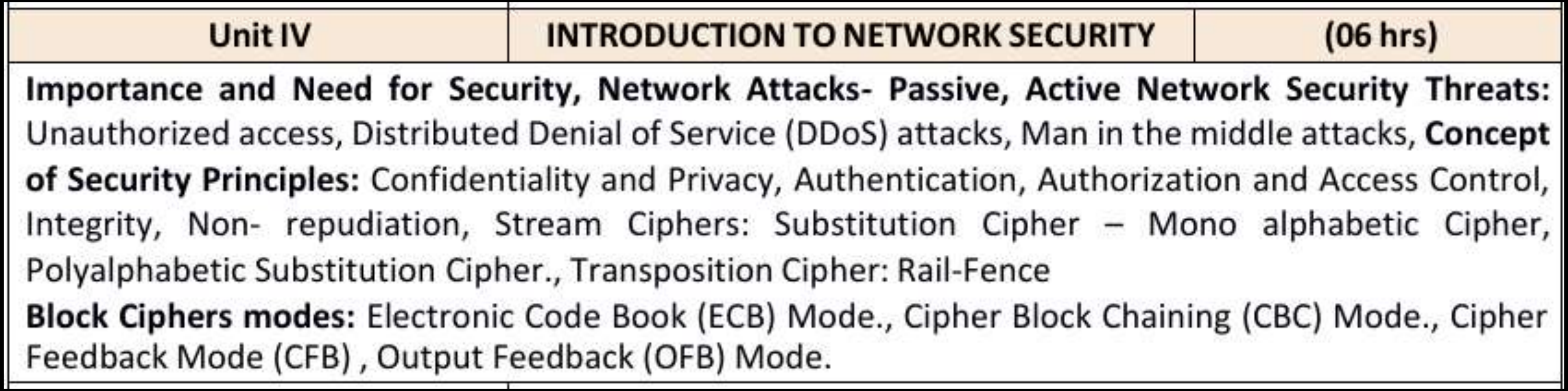
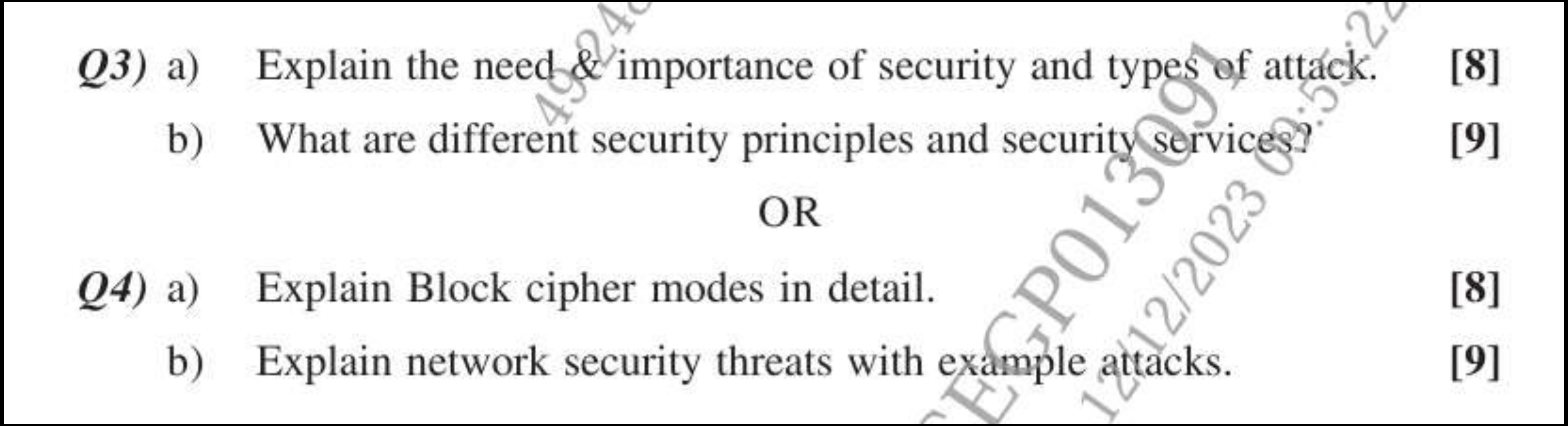
full one-shot videos on :**JK Coding Pathshala YouTube channel**

JK Coding Pathshala

https://youtube.com/@jayeshkande9215?feature=shared



Unit IV	INTRODUCTION TO NETWORK SECURITY	(06 hrs)
Importance and Need for Security, Network Attacks- Passive, Active Network Security Threats: Unauthorized access, Distributed Denial of Service (DDoS) attacks, Man in the middle attacks, **Concept of Security Principles:** Confidentiality and Privacy, Authentication, Authorization and Access Control, Integrity, Non- repudiation, Stream Ciphers: Substitution Cipher – Mono alphabetic Cipher, Polyalphabetic Substitution Cipher., Transposition Cipher: Rail-Fence **Block Ciphers modes:** Electronic Code Book (ECB) Mode., Cipher Block Chaining (CBC) Mode., Cipher Feedback Mode (CFB) , Output Feedback (OFB) Mode.		



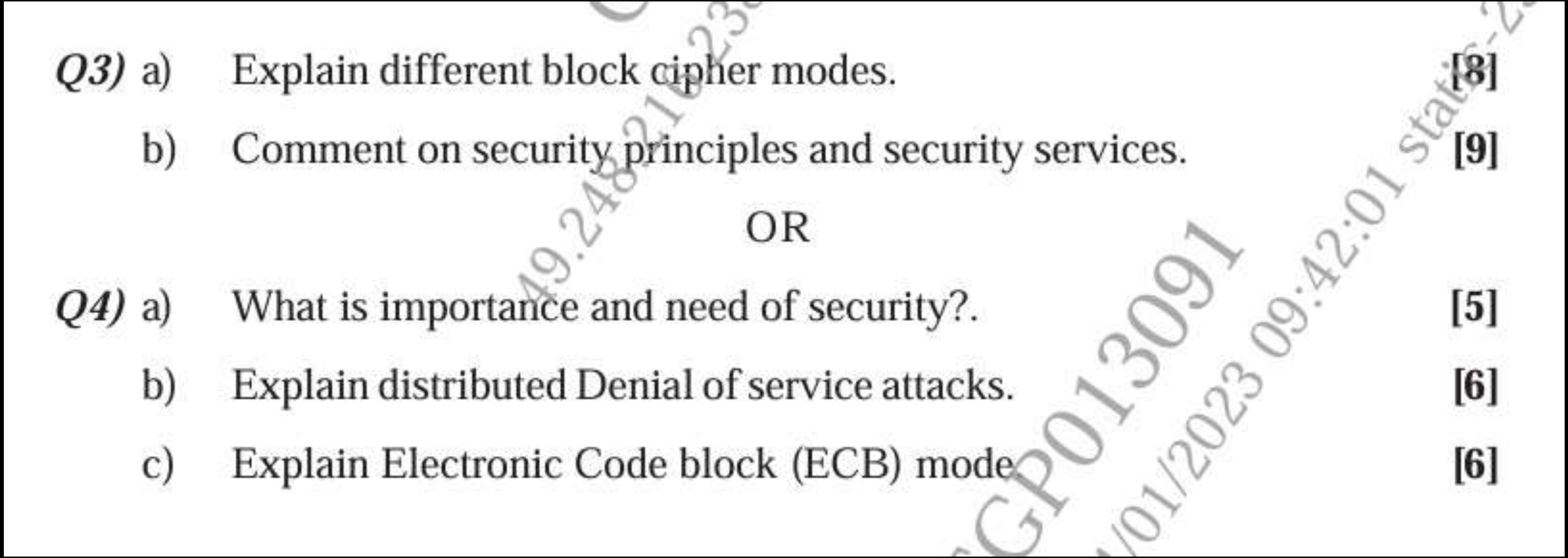
Q3) a) Explain the need & importance of security and types of attack. **[8]**

b) What are different security principles and security services? **[9]**

OR

Q4) a) Explain Block cipher modes in detail. **[8]**

b) Explain network security threats with example attacks. **[9]**



Q3) a) Explain different block cipher modes. **[8]**

b) Comment on security principles and security services. **[9]**

OR

Q4) a) What is importance and need of security?. **[5]**

b) Explain distributed Denial of service attacks. **[6]**

c) Explain Electronic Code block (ECB) mode. **[6]**

Q3) a) What is network attack? Write short note on following with suitable example? **[8]**

i) Active attack

ii) Passive attack

b) What is Cipher Feedback Mode (CFM)? Explain the process of CFM with suitable diagram. **[9]**

OR

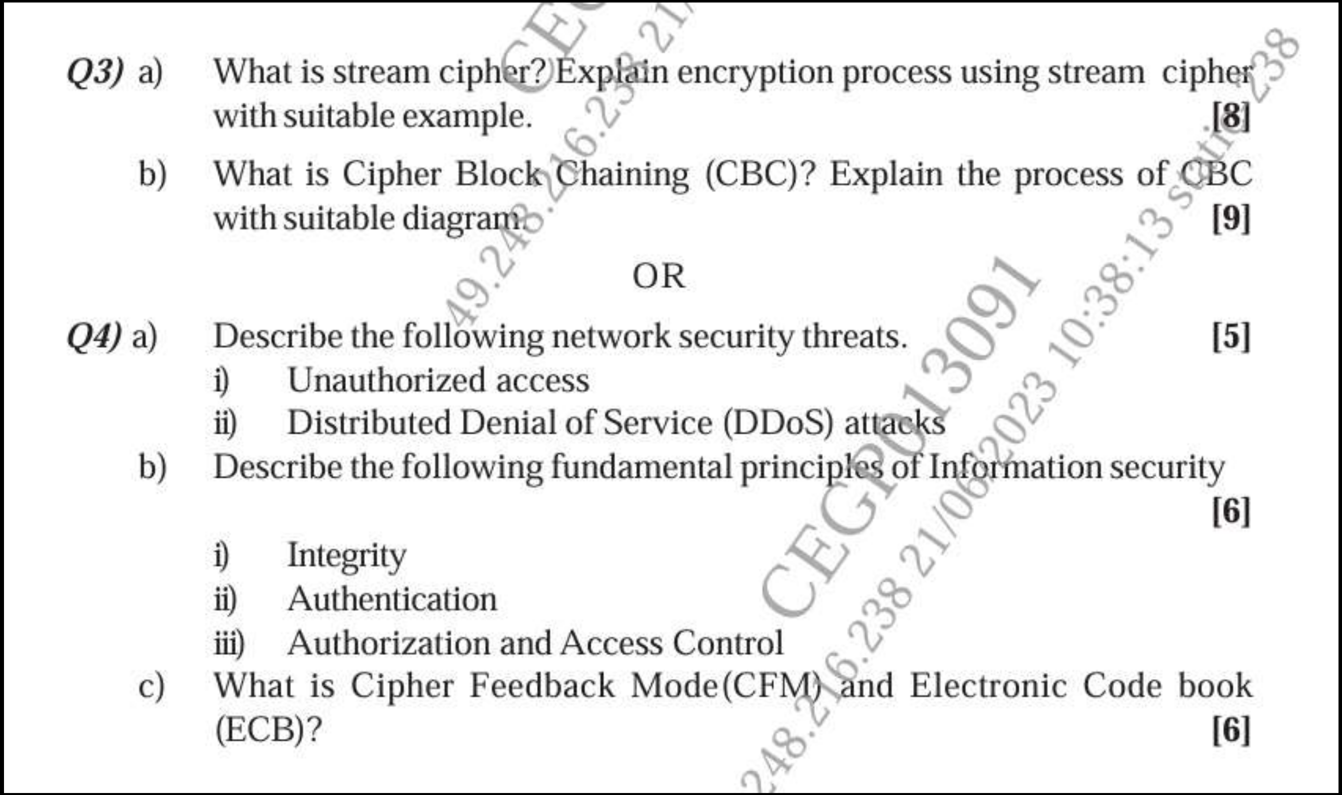
Q4) a) What is Electronic Code Book (ECB)? Explain the process of ECB with suitable diagram. **[5]**

b) Describe the following network security threats **[6]**

i) Unauthorized access

ii) Distributed Denial of Service (DDoS) attacks

c) Differentiate between Active attack and Passive attack **[6]**



Q3) a) What is stream cipher? Explain encryption process using stream cipher with suitable example. **[8]**

b) What is Cipher Block Chaining (CBC)? Explain the process of CBC with suitable diagram. **[9]**

