CRYPTOGRAPHY AND NETWORK SECURITY

Full Notes – Clear, Descriptive and Exam-Oriented

Basic Encryption Model

B.Tech / AKTU

Security Attacks • Security Services • Classical Ciphers • Cryptanalysis
Steganography • Stream and Block Ciphers • Shannon Theory • Feistel • DES
Differential Cryptanalysis • Block Cipher Modes • Triple DES

Presented by Dr. Aadarsh Malviya

Dronacharya Group of Institutions, Greater Noida

Contents

1. Introduction to Cryptography

Cryptography is the science of protecting information from unauthorized access. It changes readable information into an unreadable form and allows an authorized receiver to recover the original information.

Plaintext is the original readable message. Ciphertext is the transformed message produced by encryption. A key controls how the encryption and decryption operations are performed.

Basic Encryption Model

Basic equations

$$C = E(K, P)$$

$$P = D(K, C)$$

Symbol	Meaning
P	Plaintext
C	Ciphertext
K	Cryptographic key
E	Encryption algorithm
D	Decryption algorithm

Symmetric cryptography: the same secret key, or closely related secret keys, are used for encryption and decryption. DES and 3DES are examples discussed in these notes.

2. Security Attacks

A security attack is an action that attempts to break one or more security properties such as confidentiality, integrity, authentication or availability.

2.1 Passive Attacks

In a passive attack, the attacker observes communication but does not normally change the transmitted information. The main goal is to learn useful information without being detected.

- Release of message contents – the attacker reads confidential information.
- Traffic analysis – the attacker studies message size, timing, frequency or communication patterns, even when the message is encrypted.

Security Attack

Observes communication

2.2 Active Attacks

In an active attack, the attacker changes the communication or interferes with normal operation. Active attacks can affect integrity, authentication or availability.

- Masquerade – an attacker pretends to be an authorized user or system.
- Replay – a valid message is captured and transmitted again later.
- Modification of messages – the attacker changes the contents of a message.
- Denial of Service (DoS) – the attacker prevents legitimate users from obtaining a service.

Security Attack

Modifies, injects, replays or disrupts

Passive and Active Attacks – Comparison

Feature	Passive Attack	Active Attack
Main objective	Obtain information	Modify or disrupt
Data modification	No	Yes
Typical examples	Release of contents, traffic analysis	Replay, masquerade, modification, DoS
Detection	Often difficult	May be easier to detect

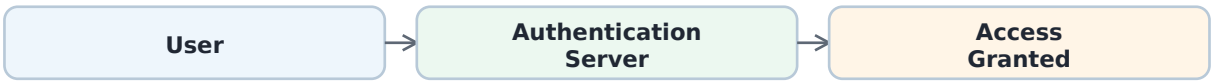
3. Security Services

A security service is a service provided by a system to protect information and communication against security attacks.

3.1 Authentication

Authentication verifies the identity of a user, device or system. In simple words, it answers the question: Who is communicating?

Authentication and Access Control



3.2 Access Control

Access control ensures that only authorized users or systems can use a protected resource. Permissions may specify who can read, write, execute or modify a resource.

3.3 Data Confidentiality

Confidentiality protects information from unauthorized disclosure. Encryption is a major mechanism used to provide confidentiality.

3.4 Data Integrity

Integrity means that data has not been changed, deleted or inserted in an unauthorized manner.

3.5 Non-Repudiation

Non-repudiation provides evidence of an action or communication so that a party cannot easily deny having performed that action. Digital signatures are commonly used for this purpose.

4. Security Mechanisms

A security mechanism is a technique or process used to implement a security service. A single mechanism may contribute to more than one security objective.

- Encryption – protects confidentiality by transforming plaintext into ciphertext.
- Digital signatures – support authentication, integrity and non-repudiation.
- Authentication exchange – verifies the identity of communicating parties.
- Access control – restricts use of resources to authorized users.
- Data integrity mechanisms – help detect unauthorized changes.
- Traffic padding – adds additional traffic to make traffic analysis more difficult.
- Routing control – selects communication paths according to security requirements.
- Notarization – uses a trusted third party to provide evidence about an action or transaction.

