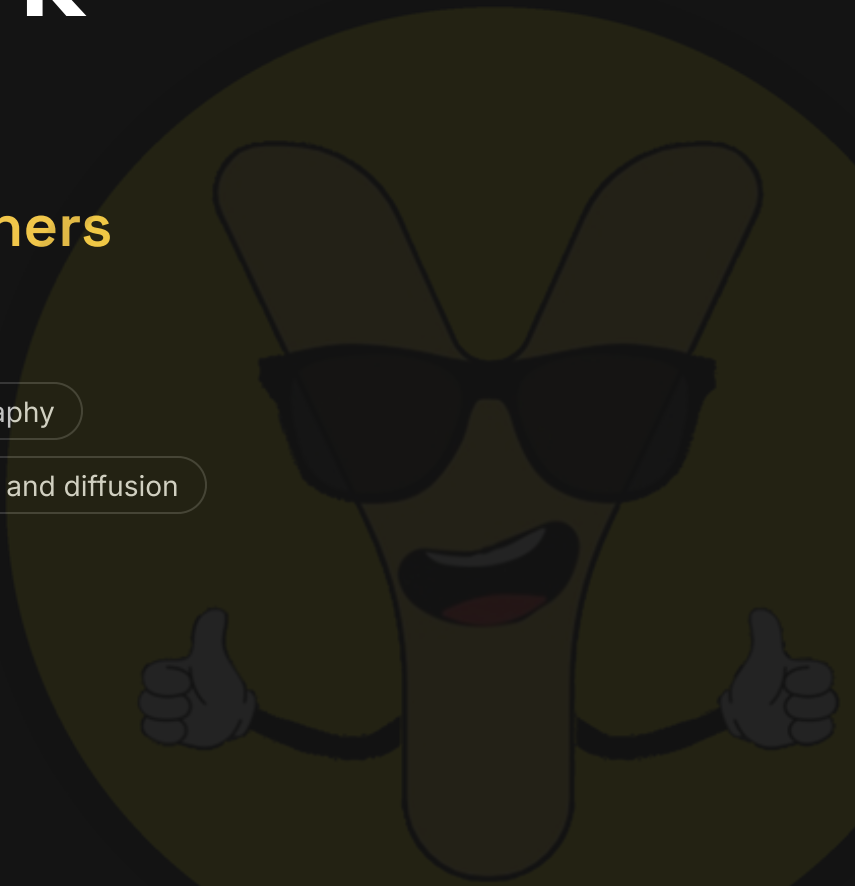
AKTU · 4TH YEAR · SEMESTER 7 · BCS072

Cryptography and Network Security

Unit 1 — Introduction and Classical/Modern Block Ciphers

- Introduction to security attacks, services and mechanism
- Classical encryption techniques- substitution ciphers and transposition ciphers
- Cryptanalysis
- Steganography
- Stream and block ciphers
- Modern Block Ciphers: Block ciphers principles
- Shannon's theory of confusion and diffusion
- Feistel structure
- Data encryption standard (DES)
- Strength of DES
- Idea of differential cryptanalysis



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Unit 1 Outline

Coverage of Introduction and Classical/Modern Block Ciphers as per syllabus.

- Security attacks, services, and mechanisms
- Classical encryption: substitution and transposition ciphers
- Cryptanalysis and Steganography
- Stream and block ciphers
- Modern Block Ciphers: Principles, Shannon theory, Feistel structure
- DES, strength, differential cryptanalysis, modes of operation, Triple DES

Security Attacks Overview

Attacks compromise the security of information owned by an organization.

- Passive Attacks
  - Eavesdropping or monitoring transmissions
  - Goal is to obtain information
  - Examples: Release of message contents, Traffic analysis
  - Difficult to detect; prevention is the key
- Active Attacks
  - Involve modification of data stream or creation of false stream
  - Examples: Masquerade, Replay, Modification of messages, Denial of Service (DoS)
  - Easy to detect; recovery is the key

Security Services and Mechanisms

Security services enhance the security of data processing systems.

- Security Services (ITU-T X.800)
  - Confidentiality: Protecting data from unauthorized disclosure
  - Authentication: Verifying identity
  - Integrity: Ensuring data has not been altered
  - Non-repudiation: Preventing denial of transmission
  - Access Control: Restricting resource access
- Security Mechanisms
  - Features designed to detect, prevent, or recover from a security attack
  - Examples: Encryption, Digital Signatures, Access Control Mechanisms, Notarization

Classical Encryption Techniques

SYMMETRIC CIPHER MODEL

A scheme where the sender and receiver share a single common secret key for both encryption and decryption.