OR

Q4) a) Describe the following network security threats. **[5]**

i) Unauthorized access

ii) Distributed Denial of Service (DDoS) attacks

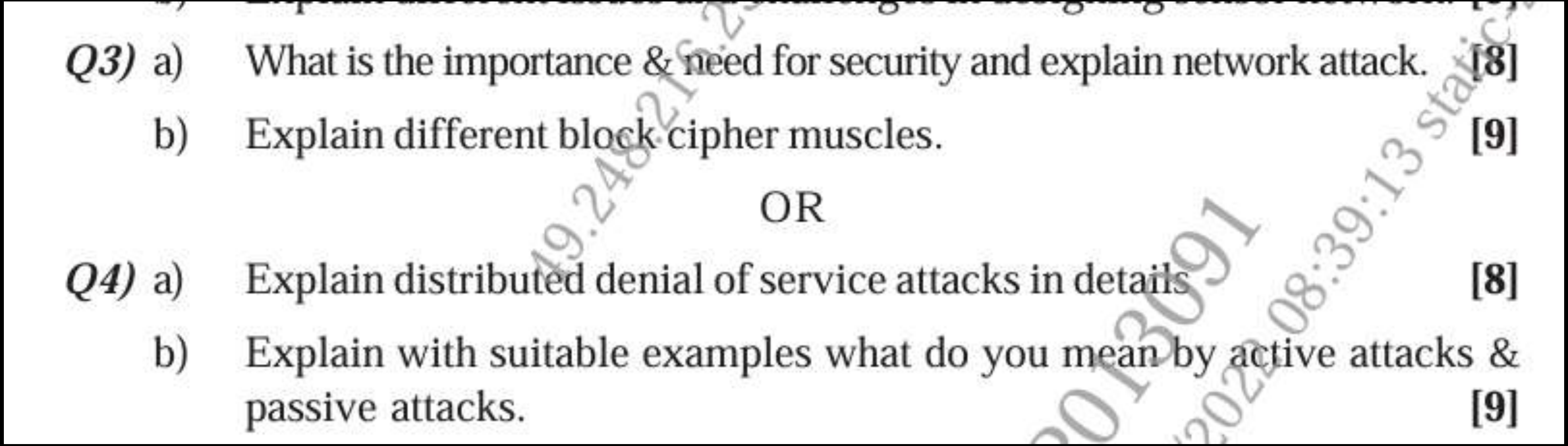
b) Describe the following fundamental principles of Information security **[6]**

i) Integrity

ii) Authentication

iii) Authorization and Access Control

c) What is Cipher Feedback Mode(CFM) and Electronic Code book (ECB)? **[6]**



Q3) a) What is the importance & need for security and explain network attack. [8]

b) Explain different block cipher muscles. [9]

OR

Q4) a) Explain distributed denial of service attacks in details [8]

b) Explain with suitable examples what do you mean by active attacks & passive attacks. [9]

🔐 Importance and Need for Security

1. Data Protection (Data ki Raksha)

Aaj ke digital zamaane mein har kisi ka personal data — jaise bank details, Aadhaar number, passwords — online hota hai. Agar security nahi hogi, toh hackers aasani se is data ko chura sakte hain.

□ **Real-life Example**:
Socho tumne ek online shopping website par apna debit card detail diya aur wo website secure nahi thi. Ek hacker ne us website ko hack kar liya aur tumhara card detail use karke paise nikaal liye.

☞ **Conclusion**: Isiliye data ko encrypt karna, passwords secure rakhna, aur secure platforms use karna zaroori hai.

2. Unauthorized Access se Protection

Security ensure karti hai ki sirf authorized log hi kisi system ya data tak pahunch sakein.

□ **Real-life Example**:

Tumhare college ka online portal hai jisme tumhare marks, attendance, aur fees ka data hota hai. Agar koi unauthorized student us portal ko access kare aur tumhare marks badal de — toh kya hoga?

☞ **Conclusion**: Isiliye user authentication (jaise login + password) kaafi important hai.

3. Business Reputation (Reputation ki Suraksha)

Agar kisi company ka data leak ho jata hai, toh unki reputation kharab ho sakti hai. Customers ka trust chala jata hai.

□ **Real-life Example**:

Facebook ka data leak scandal ya kisi bank ka cyber attack — jiske baad log un services se door ho jaate hain.

☞ **Conclusion**: Company ko apna aur apne users ka data secure rakhna chahiye to maintain trust.

4. National Security (Desh ki Suraksha)

Government systems jaise military, intelligence agencies ke data ka secure hona bahut zaroori hai. Agar ye data dusri countries ke haath lag jaye, toh national security khatre mein pad sakti hai.

□ **Real-life Example**:
Cyber attacks on defense websites ya confidential government documents ka leak ho jana.

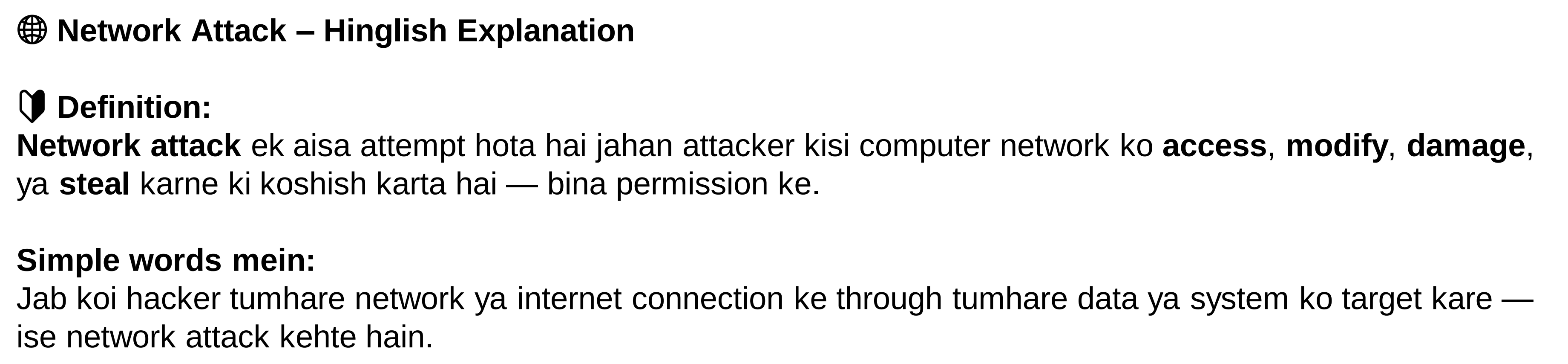
☞ **Conclusion**: National level par bhi cyber security ek badi zarurat hai.

5. Financial Security

Online banking, UPI, wallets — sab digital ho gaya hai. Agar security na ho, toh logon ke crores ka nuksaan ho sakta hai.

□ **Real-life Example**:
Kisi ka UPI PIN leak ho gaya aur uske bank account se saare paise nikal gaye.

☞ **Conclusion**: OTP, PIN, encryption jaise measures isliye use kiye jaate hain.



🌐 Network Attack – Hinglish Explanation

🔰 Definition:

Network attack ek aisa attempt hota hai jahan attacker kisi computer network ko **access**, **modify**, **damage**, ya **steal** karne ki koshish karta hai — bina permission ke.

Simple words mein:

Jab koi hacker tumhare network ya internet connection ke through tumhare data ya system ko target kare — ise network attack kehte hain.

🔍 1. Passive Attack (Chupke se Sunna ya Dekhna)

Definition:
Passive attack wo hota hai jisme attacker sirf **monitor karta hai data** ko bina kisi change kiye.
Ye attack secretly hota hai — system ya data ko **damage nahi karta**, bas uska **observation** karta hai.

□ **Real-life Example:**

Socho tum ek public Wi-Fi (jaise airport ya café) use kar rahe ho. Ek hacker bhi us Wi-Fi se connected hai.
Wo hacker ek tool use karta hai jaise **packet sniffer** aur tumhare data packets ko **chupke se read karta hai** — jaise tumhara email content, login credentials, ya OTPs.

⚠□ **Impact**: Tumhe pata bhi nahi chalta, lekin tumhara confidential data chori ho chuka hota hai.

□ **Common Passive Attack Types:**

- Eavesdropping (Jasoosi)
- Traffic analysis

☞ **Summary**:
Passive attack = **Observe/Sniff** karta hai data without changing it.
"Chupke se dekhna, bina ched-chaad ke."

✹ 2. Active Attack (Data me Chhed-Chhad karna)

Definition:
Active attack me attacker **data ko modify karta hai**, **fake data inject karta hai**, ya **network service ko disrupt karta hai**.
Ye attack visible hota hai, aur system ya user ko **nuksaan pahuchata hai**.

□ Real-life Example:

Socho tumhare friend ne tumse ₹500 maange aur tumne UPI se bhejne wale ho.
Ek attacker ne tumhare device aur bank server ke beech ka connection hack kar liya.
Wo transaction ke data ko modify kar deta hai — ₹500 ki jagah ₹5000 bhej diye jaate hain.

⚠□ **Impact**: Tum sochte ho ₹500 gaye, lekin ₹5000 nikal gaye!

□ Common Active Attack Types:

- **Man-in-the-middle attack** (beech me ghus kar data badalna)
- **Denial of Service (DoS)** (server ko crash kar dena)
- **Session hijacking** (user ke login session ko hack kar lena)
- **Message modification** (data ko alter kar dena)

☞ **Summary**:
Active attack = **Modify, Inject, Disrupt**
"Khule aam tod-phod karna ya data ka misuse karna."

🔢 **Point**	● **Active Attack**	⊜ **Passive Attack**
1️⃣ **Kya karta hai?**	Data ko **modify, delete, inject** karta hai	Sirf **monitor ya observe** karta hai
2️⃣ **Intent (Uddeshya)**	**Damage**, disrupt ya misuse karna	Secretly **gather information**
3️⃣ **System par asar**	System/service ko **nuksaan** pahuchata hai	System par **koi effect nahi**, bas spying karta hai
4️⃣ **Detection**	Asaani se **detect** ho jata hai	**Detect karna mushkil** hota hai
5️⃣ **Example**	Man-in-the-middle, DoS, Session Hijack	Eavesdropping, Packet Sniffing
6️⃣ **Real-life analogy**	Bank ke transaction ko change kar dena	Deewar ke peeche se kisi ki baat sun lena
7️⃣ **Network Traffic**	**Alter karta hai** traffic ko	Sirf **observe karta hai** traffic ko
8️⃣ **Security Impact**	High – **confidentiality, integrity, availability** risk	Moderate – **confidentiality** risk only

🔐 SECURITY THREATS

1️⃣ Unauthorized Access (Bina Permission ke Access)

📌 **Definition:**
Jab koi person ya program bina proper **authorization** ke kisi system, network, ya data ko access karta hai — ise unauthorized access kehte hain.