Security problem	Security service	Typical mechanism
Unauthorized reading	Confidentiality	Encryption
False identity	Authentication	Authentication exchange
Unauthorized modification	Integrity	Integrity mechanism
Denial of responsibility	Non-repudiation	Digital signature

5. Classical Encryption Techniques

Classical encryption techniques are traditional methods used to hide information. Two important categories are substitution and transposition.

6. Substitution Ciphers

In a substitution cipher, a plaintext symbol is replaced by another symbol according to a defined rule. The order of symbols is generally preserved, but the symbols themselves are changed.

6.1 Caesar Cipher

The Caesar cipher shifts every alphabetic character by a fixed number of positions. For example, with a shift of 3, A becomes D, B becomes E, and so on.

$$C = (P + K) \bmod 26$$

Example: HELLO with a shift of 3 becomes KHOOR.

6.2 Monoalphabetic Substitution Cipher

Each plaintext letter is mapped to one fixed ciphertext letter. The same substitution is used throughout the message. Because normal languages have recognizable letter frequencies, frequency analysis can often be used against this cipher.

6.3 Playfair Cipher

The Playfair cipher encrypts two letters at a time using a 5 × 5 matrix. Usually I and J share one cell. The key is used to construct the matrix.

Playfair Key Matrix				
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Playfair rules: If both letters are in the same row, use the letters to their right. If both are in the same column, use the letters below them. Otherwise, form a rectangle and use the letters at the opposite corners in the same rows.

6.4 Hill Cipher

The Hill cipher is a polygraphic substitution cipher based on matrix multiplication. Plaintext letters are converted into numbers, grouped into vectors and multiplied by a key matrix.

$$C = K \times P \bmod 26$$

$$P = K^{-1} \times C \bmod 26$$

The key matrix must have a modular inverse modulo 26; otherwise decryption cannot be performed using the same matrix method.

6.5 Vigenère Cipher

The Vigenère cipher uses a keyword. Each key character gives a different Caesar shift, so the same plaintext letter can be encrypted in different ways at different positions.

$$C_i = (P_i + K_i) \bmod 26$$

Example: ATTACKATDAWN with a repeated key such as LEMON uses a different shift according to the corresponding key letter.

7. Transposition Ciphers

In a transposition cipher, the letters are not replaced. Instead, their positions are rearranged according to a rule.

7.1 Rail Fence Cipher

The plaintext is written in a zig-zag pattern across a specified number of rails. The ciphertext is then obtained by reading the rails from top to bottom.

Rail 1	H				L				O
Rail 2		E		L		W		R	
Rail 3			L				O		

7.2 Columnar Transposition Cipher

The plaintext is written into rows beneath a keyword. The columns are then read in the order determined by the alphabetical order of the keyword letters.

Substitution vs Transposition

Substitution	Transposition
Characters are replaced.	Characters are rearranged.
The symbols themselves change.	The symbols remain the same.
Examples: Caesar, Playfair, Hill, Vigenère.	Examples: Rail Fence, Columnar Transposition.

8. Cryptanalysis

Cryptanalysis is the study of methods used to analyze a cryptographic system and recover plaintext, key information or other useful information without having authorized knowledge of the secret key.

The purpose of cryptanalysis is to understand how much information an attacker can obtain from the available data and weaknesses of a cryptographic system.

8.1 Major Cryptanalytic Attacks

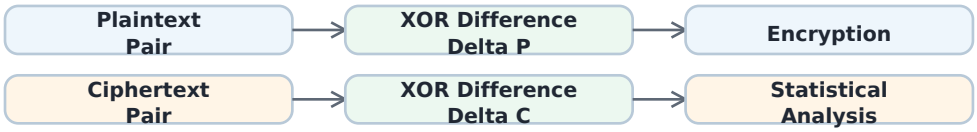
- Ciphertext-only attack: the attacker has only ciphertext and tries to discover the plaintext or key.
- Known-plaintext attack: the attacker knows some plaintext and its corresponding ciphertext.
- Chosen-plaintext attack: the attacker chooses plaintext messages and obtains their ciphertexts.
- Chosen-ciphertext attack: the attacker chooses ciphertexts and obtains the corresponding plaintexts.
- Brute-force attack: the attacker systematically tries possible keys until the correct key is found.