- Plaintext: Original intelligible message X
- Encryption algorithm: Performs substitutions and transformations
- Secret Key: Input to encryption and decryption K
- Ciphertext: Randomized scrambled message $Y = E(K, X)$
- Decryption algorithm: Reverses encryption to recover plaintext $X = D(K, Y)$

Substitution Ciphers

Letters of plaintext are replaced by other letters, numbers, or symbols.

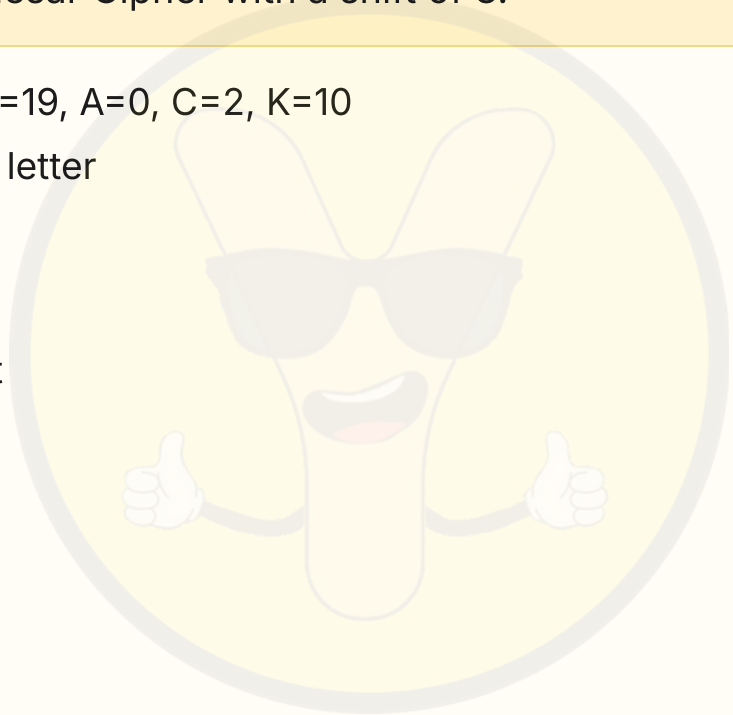
- Caesar Cipher
  - Replaces each letter by 3 positions down the alphabet
  - Mathematical formula: $C = (P + 3) \pmod{26}$
  - Decryption formula: $P = (C - 3) \pmod{26}$
  - Vulnerable to brute force due to only 25 possible keys
- Monoalphabetic and Polyalphabetic Ciphers
  - Monoalphabetic uses a fixed permutation of the alphabet (26! keys)
  - Polyalphabetic (e.g., Vigenère cipher) uses multiple substitution alphabets based on a keyword

Caesar Cipher Example

Encrypt the plaintext "ATTACK" using Caesar Cipher with a shift of 3.

1. Convert letters to numbers: A=0, T=19, T=19, A=0, C=2, K=10
2. Apply $C = (P + 3) \pmod{26}$ for each letter
3. A $\rightarrow (0 + 3) \pmod{26} = 3 = D$
4. T $\rightarrow (19 + 3) \pmod{26} = 22 = W$
5. Repeat for all letters to get the ciphertext

Ciphertext is "DWWDFN"



Transposition Ciphers

Plaintext letters are not replaced, but their positions are permuted or scrambled.

- Rail Fence Cipher
  - Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
  - Example: HELLO WORLD written in 2 rails gives H L O O D E L W R L
- Row Transposition Cipher
  - Plaintext is written in a matrix of specified rows/columns and read out by columns based on a key permutation
  - Hides letter frequencies completely unlike simple substitution

Substitution vs Transposition

Feature	Substitution Cipher	Transposition Cipher
Operation	Replaces characters with other characters	Rearranges the positions of characters
Letter Frequency	Preserves natural language frequency statistics	Flattens out letter frequency distribution
Example	Caesar Cipher, Vigenère Cipher	Rail Fence, Row Transposition
Vulnerability	Weak to frequency analysis	Weak to anagramming and pattern attacks

Cryptanalysis and Steganography

Distinction between deciphering encrypted text and hiding the existence of a message.

