fixed matrix over GF(2^8). MixColumns ensures that modifying a single input bit changes all 16 state bytes within 2 rounds! (Omitted in the final round).
- **4. AddRoundKey:** Bitwise XORs each byte of the State Matrix with the corresponding 128-bit round subkey derived from the master key via AES Key Expansion.

5.3 Asymmetric Key Cryptography & The RSA Algorithm

Definition: Asymmetric Key Cryptography (Public-Key Cryptography)

Asymmetric Key Cryptography uses mathematically related Key Pairs: a Public Key (distributed openly to anyone for encryption or signature verification) and a Private Key (kept strictly confidential by the owner for decryption or signature generation).

The RSA Algorithm (Rivest, Shamir, Adleman - 1977)

RSA is the most widely deployed asymmetric cryptosystem. Its security rests on the computational hardness of factoring the product of two very large prime numbers (Integer Factorization Problem).

Step-by-Step RSA Key Generation Algorithm

- **Step 1:** Choose two very large, distinct prime numbers p and q.
- **Step 2:** Compute the modulus n = p * q. (The bit length of n is the RSA key size, typically 2048 or 4096 bits).
- **Step 3:** Compute Euler's Totient Function: phi(n) = (p - 1) * (q - 1).
- **Step 4:** Select a public exponent e such that 1 < e < phi(n), and e is coprime to phi(n) (gcd(e, phi(n)) = 1). Common choice: e = 65537.
- **Step 5:** Compute the private exponent d such that: d * e = 1 (mod phi(n)), meaning d is the modular multiplicative inverse of e modulo phi(n), computed using the Extended Euclidean Algorithm.
- **Key Pairs Established:** Public Key = (e, n); Private Key = (d, n).

RSA Encryption and Decryption Formulas

- **Encryption (Sender uses Public Key {e, n}):** Ciphertext C = (P^e) mod n [where plaintext P < n]
- **Decryption (Receiver uses Private Key {d, n}):** Plaintext P = (C^d) mod n

Step-by-Step Numerical Example of RSA (Classic Exam Problem)

Problem: Let p = 3, q = 11, and choose e = 7. Encrypt message P = 5 and verify decryption.

- **1. Modulus n:** n = p * q = 3 * 11 = 33.
- **2. Totient phi(n):** phi(n) = (3 - 1) * (11 - 1) = 2 * 10 = 20.
- **3. Public Exponent e:** e = 7 (Coprime to 20 since gcd(7, 20) = 1). Public Key = (7, 33).
- **4. Private Exponent d:** d * 7 = 1 (mod 20) -> Testing values: 7 * 3 = 21 = 1 (mod 20). Thus, d = 3. Private Key = (3, 33).
- **5. Encryption of P = 5:** C = (5^7) mod 33 = 78125 mod 33 = 14. Ciphertext C = 14.
- **6. Decryption of C = 14:** P = (14^3) mod 33 = 2744 mod 33 = 5. Plaintext P = 5 (Verified perfectly!).

5.4 Hash Functions & Digital Signatures

1. Cryptographic Hash Functions

A cryptographic hash function H takes an arbitrary-length message M and compresses it into a fixed-size bit string h = H(M) called a Message Digest or Hash Value.

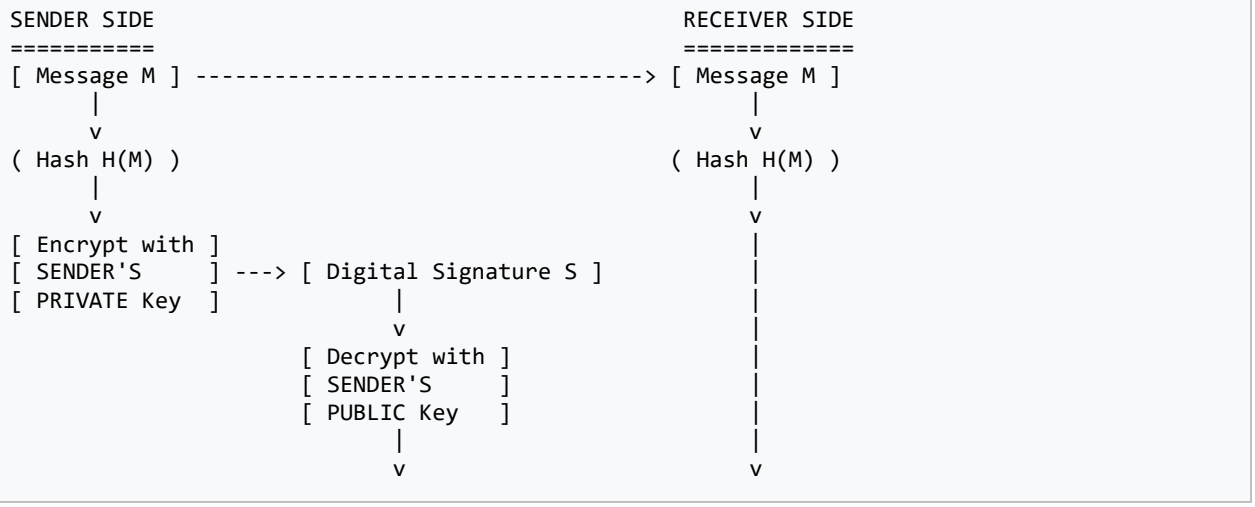
- **Essential Security Properties:**
  - Pre-image Resistance (One-Way Property): Given hash h, it is computationally impossible to find the original message M such that H(M) = h.
  - Second Pre-image Resistance (Weak Collision Resistance): Given message M1, it is impossible to find a different message M2 such that H(M1) = H(M2).
  - Collision Resistance (Strong Collision Resistance): It is computationally impossible to find ANY two arbitrary messages M1 and M2 such that H(M1) = H(M2).
  - Avalanche Effect: Changing even a single bit in the input message alters more than 50% of the output hash bits randomly.
- **Standard Algorithms:** MD5 (128-bit, broken), SHA-1 (160-bit, deprecated), SHA-256 (256-bit secure standard), SHA-3 (Keccak sponge function).