□ **Real-Life Example:**
Socho tumhare college ka result portal hai jisme sirf teachers login kar sakte hain. Agar koi student teacher ka username-password guess karke login kare aur marks change kar de — ye unauthorized access hoga.

🔒 **Impact:**
- Confidential data leak ho sakta hai
- System integrity kharab ho sakti hai
- Personal ya financial information misuse ho sakti hai

□ **Prevention:**
- Strong passwords
- Two-Factor Authentication (2FA)
- Role-based access control

2️⃣ DDoS Attack (Distributed Denial of Service)

📌 **Definition:**

DDoS attack mein attacker kai devices (botnets) ka use karke kisi website ya server par itna zyada traffic bhejta hai ki wo **crash ya slow** ho jaye.

□ **Real-Life Example:**

Socho Flipkart pe sale chal rahi hai aur ek attacker ne botnet se itna fake traffic bheja ki Flipkart ka server crash ho gaya — asli customers kuch kharid hi nahi paaye.

💣 **Impact:**

- Server down ho jata hai
- Business ko loss hota hai
- Customers frustrated ho jaate hain

□ **Prevention:**

- Load balancers
- Rate limiting
- DDoS protection services (Cloudflare, AWS Shield)

3️⃣ Man-in-the-Middle (MITM) Attack

📌 **Definition:**

Is attack mein attacker tumhare aur dusre person ke beech **communication ka beech ka rasta pakad leta hai**, jisse dono ko pata hi nahi chalta ki koi third-party sun rahi hai ya data modify kar rahi hai.

□ **Real-Life Example:**

Tum ek unsecured Wi-Fi (jaise railway station par) se bank login kar rahe ho, aur attacker beech mein ghus ke tumhara username-password capture kar leta hai — ye MITM attack hai.

📉 **Impact:**

- Personal info (passwords, OTPs) leak ho jata hai
- Financial frauds ho sakte hain
- Data integrity break ho sakti hai

□ **Prevention:**

- HTTPS websites ka use karo
- VPN ka use karo
- Public Wi-Fi avoid karo

🔢 Threat Type	📌 Definition	⍰ Real-Life Example	🔒 Impact/Effect
Unauthorized Access	Bina permission ke system/data access	Student ne teacher login se marks change kiye	Data leak, security breach
DDoS Attack	Fake traffic bhej kar server ko slow/crash karna	Botnet se Flipkart server crash	Server down, business loss
Man-in-the-Middle (MITM)	User aur server ke beech data ko secretly read/modify karna	Public Wi-Fi se bank login aur data chura liya	Login info leak, financial fraud

🔐 Concept of Security Principles with Real-Life Examples

1️⃣ Confidentiality and Privacy

◆ **Meaning:**
Data ko sirf **authorized logon** ke liye hi accessible banaya jata hai. Kisi bhi unauthorized person ko data nahi milna chahiye.
Privacy matlab kisi ki personal information ko protect karna, jise bina unki permission ke share nahi karna.

□ **Real-Life Example:**

- Tum apne phone mein apne private photos aur messages rakhte ho. Agar kisi ne bina tumhari permission ke wo dekha ya share kiya, to confidentiality and privacy break ho gayi.
- Bank account ka password sirf tumhare paas hota hai. Agar kisi aur ko pata chal jaye to tumhara paisa khatra mein hai.

2️⃣ Authentication

◆ **Meaning:**
System verify karta hai ki jo user claim kar raha hai, wo waise hi hai ya nahi. Matlab user ki **pehchaan confirm karna**.

□ **Real-Life Example:**

- Jab tum apne Gmail account mein login karte ho, tum username aur password dalte ho. System check karta hai ki ye details sahi hain ya nahi.
- ATM card ke sath PIN daalna bhi authentication ka example hai.

3️⃣ Authorization and Access Control

◆ **Meaning:**

Authentication ke baad decide hota hai ki user ko system ke kis part ya data tak **kaunse adhikar** milenge. Matlab, user kya kar sakta hai aur kya nahi.

□ **Real-Life Example:**

- College portal mein teachers ko students ke marks edit karne ka access hota hai, par students ko sirf apne marks dekhne ka access hota hai.
- Facebook mein tum apne posts ko public, friends, ya private set kar sakte ho — ye authorization hai.

4️⃣ Integrity

◆ **Meaning:**

Data ka asli aur **unchanged rehna** zaroori hai. Koi bhi unauthorized person data ko badal nahi sakta.

□ **Real-Life Example:**

- Agar tumne online shopping mein ₹1000 ka order diya aur invoice mein ₹10000 likh diya gaya, to integrity fail ho gayi.
- Exam results portal par agar marks galat dikhaye jaye to bhi integrity ka issue hota hai.

5️⃣ Non-Repudiation

◆ **Meaning:**
User apne kiye gaye kaam (jaise message bhejna, transaction karna) ko baad mein **inatkar na kar sake**.

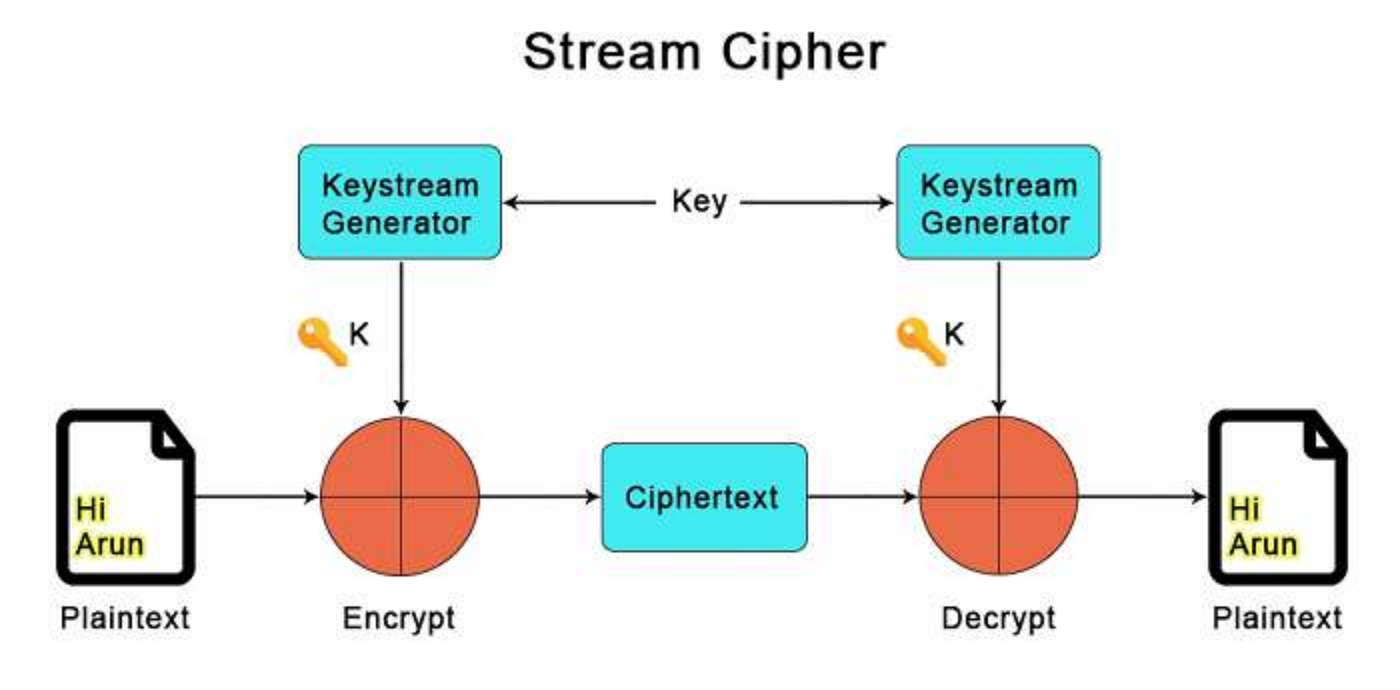
□ **Real-Life Example:**

- Tumne kisi ko UPI se paise bheje aur bank ke pass digital receipt saved hai, to tum ye claim nahi kar sakte ki maine paise nahi bheje.
- Email mein jab tum digital signature lagate ho, to sender ko apne message bhejne se inkaar nahi kar sakta.

Principle	Meaning (Hinglish)	Real-Life Example
Confidentiality & Privacy	Data sirf authorized users ke liye ho	Private photos sirf apne phone mein
Authentication	User ki identity verify karna	Gmail login with username & password
Authorization & Access Control	User ko kya karne ki permission hai batana	Teacher ko marks edit karne ka right, student ko nahi
Integrity	Data ko unchanged aur asli rakhna	Online order ka sahi invoice dikhana
Non-Repudiation	User apne kaam se inkaar na kar sake	Bank transaction ka digital receipt

Security Service	Definition	Real-Life Example	Explanation
Access Control	Authorized logon ko hi system ya data tak access dena.	Office building mein ID card se entry control.	Sirf authorized employees hi building mein enter kar sakte hain apna ID card dikhake.
Data Encryption	Data ko unreadable form mein convert karna jab tak authorized user na dekhe.	WhatsApp messages end-to-end encrypted hoti hain.	Jab aap message bhejte hain, wo encrypt ho jata hai, aur sirf receiver hi decrypt kar pata hai.
Firewall Service	Network traffic ko monitor aur filter karna unauthorized access rokne ke liye.	Company network mein firewall laga hota hai.	Firewall unauthorized websites ya hackers ko network mein aane se rokta hai.
Intrusion Detection System (IDS)	Suspicious activities ko detect karna network ya system par.	Bank network mein IDS suspicious login attempt detect karta hai.	Agar koi unknown IP se bank system ko hack karne ki koshish karta hai to IDS alert karta hai.
Virus and Malware Protection	System ko harmful software se bachana.	Antivirus software jo aapke computer ko viruses se protect karta hai.	Antivirus aapke system ko scan karta hai aur malware delete karta hai.
Backup Service	Data ka duplicate copy banake safe rakhna.	Company server data ka daily backup.	Agar original data corrupt ya delete ho jaye, to backup se recover kar sakte hain.
Security Auditing	Systems aur processes ki regular checking karna security flaws ke liye.	IT team ke regular security audits.	Company ki security team software aur network ko check karti hai vulnerabilities ke liye.
Physical Security Service	Buildings, equipment, and personnel ko physical threats se bachana.	Security guards, CCTV cameras, biometric entry system.	Office mein guards aur cameras lagaye hote hain unauthorized entry rokne ke liye.

🔐 Stream Ciphers



🔐 Stream Cipher Example using XOR

Plaintext: "Hi"

Keystream: Random (e.g., for demo)

Character	ASCII (Decimal)	Binary (Plaintext)	Keystream (Binary)	XOR Result (Ciphertext Binary)	Ciphertext (Char)	Explanation (हिंदी + English)
H	72	01001000	00110110	01111110	~	H का binary XOR किया keystream से → मिला ~
i	105	01101001	11001100	10100101	¥	i का binary XOR किया keystream से → मिला ¥

🔓 Decryption (XOR Ciphertext with Same Keystream)

Ciphertext	Binary (Ciphertext)	Keystream (Binary)	XOR Result (Plaintext Binary)	Plaintext (Char)	Explanation (हिंदी + English)
~	01111110	00110110	01001000	H	Ciphertext ~ को फिर से उसी keystream से XOR किया → H मिला
¥	10100101	11001100	01101001	i	Ciphertext ¥ को फिर से उसी keystream से XOR किया → i मिला

Final Output

- **Original Plaintext** → Hi
- **Ciphertext** → ~¥
- **Decrypted Plaintext** → Hi

🔐 What is a Substitution Cipher?