- Cryptanalysis
  - Art and science of breaking ciphertext without knowing the key
  - Ciphertext-only, Known-plaintext, Chosen-plaintext, and Chosen-ciphertext attacks
- Steganography
  - Hides the very existence of a message inside a cover medium (image, audio)
  - Drawback: High overhead, once detected, the message is compromised
  - Differs from cryptography which hides the meaning, not existence

Stream Ciphers vs Block Ciphers

Feature	Stream Cipher	Block Cipher
Processing Unit	Processes input one byte or bit at a time	Processes input in fixed blocks (e.g., 64-bit, 128-bit)
Memory Requirement	Low memory, fast execution	Requires buffering of entire block
Error Propagation	Errors usually affect only single bits	Errors can corrupt entire blocks depending on mode
Examples	RC4, ChaCha20	DES, AES, IDEA

Modern Block Ciphers & Shannon Theory

Foundational principles governing modern symmetric block cipher design.

- Block Cipher Principles
  - Based on Claude Shannon's concept of substitution and transposition (SPN)
  - Goal: Make statistical relationship between ciphertext and plaintext as complex as possible
- Confusion
  - Makes the relationship between ciphertext and the encryption key as complex as possible
  - Usually achieved via complex substitution boxes (S-boxes)
- Diffusion
  - Flattens statistical structure of plaintext across the ciphertext
  - Changing one plaintext bit changes many ciphertext bits; achieved via permutation (P-boxes)

Feistel Cipher Structure

FEISTEL NETWORK

A symmetric structure used in the construction of block ciphers, dividing the block into two halves processed iteratively.

- Proposed by Horst Feistel at IBM (basis for DES)
- Splits input block of length $2W$ into Left L_0 and Right R_0 halves
- Executes n rounds of identical operation
- Round function F takes subkey K_i and right half R_{i-1}
- Enables decryption to use the exact same algorithm as encryption by reversing subkeys

Feistel Cipher Round Structure



Single round of a Feistel cipher showing splitting, function F application, and swapping.

Data Encryption Standard (DES)

The most influential block cipher standard, published by NIST in 1977.

- Block size: 64 bits; Key length: 56 bits (effective) + 8 parity bits = 64 bits
- Structure: 16 rounds of Feistel network
- Initial Permutation (IP) splits data block at the start and Inverse IP at the end
- Round Function F: Expands 32-bit R to 48 bits, XORs with 48-bit subkey
- Passes through 8 substitution boxes (S-boxes) reducing to 32 bits, then Permutation P

Strength of DES and Cryptanalysis

Evaluating the security limits and vulnerabilities of DES.

- Key Size Vulnerability
  - 56-bit key space means 2^{56} possible keys
  - Easily vulnerable to brute-force attack today (tested by EFF Deep Crack in 1998 in 56 hours)
- Design Criteria Security
  - S-boxes and design rules were kept classified by NSA
  - Resistant to brute force when built, but key size is too small for modern standards
- Differential Cryptanalysis
  - Chosen-plaintext attack analyzing XOR differences of plaintext pairs
  - Exploits structural weaknesses in S-boxes; DES was surprisingly resistant to this

Block Cipher Modes of Operation

Techniques for applying a block cipher to securely encrypt data larger than block size.

- Electronic Codebook (ECB)
  - Each block encrypted independently; identical plaintexts produce identical ciphertexts (insecure for patterns)
- Cipher Block Chaining (CBC)
  - Previous ciphertext XORed with current plaintext before encryption; uses Initialization Vector (IV)
- Cipher Feedback (CFB) & Output Feedback (OFB)
  - CFB turns block cipher into a stream cipher; OFB generates keystream independent of message stream
- Counter (CTR) Mode
  - Encrypts successive values of a counter to generate keystream; allows high parallelism

Triple DES (3DES)

An enhancement of DES designed to extend its life without changing the core algorithm.

- Working Principle
  - Applies DES algorithm three times to each data block
- Two-Key Triple DES
  - Encrypt with K_1, Decrypt with K_2, Encrypt with K_1
  - Effective key length of 112 bits
- Three-Key Triple DES
  - Encrypt with K_1, Decrypt with K_2, Encrypt with K_3
  - Effective key length of 168 bits; used in financial systems
- Drawback
  - Relatively slow in software compared to modern AES due to triple processing overhead

Exam Corner

- **Q1** Differentiate between active and passive security attacks with suitable examples.
- **Q2** Explain the working principle of Caesar Cipher and find the ciphertext for "EXAM" with a shift of 4.
- **Q3** Explain Shannon's concepts of Confusion and Diffusion in block cipher design.
- **Q4** Draw the general Feistel cipher encryption structure and explain its components.
- **Q5** Describe the DES round function F(R, K) with a neat block diagram.
- **Q6** What is differential cryptanalysis? How does it apply to block ciphers?
- **Q7** Compare ECB and CBC modes of operation with advantages and disadvantages.
- **Q8** Why was Triple DES introduced? Explain 3-key Triple DES encryption and decryption.

Unit 1 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 2 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

