Cryptography and Network Security

Short notes for B.Tech CSE / IT · BCA · MCA · M.Tech

Uncodemy Handwritten Notes · free for students

I. Introduction

- **Cryptography** = the science of keeping messages secret and safe. **Cryptanalysis** = breaking them. Together = **cryptology**.
- **Plaintext** → (encryption with key) → **ciphertext** → (decryption) → plaintext.

➤ CIA triad and other goals

Goal	Meaning	Tool
Confidentiality	Only allowed people can read	Encryption
Integrity	Data is not changed	Hash, MAC
Availability	System is usable when needed	Backups, DDoS protection
Authentication	Prove who you are	Passwords, certificates
Non-repudiation	Sender cannot deny sending	Digital signature

➤ Attacks (X.800 view)

- **Passive**: only watch. Release of message contents, traffic analysis. Hard to detect, so prevent.
- **Active**: change data. Masquerade, replay, modification, denial of service. Easier to detect, so detect and recover.

➤ Cryptanalysis attack types

- Ciphertext-only, known-plaintext, chosen-plaintext, chosen-ciphertext.
- **Brute force**: try every key. A k-bit key has 2^k possible keys.

2. Classical Ciphers

➤ Substitution ciphers

- **Caesar cipher**: shift each letter by k.

> **FORMULA** Caesar: $C = (P + k) \bmod 26$, $P = (C - k) \bmod 26$. Letters A = 0 … Z = 25.

> **EXAMPLE** "HELLO" with k = 3 → H(7)+3 = 10 = K, E→H, L→O, L→O, O→R. Ciphertext = "KHOOR".

- Only 25 useful keys, so brute force is trivial.
- **Monoalphabetic**: any fixed letter mapping (26! keys), broken by frequency analysis.
- **Playfair**: 5×5 key matrix (I and J together), encrypts letter pairs.
- **Vigenère** (polyalphabetic): $C_i = (P_i + K_i) \bmod 26$ with a repeating keyword.

> **EXAMPLE** Vigenère, plaintext "ATTACK", key "LEMON" → key stream LEMONL. A(0)+L(11) = L, T(19)+E(4) = X, T(19)+M(12) = 31 mod 26 = F, A+O(14) = O, C(2)+N(13) = P, K(10)+L(11) = V. Ciphertext = "LXFOPV".

- **Hill cipher**: $C = K \cdot P \bmod 26$ using a key matrix (needs inverse matrix to decrypt).
- **One-time pad**: random key as long as the message, used once. Perfectly secure but hard to manage.

➤ Transposition ciphers

- Rearrange letter positions. Examples: **Rail fence**, **columnar transposition**.

> **EXAMPLE** Rail fence, 2 rails, "HELLOWORLD": row 1 = H L O O L, row 2 = E L W R D. Ciphertext = "HLOOLELWRD".

- **Steganography** = hiding the existence of a message (e.g. inside an image), not just its meaning.

3. Symmetric Key Cryptography

- Same key for encryption and decryption. Fast. Problem: key distribution.

- **Block cipher** (fixed-size blocks, e.g. DES, AES) vs **stream cipher** (bit / byte at a time, e.g. RC4).
- Shannon's ideas: **confusion** (hide key-ciphertext relation, by substitution) and **diffusion** (spread plaintext effect, by permutation).

➤ DES (Data Encryption Standard)

- Block size 64 bits, key 64 bits of which 56 bits are used (8 parity bits).
- **Feistel structure**, 16 rounds, each with a 48-bit round key.
- Round function: expansion (32 → 48 bits), XOR with key, 8 S-boxes (48 → 32), permutation.
- Weak today due to small key. **Double DES** suffers meet-in-the-middle. **Triple DES** (3DES) uses 2 or 3 keys.

➤ AES (Advanced Encryption Standard)

- Based on the Rijndael cipher. Block size 128 bits. Not a Feistel cipher (it is an SPN).

Key size	Rounds
128 bits	10
192 bits	12
256 bits	14

- Each round: **SubBytes**, **ShiftRows**, **MixColumns**, **AddRoundKey**. The last round skips MixColumns.

➤ Block cipher modes

Mode	Idea	Note
ECB	Each block encrypted alone	Same plaintext → same ciphertext (weak)
CBC	XOR with previous ciphertext block, uses IV	Common, error spreads to next block
CFB	Turns block cipher into stream cipher	Self-synchronising
OFB	Keystream from repeated encryption of IV	Bit errors do not spread
CTR	Encrypt a counter, XOR with plaintext	Parallel, random access

4. Number Theory Basics

- **GCD** by Euclid: $\gcd(a, b) = \gcd(b, a \bmod b)$.
- **Modular inverse**: $a^{-1} \bmod n$ exists only if $\gcd(a, n) = 1$. Found with the extended Euclidean algorithm.
- **Euler's totient** $\phi(n)$ = count of numbers from 1 to n coprime to n. For prime p, $\phi(p) = p - 1$. For $n = p \cdot q$, $\phi(n) = (p - 1)(q - 1)$.
- **Fermat's little theorem**: $a^{(p-1)} \equiv 1 \pmod{p}$ if p is prime and p does not divide a.
- **Euler's theorem**: $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$.

EXAMPLE $\gcd(48, 18)$: $48 \bmod 18 = 12$, $18 \bmod 12 = 6$, $12 \bmod 6 = 0$, so gcd = 6.