Definition:

Substitution cipher ek **encryption technique** hai jisme **plaintext ke letters ko kisi aur letter ya symbol se replace (substitute)** kiya jaata hai.
☞ Ye technique message ko unreadable bana deti hai jab tak original substitution rule (key) na pata ho.

□ **Simple Meaning:**
"Har letter ko kisi naye letter ya symbol se badal do!"
(Replace every character in the original message with another one.)

1. Monoalphabetic Substitution Cipher

Definition:
Monoalphabetic cipher mein har letter of the plaintext **replace hota hai ek fixed letter se** from the alphabet.
☞ **Ek hi substitution pattern** poore message ke liye use hota hai.

□ **Steps:**

1.Plaintext alphabet: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2.Cipher alphabet (random or fixed): Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
Yahaan pe 'A' replace hoga 'Q' se, 'B' replace hoga 'W' se, and so on...

🔤 **Example:**

Plaintext: HELLO

Substitution Key:

Plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

🔄 **Substitute each letter**:

- H → I
- E → T
- L → S
- L → S
- O → G

Ciphertext = ITSSG

🔐 2. Polyalphabetic Substitution Cipher

Definition:
Ismein multiple cipher alphabets use kiye jaate hain. Har letter ka substitution depend karta hai **position** pe aur **keyword** pe.
☞ Most famous: **Vigenère Cipher**

□ **Steps (Vigenère Cipher):**

1. Choose a **keyword** (e.g., KEY)
2. Repeat keyword to match length of plaintext.
3. Use formula:

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

Where:

- C_i = Cipher character
- P_i = Plain character (A=0, B=1...)
- K_i = Key character (A=0, B=1...)

🔤 **Example:**

Plaintext: HELLO

Keyword: KEY → repeat → KEYKE

Plaintext : H E L L O

Key : K E Y K E

(10 4 24 10 4)

Positions : 7 4 11 11 14 (H=7, E=4, L=11, O=14)

Add (mod 26):

Cipher : (7+10) (4+4) (11+24) (11+10) (14+4)

= 17 8 9 21 18

Ciphertext : R I J V S

Final Ciphertext = RIJVS

Feature 🔍	Monoalphabetic Cipher 🔤	Polyalphabetic Cipher 🔡
🔑 **Substitution Rule**	Ek hi fixed substitution rule poore message ke liye.	Multiple rules use hote hain, based on keyword.
🔄 **Letter Mapping**	Har letter ka same substitution hota hai har jagah.	Ek letter ka substitution bar-bar change hota hai.
🔐 **Security**	Kam secure – frequency analysis se crack ho sakta hai.	Zyada secure – frequency analysis difficult hota hai.
🎯 **Example**	Caesar Cipher, Simple Substitution Cipher	Vigenère Cipher, Beaufort Cipher
Logic	A → M, B → N... fixed hai sabke liye.	A → X (1st), A → K (2nd), A → P (3rd)... alag ho sakta hai.
🔢 **Key Type**	Single substitution key	Keyword used (repeat hota hai)
Plaintext vs Cipher	HELLO → ITSSG (same pattern)	HELLO → RIJVS (based on "KEY")
Mathematical Formula	C = (P + K) mod 26 (K = fixed)	C = (P + K[i]) mod 26 (K[i] = keyword letter)
📉 **Frequency Attack Resistance**	Low – frequency patterns remain visible	High – patterns get broken due to varying keys

🔍 Real-Life Analogy:

- □ *Monoalphabetic Cipher*: Jaise tumhara dost hamesha "Jayesh" ko "Xayesh" bolta hai — **hamesha ek hi tarah se**.

- 👥 *Polyalphabetic Cipher*: Par agar wo har baar alag nickname use kare (Xayesh, Jayu, JayRock) — **toh samajhna mushkil ho jaata hai**!

🔀 What is a Transposition Cipher?

🔐 Definition:

Transposition Cipher ek aisa cipher hota hai jisme:

"Letters ko replace nahi kiya jaata, sirf unka order (position) change kiya jaata hai.“

💡 *Yaani characters wahi rehte hain, but jagah badal jaati hai.*

□ Easy Explanation:

- Agar original message hai: HELLO
- Toh Transposition Cipher bas iska **sequence change karega**.
- Example: LOHEL, ELHLO, etc.

☞ **Koi bhi naya letter add ya replace nahi hota**, sirf **letters ki arrangement change hoti hai**.

🔀 Transposition Cipher: Rail Fence Cipher

Definition:

Rail Fence Cipher ek **Transposition Cipher** hai jisme **letters ka position change hota hai** (but letters replace nahi hote).

☞ Ismein hum plaintext ke letters ko ek **zig-zag pattern** mein likhte hain multiple "rails" par (jaise ek fence) aur fir line by line read karte hain.

□ EASY EXAMPLE – Rail Fence Cipher (2 Rails)

🔤 **Plaintext: HELLOWORLD**

🔑 **Key: 2 Rails**

- Step-by-Step Zig-Zag Pattern

Position	1	2	3	4	5	6	7	8	9	10
Plaintext	H	E	L	L	O	W	O	R	L	D
Rail 1 (↑)	H		L		O		O		L	
Rail 2 (↓)		E		L		W		R		D

Step 2: Read Line by Line

- **Rail 1** → H L O O L
- **Rail 2** → E L W R D

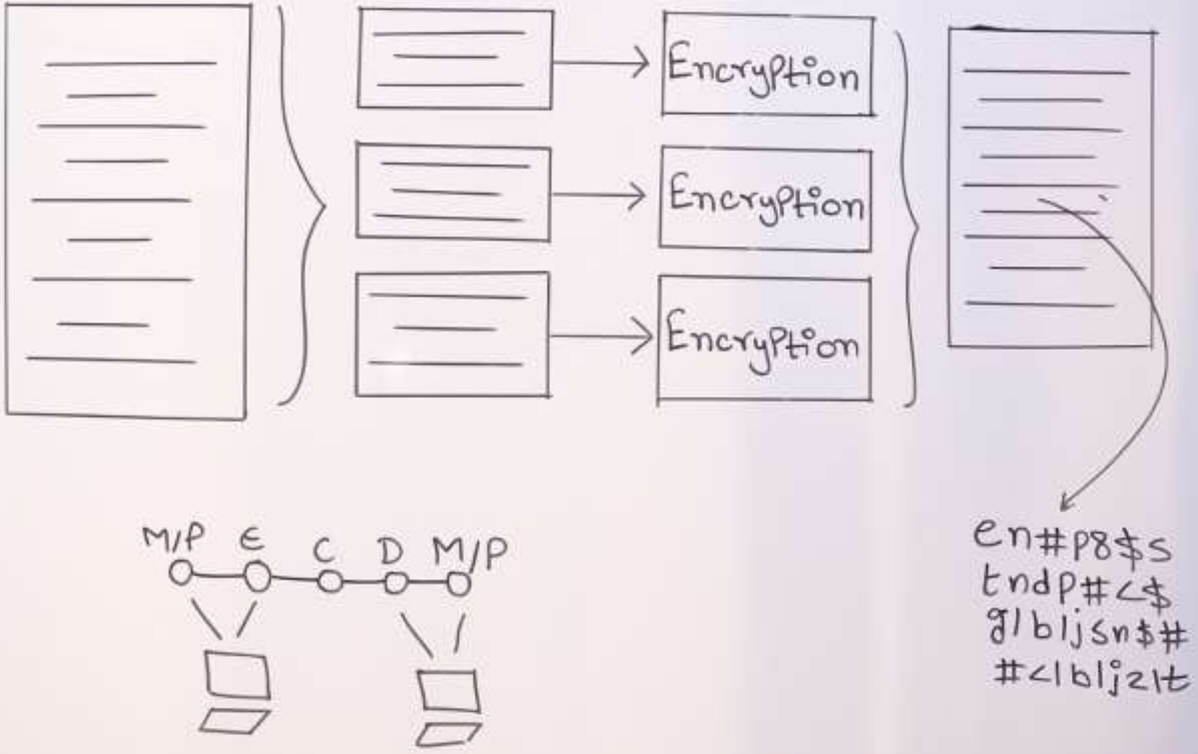
🔐 Final Ciphertext: HLOOLELWRD

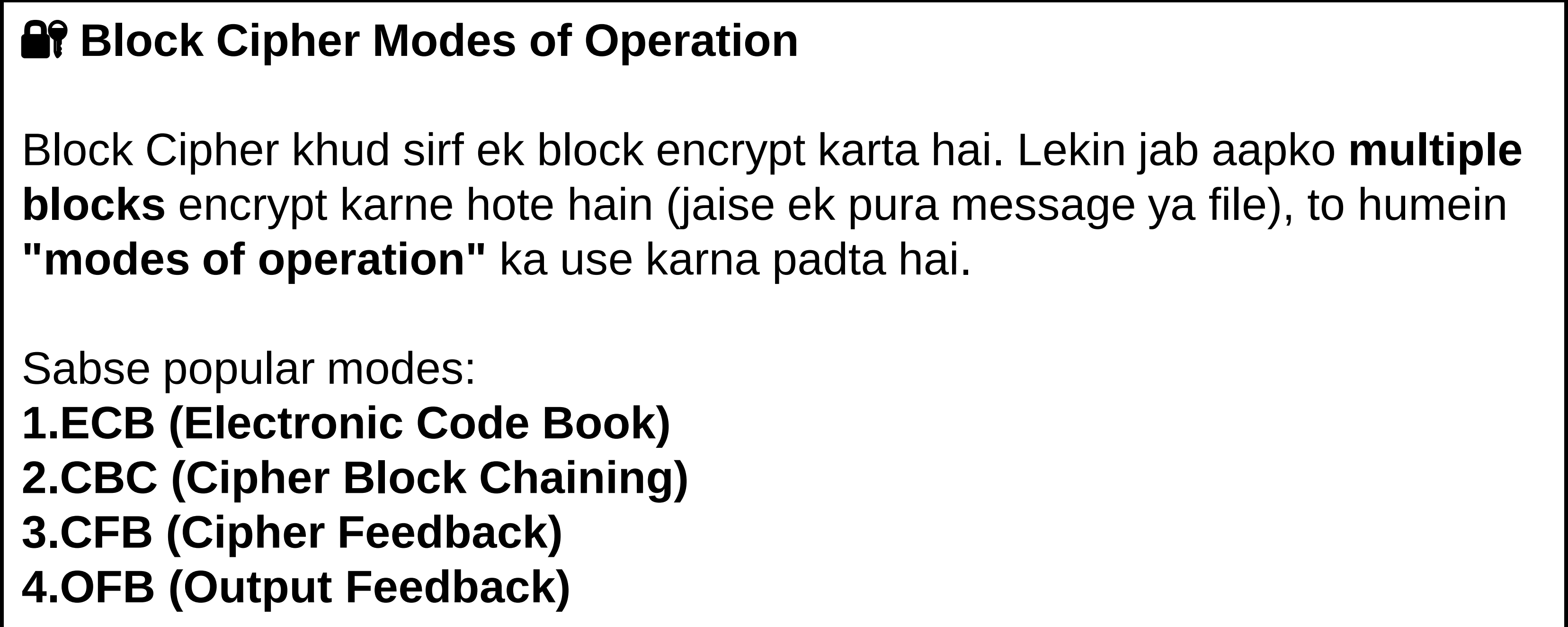
💡 Block Cipher Kya Hai?