For a key of k bits, there can be up to 2^k possible key values. A larger key space generally makes exhaustive key search more difficult.

8.2 Differential Cryptanalysis – Basic Idea

Differential cryptanalysis studies how a difference between two plaintext inputs can lead to a difference between their ciphertext outputs. The attacker looks for statistical patterns in these differences.

Differential Cryptanalysis – Basic Idea



The important idea is to compare two related inputs rather than analyze only one message. In an XOR-based analysis, the differences are written as:

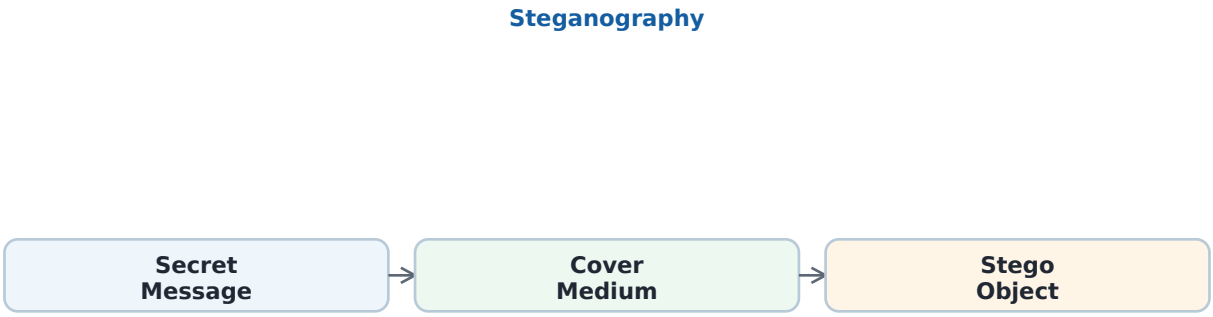
$$\Delta P = P_1 \text{ XOR } P_2$$

$$\Delta C = C_1 \text{ XOR } C_2$$

9. Steganography

Steganography is the technique of hiding secret information inside another apparently normal medium. The medium may be an image, audio file, video, text or another digital object.

The main goal is not merely to make the message unreadable, but to make the presence of the message less obvious.



Cryptography and Steganography

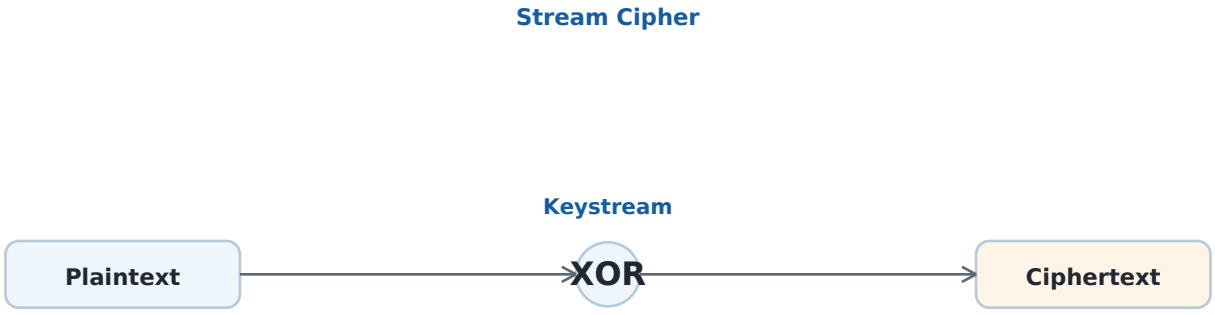
Cryptography	Steganography
Changes plaintext into ciphertext.	Hides information inside another medium.
The existence of ciphertext is usually visible.	The existence of the hidden information may be concealed.
Main goal: protect the meaning of information.	Main goal: conceal the presence of information.

10. Stream and Block Ciphers

Modern symmetric ciphers are commonly described as stream ciphers or block ciphers. The major difference is the way plaintext is processed.