2. Digital Signatures

Definition: Digital Signature

A Digital Signature is a mathematical cryptographic scheme for demonstrating the authenticity, integrity, and non-repudiation of digital messages. It is created by encrypting the cryptographic hash of a message using the sender's Private Key.

DIGITAL SIGNATURE GENERATION & VERIFICATION



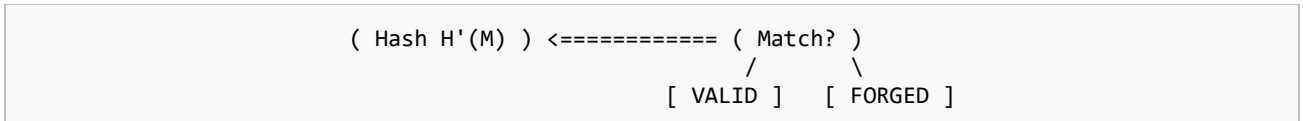


Figure: Digital Signature Workflow ensuring Authentication, Integrity, and Non-Repudiation

5.5 Access Control Models (DAC, MAC, RBAC, ABAC)

Definition: Access Control

Access Control is the fundamental security discipline that regulates which authenticated users or computational processes (Subjects) are granted authorization to execute specific operations (Read, Write, Execute, Delete) on protected network resources, files, and databases (Objects).

1. Discretionary Access Control (DAC)

DAC is an owner-centric model where the creator/owner of an object has complete discretion to grant, modify, or revoke access permissions to other users.

- **Implementation:** Enforced via Access Control Lists (ACLs) attached to objects (e.g., Linux file permissions `chmod 755 file.txt`, Windows NTFS ACLs).
- **Limitation:** High vulnerability to Trojan horses; if a user is tricked into executing malicious code, the malware inherits the user's full permissions and can reassign file permissions to unauthorized entities.

2. Mandatory Access Control (MAC / Multi-Level Security)

MAC is a strict, system-enforced model where access decisions are governed by a central security authority based on fixed Security Classification Labels assigned to all subjects and objects.

- **Security Levels:** Top Secret > Secret > Confidential > Unclassified.
- **Classic Formal Security Models:**
  - • **Bell-LaPadula Model (Confidentiality):** Enforces two rules: (1) Simple Security Property: 'No Read Up' (a subject cannot read objects at a higher security clearance), (2) *-Property (Star Property): 'No Write Down' (a subject cannot write data to a lower classification, preventing leakage).
  - • **Biba Model (Integrity):** Enforces: (1) 'No Read Down' (prevents reading corrupted low-integrity data), (2) 'No Write Up' (prevents tainting high-integrity data).
- **Applications:** Military defense systems, intelligence agencies, SELinux (Security-Enhanced Linux).

3. Role-Based Access Control (RBAC)

RBAC assigns permissions to organizational Roles (e.g., Doctor, Nurse, Billing Clerk, Network Admin), and users are assigned to roles. Users inherit permissions solely through their active role memberships.

- **Core Security Principles:**
  - Principle of Least Privilege: Users are granted only the minimum permissions necessary to perform their job duties.
  - Separation of Duties (SoD): High-risk tasks require multiple roles (e.g., one role creates purchase orders; a separate role approves payment).