Block Cipher ek encryption technique hai jo data ko **fixed-size blocks** (jaise 64-bit ya 128-bit) mein todta hai, aur har block ko ek secret key ke saath encrypt karta hai.
Yeh symmetric encryption hota hai — matlab **encrypt aur decrypt karne ke liye same key use hoti hai**.

□ Kaise kaam karta hai Block Cipher?

1. Plaintext (normal readable data) ko chhote-chhote blocks mein divide kiya jata hai.
2. Har block ko ek encryption algorithm aur secret key ke saath encrypt kiya jata hai.
3. Encrypted output ko **ciphertext** kehte hain — jo unreadable hota hai bina key ke.


Encryption
Encryption
Encryption
en#p8$s
tndp#<$
g/bljsn$#
#<lbljz1t
M/P
E
C
D
M/P



🔐 Block Cipher Modes of Operation

Block Cipher khud sirf ek block encrypt karta hai. Lekin jab aapko **multiple blocks** encrypt karne hote hain (jaise ek pura message ya file), to humein **"modes of operation"** ka use karna padta hai.

Sabse popular modes:

1. **ECB (Electronic Code Book)**
2. **CBC (Cipher Block Chaining)**
3. **CFB (Cipher Feedback)**
4. **OFB (Output Feedback)**

1️⃣ ECB – **Electronic Code Book Mode**

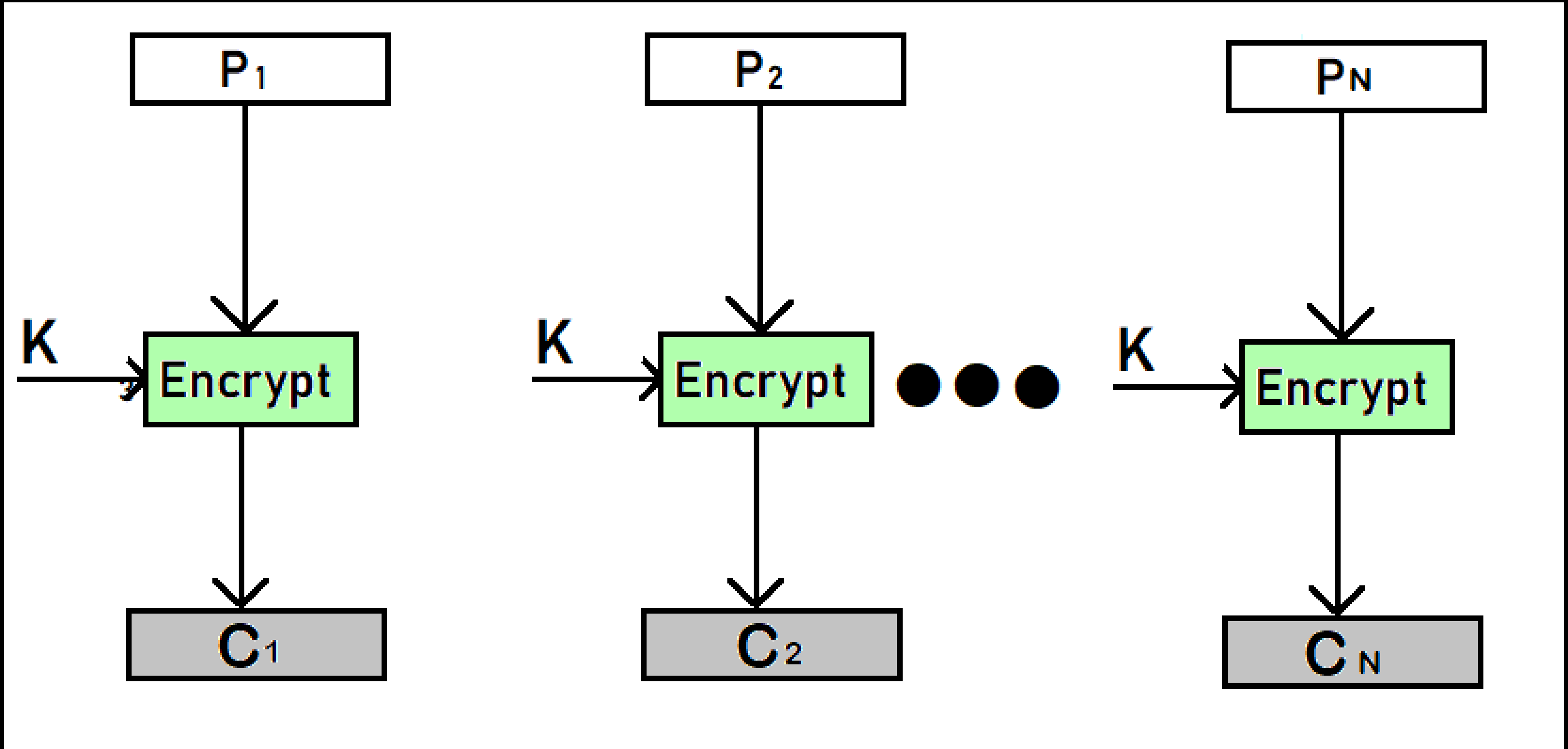
🔐 1️⃣ ECB – Electronic Code Book Mode

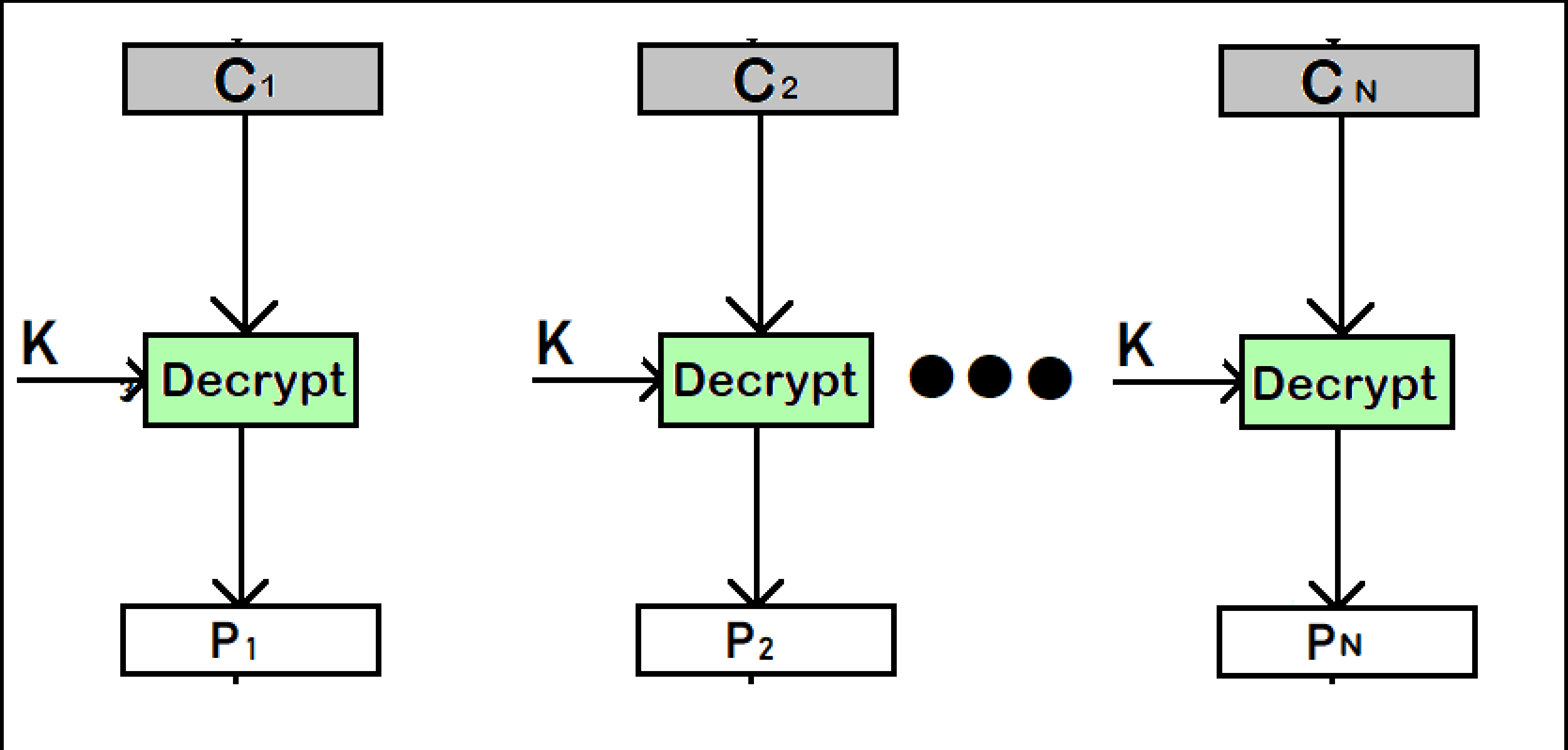
📌 Kya hota hai?

ECB mode mein **har block of data ko alag se encrypt** kiya jata hai, bina kisi chaining ke.

Matlab:

•Har block ka encryption **independently** hota hai.
•Agar koi block bar-bar repeat ho raha hai, to uska **ciphertext bhi same** repeat hoga.


P1
P2
PN
K
Encrypt
K
Encrypt
K
Encrypt
C1
C2
C N


C1
C2
CN
K
Decrypt
K
Decrypt
K
Decrypt
P1
P2
PN

Block Size ka Matlab:

- **Block size** = ek block mein kitne bits ya bytes data hota hai
- ECB mode mein **same size ke blocks** hone chahiye
- Agar data chhota ho to **padding** lagayi jaati hai

🔢 Common Block Sizes:

Algorithm	Typical Block Size
AES	**128 bits** (16 bytes)
DES	**64 bits** (8 bytes)
Triple DES	64 bits (8 bytes)

♦ **ECB mode khud block size define nahi karta**, yeh encryption algorithm (like AES, DES) ke upar depend karta hai.

□ Example Setup:

Element	Value
Plaintext	"DATA LOVE DATA" (12 characters)
Block Size	4 characters
Blocks	["DATA", "LOVE", "DATA"]
Encryption Key	"KEY1"

(Note: Real encryption mein output random jaisa hota hai. Yahaan samajhne ke liye simple letters use kar rahe hain.)

□ Step-by-Step Encryption Process:

Step	Plaintext Block	Operation	Ciphertext
1️⃣	DATA	Encrypt("DATA", "KEY1")	X1A9
2️⃣	LOVE	Encrypt("LOVE", "KEY1")	Q7B2
3️⃣	DATA (repeat)	Encrypt("DATA", "KEY1")	X1A9

🔑 Har block ko **same key** se encrypt kiya ja raha hai.
🌀 "DATA" do baar aaya, to dono baar **same ciphertext** "X1A9" mila.

🔍 Final Output:

Plaintext = DATA | LOVE | DATA
Ciphertext = X1A9 | Q7B2 | X1A9

ECB Mode ke Fayde (Advantages):

- Simple aur fast hai.
- Har block alag se encrypt hota hai (parallel processing possible hai).
- Testing ya chhoti, non-sensitive data ke liye useful hai.