10.1 Stream Cipher

A stream cipher processes data one bit or one byte at a time. It generates a sequence called a keystream. The plaintext is combined with the keystream, commonly using XOR.



$$C_i = P_i \text{ XOR } K_i$$

$$P_i = C_i \text{ XOR } K_i$$

Examples historically include RC4 and A5/1.

10.2 Block Cipher

A block cipher divides plaintext into fixed-size blocks and applies a block transformation to each block according to a key and a mode of operation. DES, 3DES and AES are examples of block ciphers.

Stream Cipher vs Block Cipher

Stream Cipher	Block Cipher
Processes bits or bytes.	Processes fixed-size blocks.
Uses a keystream.	Uses a block transformation.
Useful for continuous streams.	Useful for block-oriented data.
Example: RC4.	Examples: DES, 3DES, AES.

11. Principles of Modern Block Ciphers

A modern block cipher transforms a fixed-size plaintext block into a ciphertext block using a secret key. Instead of relying on one complicated operation, a cipher normally uses several rounds of simpler operations.

The repeated rounds are designed to make the relationship between plaintext, ciphertext and key difficult to analyze.

11.1 Product Cipher

A product cipher combines several basic transformations, particularly substitution and permutation. Repeating these transformations helps provide confusion and diffusion.

12. Shannon's Theory: Confusion and Diffusion

Claude Shannon described confusion and diffusion as important principles for designing secure cryptographic systems.

12.1 Confusion

Confusion makes the relationship between the secret key and the ciphertext complicated. Substitution operations and S-boxes are commonly used to provide confusion.

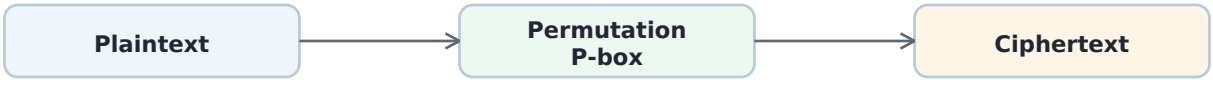
Shannon's Principle

Confusion: hide the relationship between key and ciphertext

12.2 Diffusion

Diffusion spreads the effect of one plaintext bit over many ciphertext bits. Permutation operations and repeated rounds help spread this influence.