4. Attribute-Based Access Control (ABAC)

ABAC is a next-generation, highly dynamic, context-aware access control model (standardized in XACML) that evaluates real-time access policies based on multi-dimensional Attributes:

- **Four Attribute Categories:**
  - Subject Attributes: User role, department, clearance level, security training status.
  - Resource / Object Attributes: File classification, creation date, project tag, data owner.
  - Action Attributes: Read, Write, Delete, Approve, Export.
  - Environmental / Contextual Attributes: Current time of day, geographic location (GPS/IP), device health (patch status), network security posture.
- **Example Policy:** 'Allow READ access to Financial Reports IF user is in Finance Department AND time is between 9 AM - 5 PM AND device is corporate-managed with active antivirus AND connection originates from corporate subnet.' (Core foundation of Zero Trust Architecture!).

Master Comparison Table: Access Control Models

Access Model	Decision Basis	Authority / Control	Flexibility & Context	Ideal Application Domain
DAC	Owner discretion & Object ACLs	Data Owner (User)	Low (Static ACL rules)	Desktop OS, personal file shares, small labs
MAC	Security clearance labels	Central System Administrator	Rigid (Fixed clearance levels)	Military, defense, government intelligence, SELinux
RBAC	Job roles & organizational duties	Enterprise Security Admin	Moderate (Role assignments)	Enterprises, corporate ERP, hospital healthcare

Access Model	Decision Basis	Authority / Control	Flexibility & Context	Ideal Application Domain
ABAC	Multi-attribute contextual policies	Central Policy Engine (XACML)	Maximum (Dynamic context-aware)	Cloud platforms, AWS IAM, Zero Trust Architecture

5.6 High-Yield University Exam Question Bank

Part A: Short Answer Questions (2 to 5 Marks)

Q1. What is Kerckhoffs's Principle? [2 Marks]

- **Answer:** Kerckhoffs's Principle states that a cryptographic system must remain secure even if all details of the encryption algorithm are publicly known; security must rely entirely on keeping the cryptographic key secret.

Q2. List the four round transformations in AES. [3 Marks]

- **Answer:** SubBytes (non-linear S-Box substitution), ShiftRows (cyclic row byte permutation), MixColumns (matrix column mixing over GF(2^8)), and AddRoundKey (bitwise XOR with 128-bit round subkey).

Q3. Differentiate between Symmetric and Asymmetric Key Cryptography. [4 Marks]

Parameter	Symmetric Cryptography	Asymmetric Cryptography
Key Pair	Single shared secret key for encryption & decryption	Public key (encrypt) & Private key (decrypt)
Key Distribution	Complex ($N(N-1)/2$ keys needed for N users)	Simple ($2N$ keys needed for N users)
Computational Speed	Extremely fast (AES, DES)	Slow (RSA, ECC, high mathematical overhead)
Primary Uses	Bulk data encryption (file storage, TLS payload)	Key exchange, Digital Signatures, authentication

Q4. Explain Bell-LaPadula model rules in MAC. [3 Marks]

- **Answer:** Bell-LaPadula enforces confidentiality in MAC: (1) Simple Security Property ('No Read Up'): A subject cannot read objects at a higher classification level. (2) *-Property ('No Write Down'): A subject cannot write data down to a lower classification level, preventing unauthorized data leakage.

Part B: Long Answer Questions (10 to 15 Marks Outline Guides)

- **Q5. Explain the RSA Algorithm in detail. Given primes p = 7, q = 11, choose e = 13. Derive private key d and encrypt message P = 9. Verify decryption. [15 Marks]**
- **Q6. Discuss the architecture of AES. Explain the State Matrix representation, round transformations (SubBytes, ShiftRows, MixColumns, AddRoundKey), and key expansion in detail. [12 Marks]**
- **Q7. Explain Cryptographic Hash Functions, essential security properties (Pre-image, Collision resistance), and the working mechanism of Digital Signatures. [10 Marks]**
- **Q8. Compare Access Control Models: DAC, MAC, RBAC, and ABAC in detail with architecture diagrams and real-world implementation examples. [12 Marks]**

5.7 Unit Summary & Key Takeaways

- Cryptography guarantees Confidentiality, Data Integrity, Authentication, and Non-repudiation based on Kerckhoffs's Principle.
- Symmetric ciphers: DES (64-bit block, 56-bit key, 16-round Feistel) and AES (128-bit block, 128/192/256-bit key, SPN matrix transformations).
- Asymmetric ciphers: RSA uses prime factorization hardness (n = p * q, phi(n) = (p-1)*(q-1), C = (P^e) mod n, P = (C^d) mod n).
- Hash functions (SHA-256) provide one-way collision-resistant digests; Digital Signatures encrypt hashes with sender's private key.
- Access Control: DAC (Owner discretion), MAC (Mandatory classification labels, Bell-LaPadula 'No Read Up/No Write Down'), RBAC (Roles & Least Privilege), and ABAC (Dynamic contextual attributes & Zero Trust).