❌ ECB Mode ke Nuksaan (Disadvantages):

- **Same input = same output** → attackers pattern guess kar sakte hain.
- Not secure for images, documents, or repeated data.
- Real-world use mein **secure nahi mana jata**.

□ **Real-Life Analogy:**

Socho tum ek book likh rahe ho, aur har page ko **same lock** lagakar secure kar rahe ho.

Agar koi same page baar-baar aaye, to lock bhi same hoga — to koi bhi dekh ke guess kar sakta hai ki "ye page pehle bhi tha!"

🔐 2️⃣ CBC – Cipher Block Chaining Mode

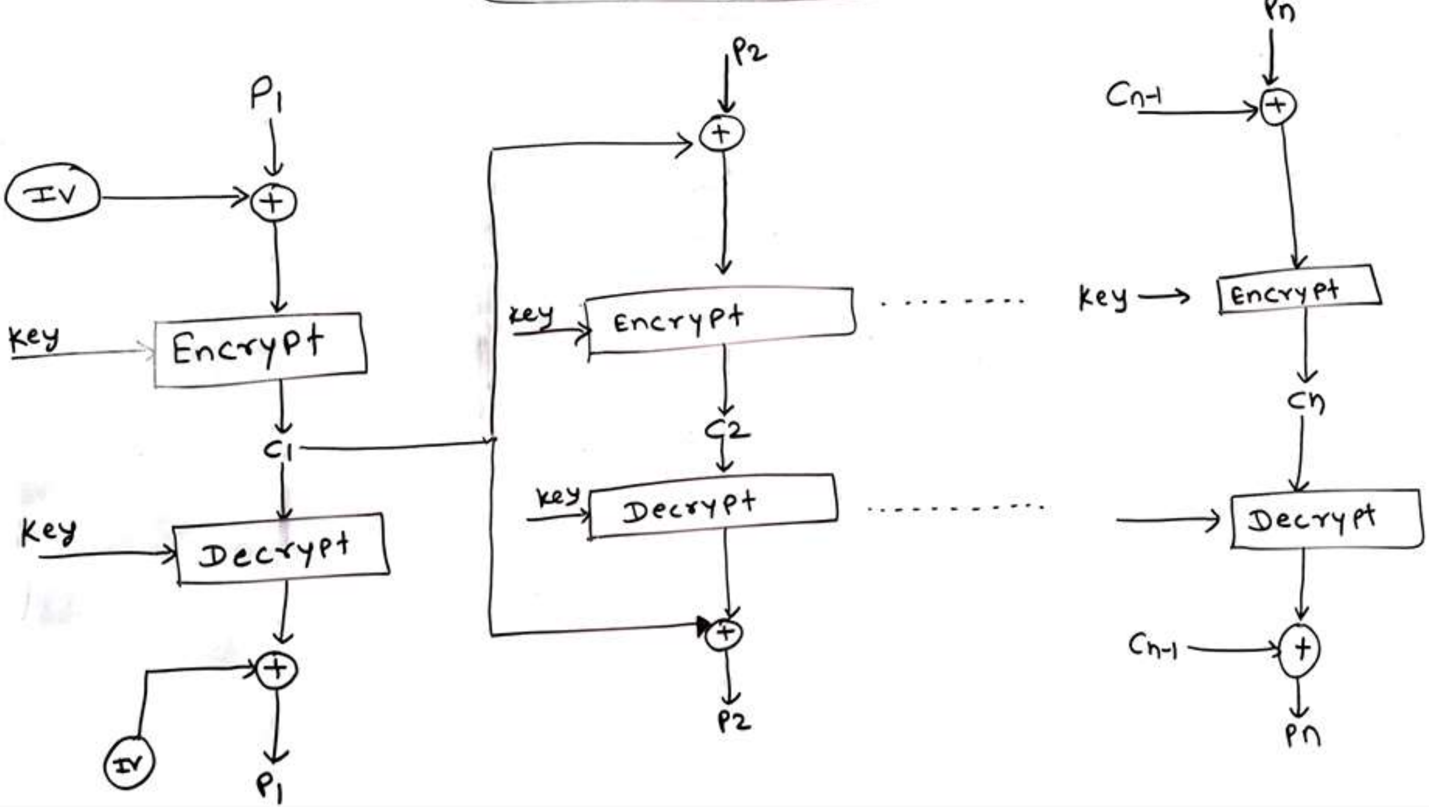
📌 Kya hota hai?

CBC mode mein:

- Har plaintext block **pichle ciphertext block** se **XOR** hota hai **encrypt hone se pehle**.
- Pehle block ke liye, koi ciphertext nahi hota, isliye **IV (Initialization Vector)** use hota hai.

Chaining ka matlab hai: har block ke encryption ka result next block ke encryption ko effect karta hai.

Cipher Block chaining (CBC)



- Example Setup:

Element	Value
Plaintext	"DATA LOVE" (8 letters)
Block Size	4 characters (like: "DATA", "LOVE")
Encryption Key	"KEY1"
IV (initial input)	"INIT"

□ CBC Mode Step-by-Step Encryption:

Step	Plaintext Block	XOR With	Result	Encrypt (with Key)	Ciphertext Block
1️⃣	DATA	IV = INIT	XOR1	Encrypt(XOR 1)	C1
2️⃣	LOVE	C1	XOR2	Encrypt(XOR 2)	C2

🔁 **Chaining effect**:

- C1 is used to encrypt next block (P2)
- C2 is used for the next... and so on...

🔁 CBC Mode Step-by-Step Decryption:

Step	Ciphertext Block	Decrypt (with Key)	Result	XOR With	Plaintext Block
1️⃣	C1	Decrypt(C1)	D1	IV = INIT	P1 = D1 ⊕ INIT
2️⃣	C2	Decrypt(C2)	D2	C1	P2 = D2 ⊕ C1

Diagram Explanation

Encryption:
P1 ─► XOR with IV ─► Encrypt ─► C1
P2 ─► XOR with C1 ─► Encrypt ─► C2
P3 ─► XOR with C2 ─► Encrypt ─► C3

Decryption:
C1 ─► Decrypt ─► D1 ─► XOR with IV ─► P1
C2 ─► Decrypt ─► D2 ─► XOR with C1 ─► P2
C3 ─► Decrypt ─► D3 ─► XOR with C2 ─► P3

CBC ke Fayde (Advantages):

- **More secure than ECB**: Same blocks ka same output nahi aata
- IV and chaining se randomness aata hai
- Commonly used in SSL/TLS, file encryption

❌ **CBC ke Nuksaan:**

- **Slow**: Har block ko pehle wale block ke ciphertext ka wait karna padta hai
- Agar ek block corrupt ho jaaye to next block bhi affect hota hai (error propagation)

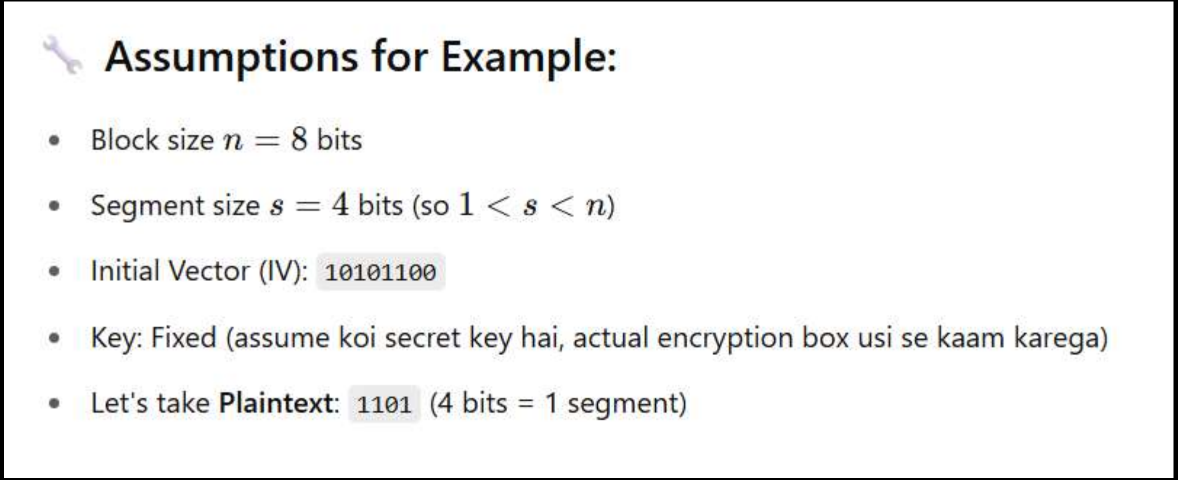
□ **Real-Life Analogy:**

Socho tum ek chittiyan likh rahe ho (P1, P2, P3...) aur har chitti likhne se pehle tumhe pichli chitti ka jawab padna padta hai.

Agar ek jawab galat hai, to agla letter bhi bekaar ho jaata hai.

🔒 CFB Mode: Basic Idea

- CFB mode mein **encryption algorithm** ko baar-baar use kiya jata hai.
- Plaintext ko directly encrypt nahi karte — pehle encryption result ke
- kuch bits liye jaate hain, fir unka XOR plaintext ke s-bit se hota hai.



🔧 Assumptions for Example:

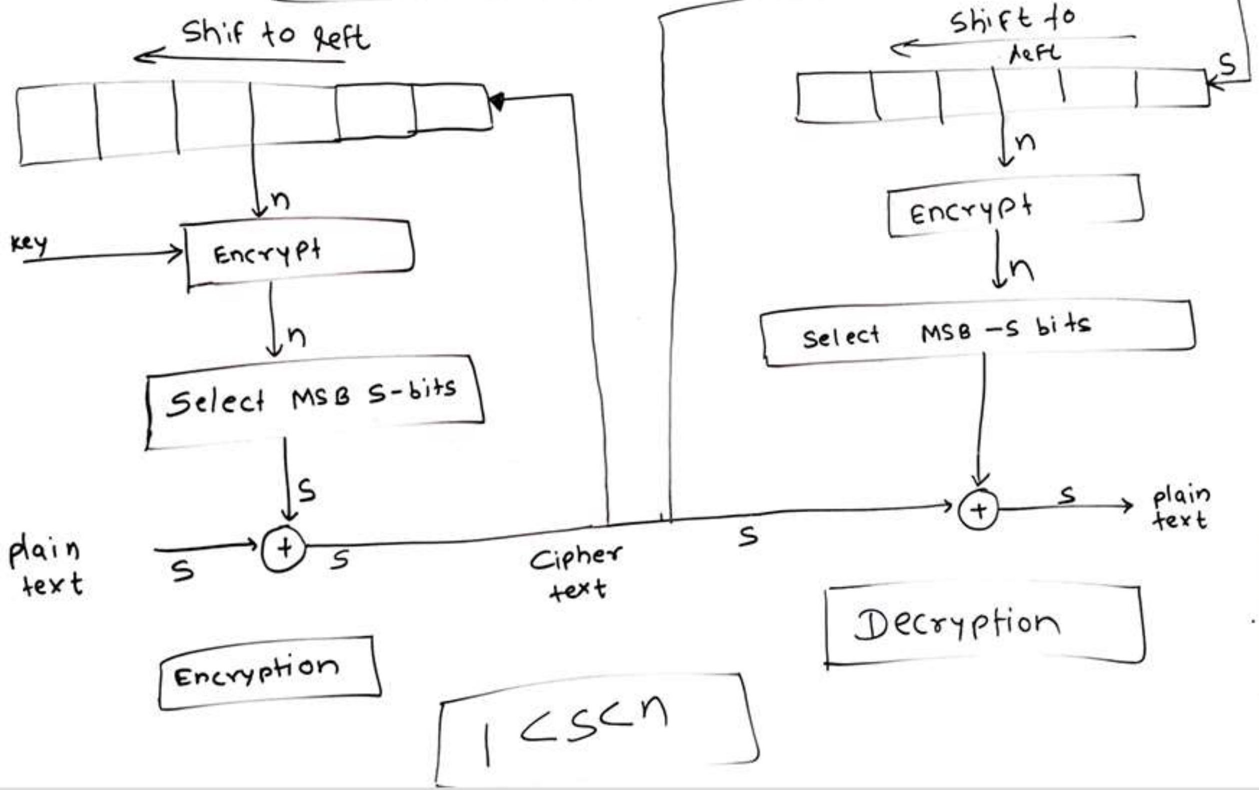
- Block size $n = 8$ bits
- Segment size $s = 4$ bits (so $1 < s < n$)
- Initial Vector (IV): `10101100`
- Key: Fixed (assume koi secret key hai, actual encryption box usi se kaam karega)
- Let's take **Plaintext**: `1101` (4 bits = 1 segment)