Shannon's Principle



Diffusion: spread plaintext influence over many ciphertext bits

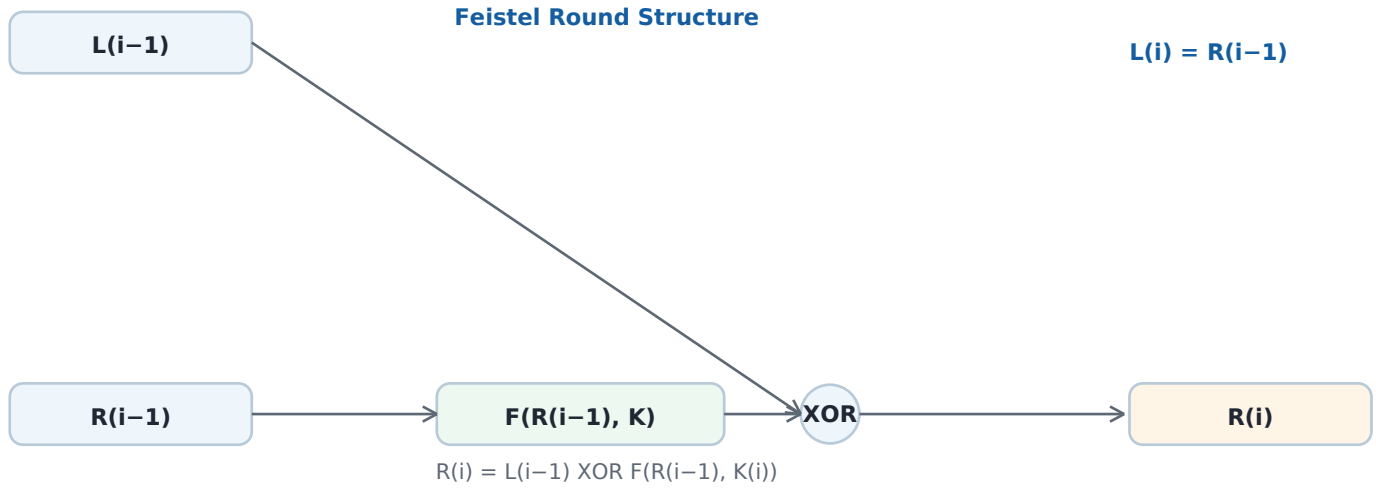
12.3 Avalanche Effect

The avalanche effect means that a small change in the plaintext or key should produce a large and apparently unpredictable change in the ciphertext.

Concept	Main purpose	Typical mechanism
Confusion	Make the key–ciphertext relationship complex	Substitution / S-box
Diffusion	Spread plaintext influence	Permutation / P-box
Avalanche effect	Large ciphertext change from a small input change	Repeated rounds

13. Feistel Structure

A Feistel network divides a data block into two halves, normally called L and R. Each round uses one half as input to a round function and combines the result with the other half using XOR.



Round equations

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \text{ XOR } F(R_{i-1}, K_i)$$

One important advantage of the Feistel structure is that encryption and decryption can use the same basic architecture. For decryption, the round keys are applied in reverse order.

14. Data Encryption Standard (DES)

DES is a symmetric block cipher that was standardized in 1977. It operates on a 64-bit data block and uses a 64-bit key input, of which 56 bits are effective key bits because 8 bits are used for parity.

DES uses a 16-round Feistel structure. Each round applies the DES round function to the right half and combines the result with the left half.

14.1 DES Overall Structure

DES Encryption Structure

14.2 Initial Permutation

The 64-bit plaintext first passes through a fixed Initial Permutation (IP). This operation rearranges the input bits and produces two 32-bit halves for the Feistel rounds.

14.3 DES Round Function

The right half is expanded from 32 bits to 48 bits, combined with a 48-bit round key, passed through eight S-boxes and then through a P-box. The resulting 32 bits are XORed with the left half.

DES Round Function F

14.4 DES F Function – Step by Step

Step	Operation	Explanation
1	Expansion	The 32-bit right half is expanded to 48 bits.
2	Key mixing	The expanded 48 bits are XORed with the 48-bit round key.
3	S-box substitution	Eight S-boxes convert 48 input bits into 32 output bits.
4	P-box permutation	The 32 bits are rearranged using the P-box.

14.5 DES S-Boxes

DES has eight S-boxes. Each S-box receives 6 bits and produces 4 bits. Therefore, $8 \times 6 = 48$ input bits become $8 \times 4 = 32$ output bits.

The S-boxes provide nonlinear substitution and are a major source of confusion in DES.

14.6 DES Key Schedule

The 64-bit DES key contains 8 parity bits, leaving 56 effective key bits. These bits are divided into two 28-bit halves. Shifts and selection operations are then used to produce sixteen 48-bit round keys.

Key flow: 64-bit key → 56 effective bits → two 28-bit halves → round shifts → sixteen 48-bit round keys.

14.7 DES Decryption

DES decryption uses the same Feistel structure as encryption. The main difference is the order of the round keys: K16, K15, …, K2, K1.

15. Strength of DES

DES has an effective key size of 56 bits. Therefore, the theoretical number of possible keys is 2^{56}.

When DES was introduced, this key size provided substantial protection. With modern computing capabilities, however, a 56-bit key is too small for many security applications because exhaustive key search can be performed much more efficiently than was possible in the past.

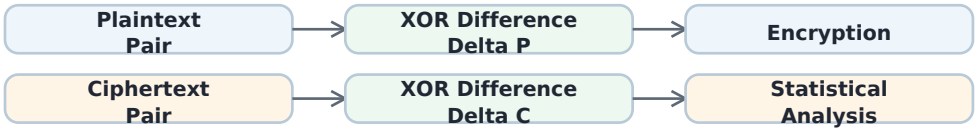
DES is therefore considered obsolete for modern secure applications.