EXAMPLE Inverse of 3 mod 7: $3 \times 5 = 15 = 2 \times 7 + 1$, so $3^{-1} = 5$.

5. Public Key Cryptography

- Two keys: **public key** (shared) and **private key** (secret). Solves key distribution. Slower than symmetric.

➤ RSA

1. Choose primes p, q. $n = p \times q$.
2. $\phi(n) = (p - 1)(q - 1)$.
3. Choose e with $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
4. Find d with $e \cdot d \equiv 1 \pmod{\phi(n)}$.
5. Public key = (e, n), private key = (d, n).

FORMULA RSA: $C = M^e \bmod n$, $M = C^d \bmod n$.

EXAMPLE $p = 3$, $q = 11 \rightarrow n = 33$, $\phi = 20$. $e = 3$ ($\gcd(3,20) = 1$). $d = 7$ since $3 \times 7 = 21 \equiv 1 \bmod 20$. $M = 4$: $C = 4^3 \bmod 33 = 64 \bmod 33 = 31$. Check: $31^7 \bmod 33$. $31 \equiv -2$, $(-2)^7 = -128$, $-128 \bmod 33 = -128 + 132 = 4$. Correct.

- Security depends on how hard it is to factor n.

➤ Diffie-Hellman key exchange

- Public: prime q and primitive root α. A picks secret X_A, sends $Y_A = \alpha^{X_A} \bmod q$. B picks X_B, sends $Y_B = \alpha^{X_B} \bmod q$.
- Shared key $K = Y_B^{X_A} \bmod q = Y_A^{X_B} \bmod q$.

EXAMPLE $q = 23$, $\alpha = 5$, $X_A = 6$, $X_B = 15$. $Y_A = 5^6 \bmod 23 = 8$. $Y_B = 5^{15} \bmod 23 = 19$. $K = 19^6 \bmod 23 = 2$ and $8^{15} \bmod 23 = 2$. Shared key = 2.

- Based on the discrete logarithm problem. Weak against **man-in-the-middle** without authentication.
- **ECC** (elliptic curve cryptography): same security as RSA with much smaller keys.

6. Hash Functions, MAC and Digital Signatures

➤ Hash function properties

1. Fixed-length output for any input
2. **Pre-image resistance**: cannot find the input from the hash
3. **Second pre-image resistance**: cannot find another input with the same hash
4. **Collision resistance**: cannot find any two inputs with the same hash

Hash	Output size
MD5	128 bits (broken)
SHA-1	160 bits (broken for collisions)
SHA-256	256 bits
SHA-512	512 bits

FORMULA Birthday attack: a collision on an n-bit hash needs about $2^{(n/2)}$ tries.

- **MAC** = tag made with a secret key; gives integrity + authentication. **HMAC** = MAC built from a hash function.
- **Digital signature**: sender signs the hash with their private key; anyone verifies with the sender's public key. Gives authentication, integrity and non-repudiation.
- Standards: RSA signature, **DSA / DSS**, ECDSA.

REMEMBER Encrypt with receiver's public key = confidentiality. Sign with sender's private key = authentication.

7. Key Management and Authentication

- **KDC (Key Distribution Centre)**: trusted server that gives session keys.
- **Kerberos**: authentication with tickets. Parts: AS (authentication server), TGS (ticket granting server), service server. Uses symmetric keys and timestamps.
- **PKI (Public Key Infrastructure)**: Certificate Authority (CA) issues **X.509 certificates** binding a public key to an identity.
- Certificates can be revoked using CRL or OCSP.

8. Network and Internet Security

Layer	Protocol	Protects
Application	PGP, S/MIME	Email
Transport	SSL / TLS, HTTPS, SSH	Web, remote login
Network	IPSec	IP packets (VPNs)

- **TLS handshake**: agree on cipher suite, verify server certificate, exchange keys, then use symmetric session keys.
- **IPSec**: **AH** gives integrity + authentication; **ESP** also gives encryption. Modes: **transport** (protects payload) and **tunnel** (protects the whole packet).
- **PGP**: email security with signing, compression, encryption and radix-64 encoding.

9. System Security

- **Malware**: virus (attaches to files), worm (spreads by itself), trojan (looks useful, harmful inside), ransomware, spyware.
- **Firewall** types: packet filter, stateful inspection, application-level gateway (proxy), circuit-level gateway.
- **IDS (Intrusion Detection System)**: signature-based (known attacks) and anomaly-based (unusual behaviour). Host-based vs network-based.
- **DoS / DDoS**: flood a target so real users cannot use it.

10. Most Asked Questions (practice)

1. Explain the CIA triad. Passive vs active attacks.
2. Encrypt a message using Caesar, Playfair and Vigenère ciphers.
3. Explain DES structure and one round of DES.
4. Explain AES rounds. Compare DES and AES.
5. Explain block cipher modes ECB, CBC, CFB, OFB and CTR.
6. Solve RSA for given p, q, e and message.
7. Explain Diffie-Hellman with an example. What is a man-in-the-middle attack?
8. Properties of hash functions. Explain HMAC and digital signatures.
9. Explain Kerberos and X.509 certificates.
10. Explain IPSec (AH, ESP) and SSL / TLS.

TIP RSA, Diffie-Hellman and classical cipher numericals are sure-shot marks. Write each step clearly and check the answer by decrypting.