🔐 Encryption Steps

Assume:

- IV (Initial Vector) = 10101100
- Key: (fixed, assume secret hai)
- Plaintext (4 bits ka ek segment) = 1101
- Let’s assume block size n = 8 bits and segment size s = 4 bits
- Encrypted output of IV = 11001010 (ye sirf example ke liye assume kiya hai)

Cipher Feedback Mode (CFB)



Step-by-step Encryption:

◈ Step 1: Start with IV

IV = 10101100

Ye IV encryption process ka starting input hota hai.

◈ Step 2: Encrypt IV using the key

IV ko block cipher ke andar daala jata hai with key:

Encrypt(10101100) = 11001010

(Note: Actual output key pe depend karta hai — yeh bas ek example hai)

◈ Step 3: Select MSB s-bits

Encrypted result = 11001010

MSB (Most Significant Bits) ke first 4 bits select karo:

MSB 4 bits = 1100

◈ Step 4: XOR with plaintext

Plaintext = 1101

XOR operation: 1100 ⨁ 1101 = 0001

➡️ Output: Ciphertext segment = 0001

◈ Step 5: Update Shift Register

- IV = 10101100
- Usme se leftmost 4 bits hata do → 1010 remove
- Ciphertext (0001) ko right side mein jod do

➡️ **New Register Input** = 11000001

Ye updated register next segment ke liye use hoga.

🔓 Decryption Steps

Same values use honge:

- IV = 10101100
- Ciphertext = 0001
- Encrypted result of IV = 11001010
- s = 4 bits

Step-by-step Decryption:

❖ Step 1: Start with IV

IV = 10101100

❖ Step 2: Encrypt IV using key

Encrypt(10101100) = 11001010

(Same result aayega, kyunki encryption block deterministic hota hai)

❖ Step 3: Select MSB s-bits

Select top 4 bits from 11001010:

MSB = 1100

❖ Step 4: XOR with Ciphertext

Ciphertext = 0001

1100 $\oplus$ 0001 = 1101

➡ Output: Original **Plaintext = 1101**

❖ Step 5: Update Shift Register

- IV = 10101100
- Remove leftmost 4 bits → 1010
- Add Ciphertext 0001 to right

➡ **New Register Input** = 11000001

Step	Encryption	Decryption
Input	IV / Previous ciphertext	IV / Previous ciphertext
Encrypt	Encrypt register	Same encryption used
Take bits	Select MSB s-bits	Select MSB s-bits
XOR	MSB ⊕ Plaintext = Ciphertext	MSB ⊕ Ciphertext = Plaintext
Register Update	Add Ciphertext to shift register	Same update as encryption

🔍 Key Points:

- CFB mode **doesn’t use decryption function** during decryption — only encryption algorithm is used.
- IV is very important — same IV + same key → same ciphertext.
- Yeh mode **stream cipher** ki tarah behave karta hai — suitable for streaming data.

✅ Advantages:

- Error in one block affects **only few future blocks**, not all.
- Can work with **data smaller than block size**.

⚠️ Disadvantages:

- Slow if parallel processing chahiye ho (because chaining hai).
- IV must be unique and unpredictable.

Real-Life Example of CFB Mode:

Scenario:

Socho aap ek secure chat app use kar rahe ho, jisme messages realtime mein chhote chhote parts (packets) mein bheje jaate hain.

CFB Mode ka role:

- CFB mode data ko thoda thoda karke encrypt karta hai, jaise ek stream.
- Ye encryption algorithm ko hi dono encryption aur decryption ke liye use karta hai, isse implementation simple hota hai.
- Agar kisi ek block mein error aa jaye, toh sirf us block tak ka effect hota hai, puri message chain nahi kharab hoti.
- Isliye voice calls ya live chats mein ye best hai jahan data continuously flow hota rahe.

Example:

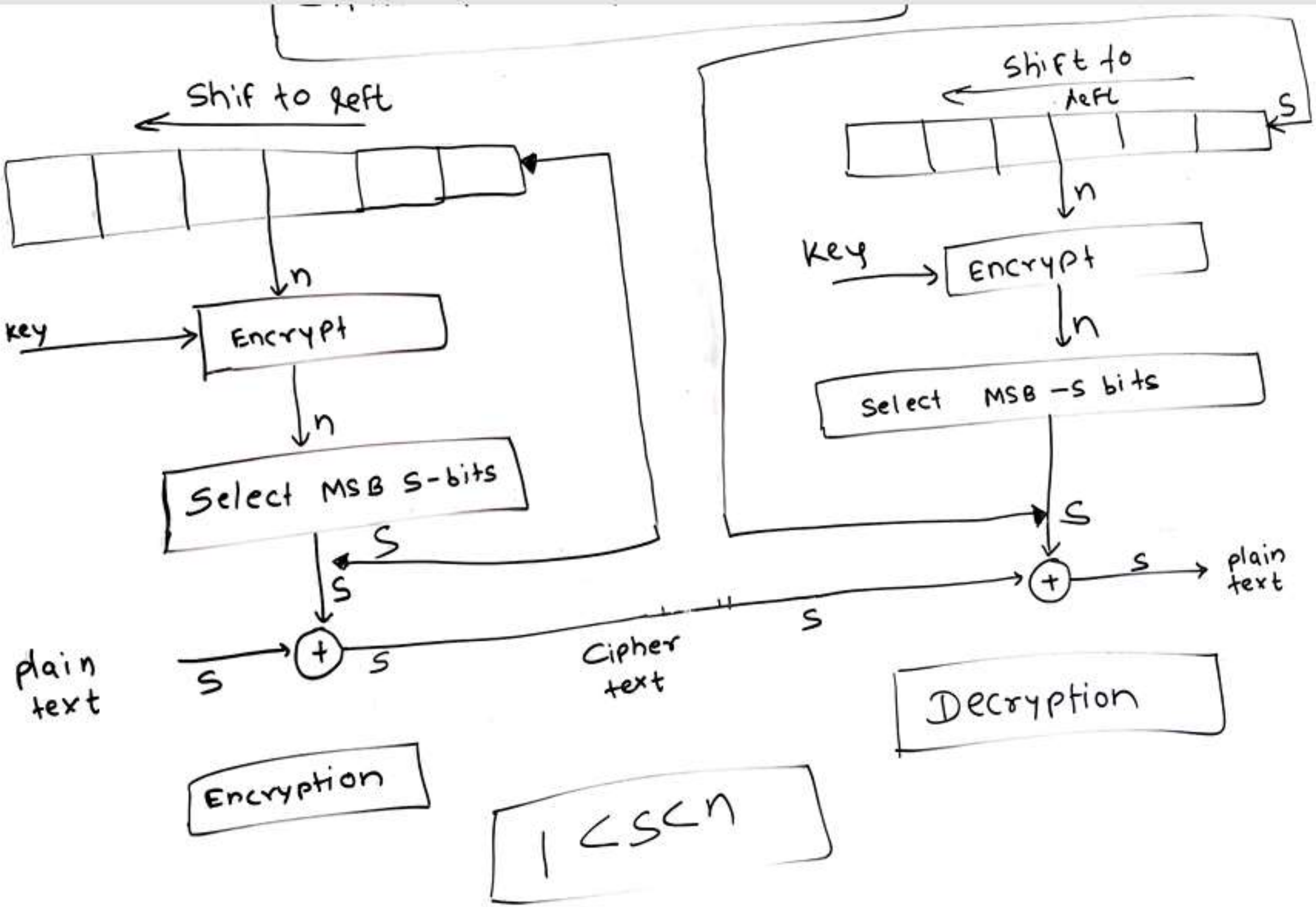
Aap message bhejte ho → har chhota part CFB se encrypt hota hai → receiver pe same process se decrypt → message secure rahta hai without delay.

🔐 What is OFB Mode?

OFB mode ka full form hai **Output Feedback Mode**. Isme **encryption algorithm ka output feedback** ke form mein use hota hai next encryption step ke liye. Iska main fayda hai ke **same plaintext** agar baar-baar encrypt karo, toh **different ciphertext** milega (agar IV alag ho).

□ Basic Idea (Simple Words Mein):

- OFB mode mein **block cipher** ko **stream cipher** banaya jata hai.
- Yahan **plaintext block** ko directly encrypt nahi kiya jata.
- Instead, ek **keystream generate** ki jati hai, jisko plaintext ke saath **XOR** kiya jata hai.


Shif to Reft
n
key
Encrypt
n
Select MSB S-bits
S
S
plain text
S
S
Cipher text
S
Shift to left
S
n
key
Encrypt
n
Select MSB -s bits
S
S
plain text
Encryption
Decryption
1 < s < n

🔐 Encryption Side (Left Side of Diagram)

Step-by-Step:

1. **Start with IV (Initialization Vector):**
   - Ek initial block hota hai — IV (not shown in the cropped image, but assumed at the top).
   - IV ko shift kiya jata hai **left** mein to prepare for encryption.
2. **Encrypt with Key:**
   - IV ya previous output block ko **key ke saath encrypt** karte hain.
   - Encrypt(IV, Key) → output n bits ka block.
3. **Select MSB s-bits:**
   - Is encrypted output se **Most Significant s bits** (yaani leftmost bits) select kiye jate hain.
4. **XOR with Plain Text:**
   - Ye s-bit output ko **XOR** kiya jata hai **plain text** block ke saath.
   - Result milta hai: **Ciphertext block**
5. **Feedback Loop:**
   - Ciphertext ke jagah, encrypted output ko **next round ke input ke liye shift** kiya jata hai (left shift).
   - Process repeat hota hai for next block.

🔓 Decryption Side (Right Side of Diagram)

Step-by-Step:

1. **Same IV or previous encrypted block used:**
   1. Encryption ke jaise hi input block ko shift kiya jata hai **left**.
2. **Encrypt with Same Key:**
   1. Us block ko phir se **key ke saath encrypt** kiya jata hai.
3. **Select MSB s-bits:**
   1. Encrypt output se **MSB s-bits** select karte hain.
4. **XOR with Ciphertext:**
   1. Ab ciphertext block ko XOR karo selected bits ke saath.
   2. Result milega: **Plain Text**
5. **Repeat:**
   1. Ye s-bit output phir se feedback mein use hota hai agle block ke liye.
   2. Same steps repeat karte hain for all blocks.