Property	DES
Block size	64 bits
Key input	64 bits
Effective key size	56 bits
Number of Feistel rounds	16
Structure	Feistel network
Modern status	Obsolete for modern secure applications

16. Differential Cryptanalysis

Differential cryptanalysis studies the relationship between differences in pairs of plaintexts and the resulting differences in ciphertexts. Instead of studying one encryption operation in isolation, the attacker studies how a difference propagates through several rounds.

Differential Cryptanalysis – Basic Idea



Basic steps

- Select or observe two plaintext values and calculate their XOR difference.
- Encrypt both plaintexts using the same secret key.
- Calculate the XOR difference between the resulting ciphertexts.
- Study statistical patterns in the input and output differences.
- Use the observed patterns to obtain information about possible key values.

$$\Delta P = P_1 \text{ XOR } P_2$$

$$\Delta C = C_1 \text{ XOR } C_2$$

The attack is based on statistical properties of difference propagation through the cipher.

17. Block Cipher Modes of Operation

A block cipher by itself encrypts one fixed-size block. A message normally contains many blocks, so a mode of operation specifies how those blocks are processed and connected.

17.1 ECB – Electronic Codebook

In ECB mode, every plaintext block is encrypted independently using the same key.

$$C_i = E(K, P_i)$$

Important limitation: identical plaintext blocks produce identical ciphertext blocks. This can reveal patterns in structured data.

17.2 CBC – Cipher Block Chaining

CBC combines each plaintext block with the previous ciphertext block before encryption. The first block uses an Initialization Vector (IV).

$$C_1 = E(K, P_1 \text{ XOR } IV)$$

$$C_i = E(K, P_i \text{ XOR } C_{i-1})$$

17.3 CFB – Cipher Feedback

CFB uses the encryption function of the block cipher to produce a stream-like output. Ciphertext is fed back into the process for the next step.

17.4 OFB – Output Feedback

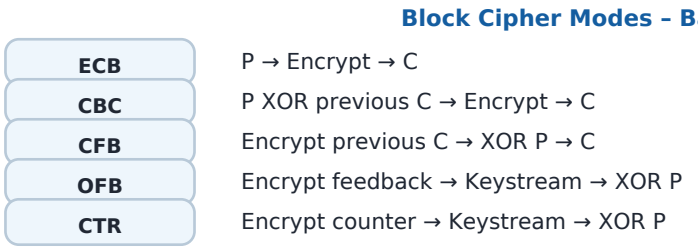
OFB repeatedly encrypts its previous output to generate a keystream. The plaintext is combined with this keystream.

17.5 CTR – Counter Mode

CTR encrypts successive counter values and uses the results as a keystream. The keystream is XORed with plaintext blocks.

$$C_i = P_i \text{ XOR } E(K, \text{Counter}_i)$$

The counter/nonce must not be reused with the same key.



Comparison of Modes

Mode	Main idea	Parallel processing	Important point
ECB	Independent encryption of each block	Yes	Patterns may be visible
CBC	Each block depends on previous ciphertext	Encryption: No	Uses an IV
CFB	Cipher feedback creates stream-like operation	Limited	Uses previous ciphertext
OFB	Feedback generates a keystream	Limited	Keystream is independent of plaintext
CTR	Counter values are encrypted to create a keystream	Yes	Counter/nonce must be unique

18. Triple DES (3DES)

Triple DES applies the DES operation three times to provide more security than single DES. A commonly described arrangement is EDE: Encrypt, Decrypt, Encrypt.

Triple DES – EDE Structure

18.1 EDE Formula

$$C = E(K_3, D(K_2, E(K_1, P)))$$

18.2 Two-Key 3DES

In two-key 3DES, two independent keys are used in the sequence K_1, K_2, K_1.

$$C = E(K_1, D(K_2, E(K_1, P)))$$

18.3 Three-Key 3DES

In three-key 3DES, K_1, K_2 and K_3 are independent keys. The nominal key material is 168 bits. Its effective security is lower than a simple interpretation of 168-bit brute-force security because of cryptanalytic techniques such as meet-in-the-middle.

18.4 Why EDE?

The EDE arrangement supports compatibility with DES. If $K_1 = K_2 = K_3$, the sequence reduces to ordinary DES encryption.

18.5 DES and 3DES

Feature	DES	3DES
Block size	64 bits	64 bits
DES operations	1	3
Effective/key material	56 effective bits	Two-key or three-key variants
Speed	Faster	Slower because DES is applied three times
Security status	Obsolete	Legacy/deprecated for many new systems

19. Important Definitions, Formulae and Revision Questions

19.1 Important Definitions

Term	Simple definition
Cryptography	The science of protecting information using cryptographic techniques.
Cryptanalysis	The study of methods for analyzing cryptographic systems and recovering information.
Plaintext	The original readable message.
Ciphertext	The transformed or encrypted message.
Encryption	The process of converting plaintext into ciphertext.
Decryption	The process of converting ciphertext back into plaintext.
Key	A value that controls a cryptographic operation.
Block cipher	A cipher that processes fixed-size blocks.
Stream cipher	A cipher that processes data as a stream of bits or bytes.
Confusion	A principle that makes the key–ciphertext relationship complex.
Diffusion	A principle that spreads plaintext influence over many ciphertext bits.
Steganography	The technique of hiding information inside another medium.

19.2 Important Formulae

Topic	Formula
Caesar	$C = (P + K) \bmod 26$
Vigenère	$C_i = (P_i + K_i) \bmod 26$
Hill	$C = K \times P \bmod 26$
Feistel	$L_i = R_{i-1}$; $R_i = L_{i-1}$ XOR $F(R_{i-1}, K_i)$
Stream cipher	$C_i = P_i$ XOR K_i
CBC	$C_1 = E(K, P_1$ XOR $IV)$
CTR	$C_i = P_i$ XOR $E(K, Counter_i)$
3DES	$C = E(K_3, D(K_2, E(K_1, P)))$

19.3 Important Examination Questions

1. Explain passive and active security attacks with suitable diagrams.
2. Explain authentication, access control, confidentiality, integrity and non-repudiation.

3. Explain security mechanisms with examples.
4. Explain substitution and transposition ciphers.
5. Explain Caesar, Playfair, Hill and Vigenère ciphers.
6. Explain cryptanalysis and its major attack types.
7. Explain steganography and compare it with cryptography.
8. Differentiate stream ciphers and block ciphers.
9. Explain the principles of modern block ciphers.
10. Explain Shannon's theory of confusion and diffusion.
11. Explain the avalanche effect.
12. Explain the Feistel structure with equations and a diagram.
13. Explain the complete structure of DES.
14. Explain the DES F function and S-boxes.
15. Explain the DES key schedule.
16. Discuss the strength and limitations of DES.
17. Explain the basic idea of differential cryptanalysis.
18. Explain ECB, CBC, CFB, OFB and CTR modes.
19. Explain Triple DES and the EDE sequence.
20. Compare DES and 3DES.

Quick Revision – One Page Summary

Security attacks: Passive attacks observe; active attacks modify or disrupt.

Security services: Authentication, access control, confidentiality, integrity and non-repudiation.

Classical ciphers: Substitution changes symbols; transposition changes positions.

Cryptanalysis: Attempts to obtain plaintext, key information or other useful information by analyzing the cryptosystem.

Steganography: Hides the existence of information inside another medium.

Stream cipher: Processes a stream of bits/bytes using a keystream.

Block cipher: Processes fixed-size blocks.

Confusion: Complicates the key–ciphertext relationship.

Diffusion: Spreads plaintext influence across many ciphertext bits.

Feistel: Divides a block into L and R and processes repeated rounds.

DES: 64-bit block, 56 effective key bits, 16 Feistel rounds.

Differential cryptanalysis: Studies differences between pairs of inputs and outputs.

Modes: ECB, CBC, CFB, OFB and CTR define how block ciphers process multiple blocks.

3DES: Applies DES three times, commonly in EDE form.

Exam writing tip: Begin with the definition, explain the working step by step, write the important formula, draw the diagram, and finish with advantages/limitations or a comparison where applicable.