⚙️ XOR ka Role (Why XOR?):

- XOR dono taraf (encryption & decryption) mein use hota hai.
- Kyunki:

Plain ⊕ Keystream = Cipher
Cipher ⊕ Keystream = Plain

Concept	Description in Hinglish
Shift Left	Feedback mechanism ka part hai, har output ko shift karke next input banta hai.
MSB s-bits	Output ke leftmost bits, jo XOR mein use hote hain.
+ symbol	Represents XOR operation.
Encrypt block	Har round mein same key se encrypt hota hai, lekin input change hota hai.
Symmetry	Encryption aur decryption ka structure same hai in OFB.

🎯 Real-Life Example (Hinglish):

Scenario:

Tum WhatsApp pe kisi ko message bhej rahe ho: "HELLO"

Assume karo:

- Each character = 1 block
- Key = Secret password
- IV = Random number har session ke start mein

Steps:

1. WhatsApp app IV generate karta hai, jaise IV = 7890
2. IV ko encrypt karta hai secret key se → output = O1
3. "H" ko ASCII mein convert karke O1 se XOR karta hai → C1
4. O1 ko fir encrypt karta hai → output = O2
5. "E" ko O2 se XOR karta hai → C2
6. Repeat for L, L, O...

Even if you type "HELLO" again, kyunki IV alag hoga, ciphertext bhi alag hoga → **same message, different encrypted output**.

DDoS Attack Kaise Kaam Karta Hai?

1.Attacker pehle kai compromised computers, devices (called **botnet**) ko control kar leta hai.
2.Ye devices simultaneously ek target website/server par request bhejna start kar dete hain.
3.Target server ya website itne zyada fake requests handle nahi kar pati.
4.Server slow ho jata hai ya crash ho jata hai, jis se legitimate users service use nahi kar pate.

Types of DDoS Attacks:

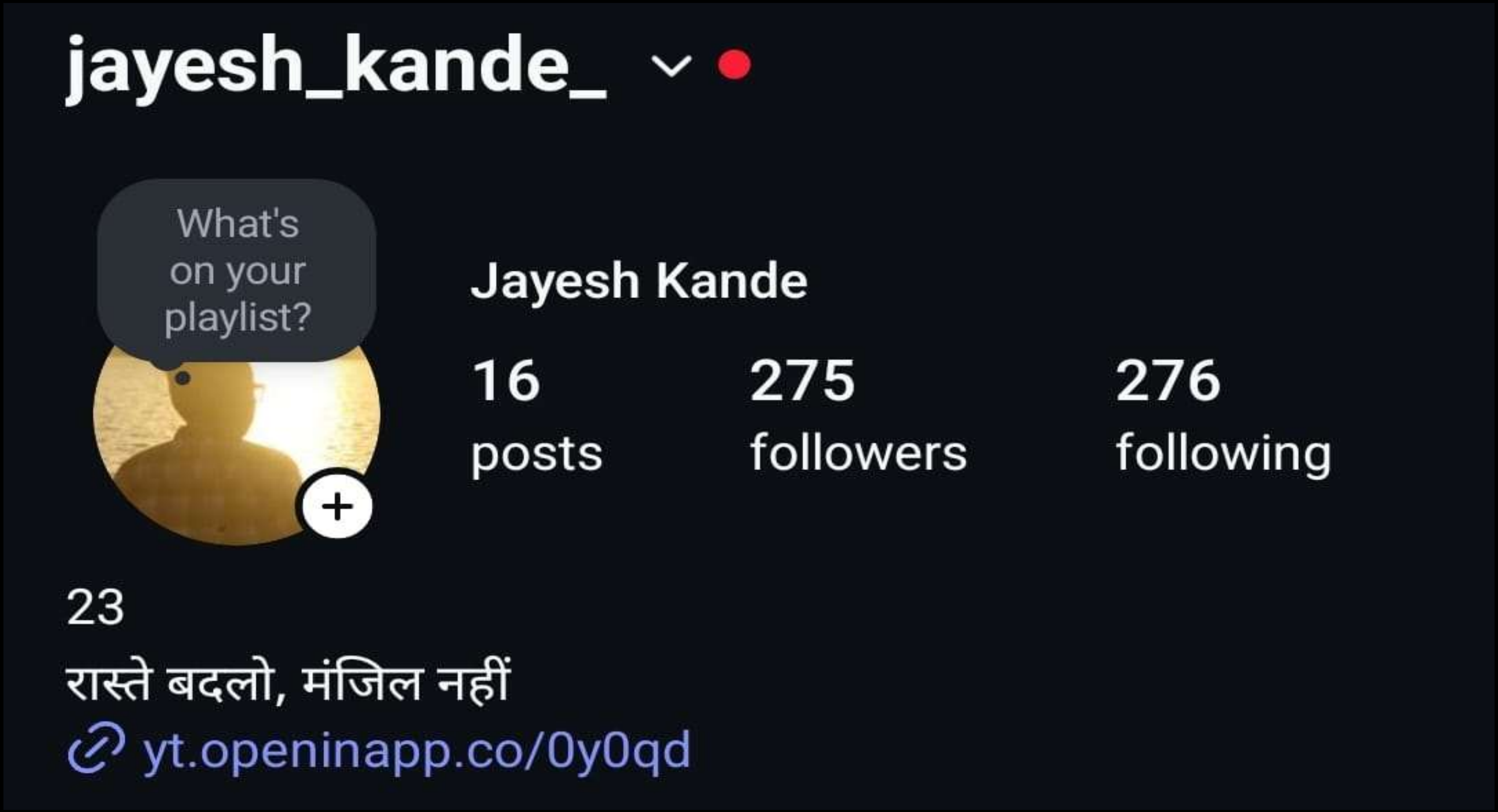
Type	Explanation	Example
Volume-based Attacks	Target ki bandwidth ko overload karna.	Flooding target with huge amount of traffic like UDP floods.
Protocol Attacks	Network protocols ki vulnerabilities ko exploit karna.	SYN flood attack jisme connection requests ko overload kiya jata hai.
Application Layer Attacks	Web server ya application layer ko target karna, jahan requests zyada complex hoti hain.	HTTP floods jisme bahut zyada web page requests bheji jati hain.

Protection Against DDoS:

Method	**Explanation**
Traffic Filtering	Suspicious traffic ko block karna.
Rate Limiting	Kisi IP se limited number of requests allow karna.
Use of CDN (Content Delivery Network)	Traffic ko distribute karna taaki overload na ho.
DDoS Protection Services	Cloudflare, Akamai jaisi companies ke special DDoS mitigation tools.
Firewall and IDS/IPS	Intrusion detection aur prevention systems lagana.

Real-Life Example:

- 2016 mein, **Dyn DNS service** par ek bada DDoS attack hua tha.
- Is attack ki wajah se Twitter, Netflix, Reddit, aur bahut si websites temporarily down ho gayi thi.
- Attack mein IoT devices ka botnet use hua tha, jise **Mirai botnet** kehte hain.



jayesh_kande_

Jayesh Kande

16 posts

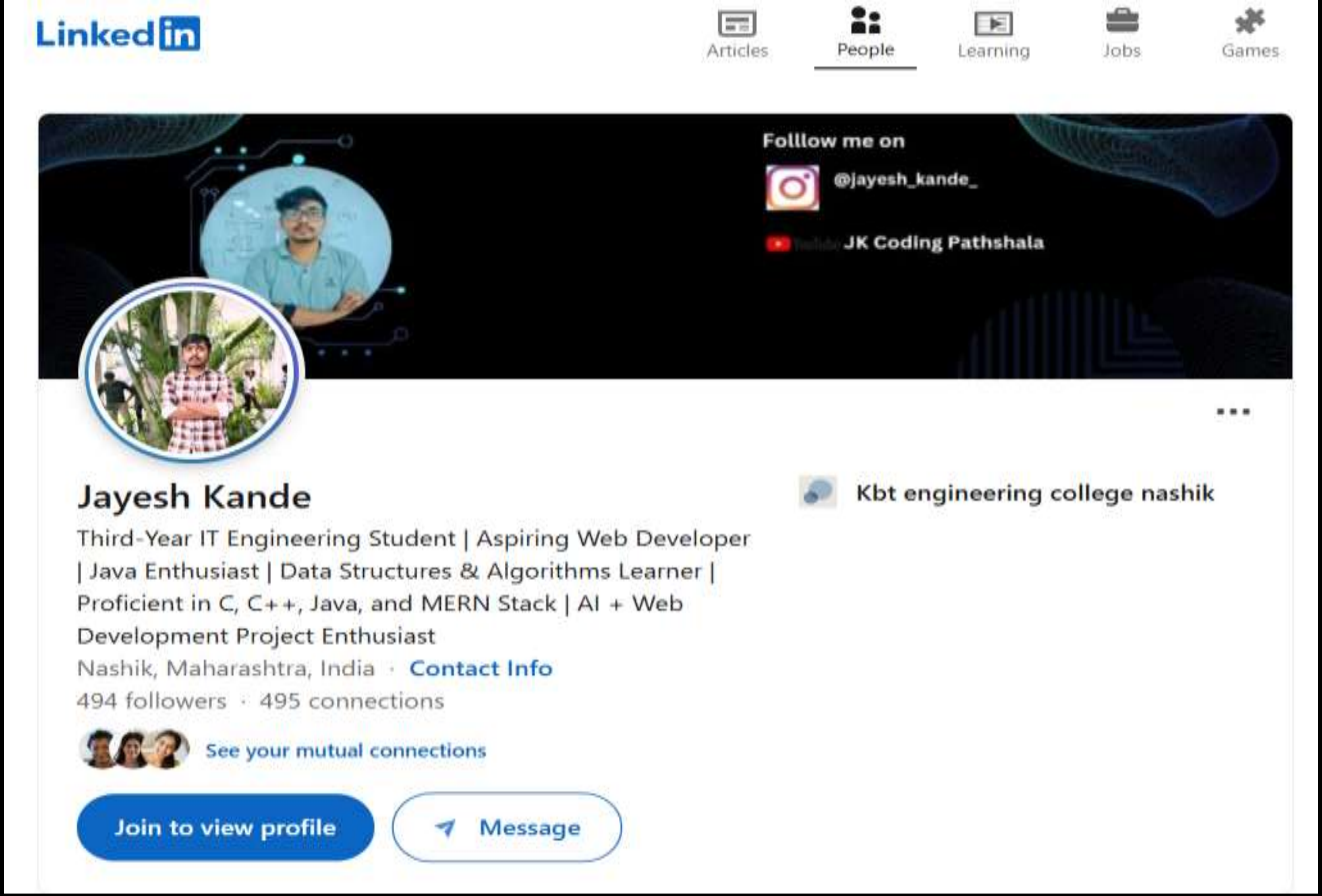
275 followers

276 following

23

रास्ते बदलो, मंजिल नहीं

yt.openinapp.co/0y0qd



Folllow me on

@jayesh_kande_

JK Coding Pathshala

Jayesh Kande

Third-Year IT Engineering Student | Aspiring Web Developer | Java Enthusiast | Data Structures & Algorithms Learner | Proficient in C, C++, Java, and MERN Stack | AI + Web Development Project Enthusiast

Nashik, Maharashtra, India · Contact Info

494 followers · 495 connections

See your mutual connections

Kbt engineering college nashik

✨ Thank You for Watching! ✨

→📱Follow us on Instagram:**@jayesh_kande_**

🔗 Connect with us on LinkedIn:[**Jayesh Kande**]