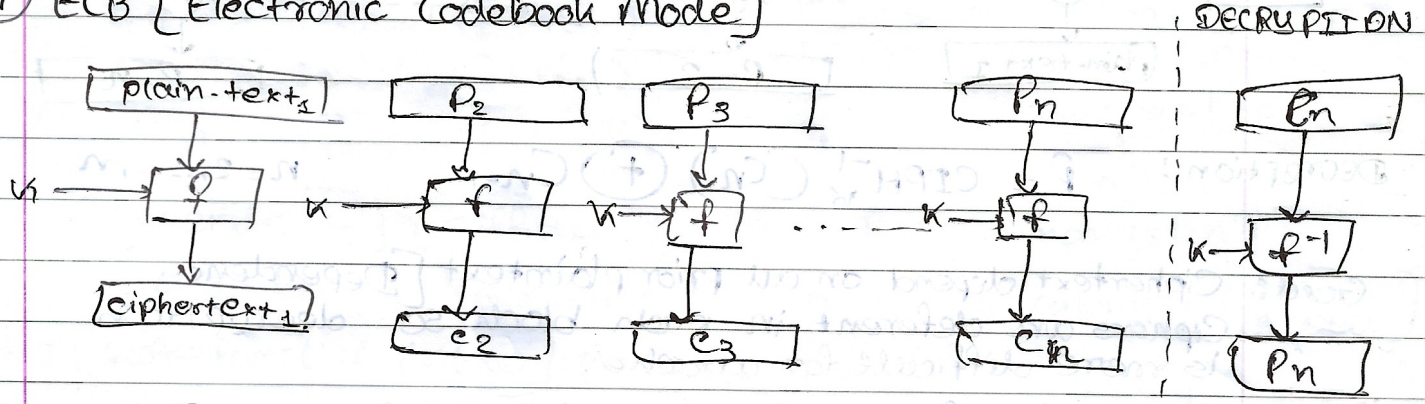
→ Block Cipher Modes of operation

Apply Block cipher repeatedly to encrypt data securely

ECB, CBC, CFB, OFB ⟶ FIPS 1981 ⟶ DES came with Modes

CTR ⟶ 2001 ⟶ AES came along

(A) ECB [Electronic Codebook Mode]



Encryption: $C_n = CIPH_K(P_n)$ $n = 1, 2, \ldots n$

Decryption: $P_n = CIPH_K(C_n)$

Good: Parallel working [Fast], if something facility it [doesn't spread]

Bad: Same keys ⟶ [Same Pattern]

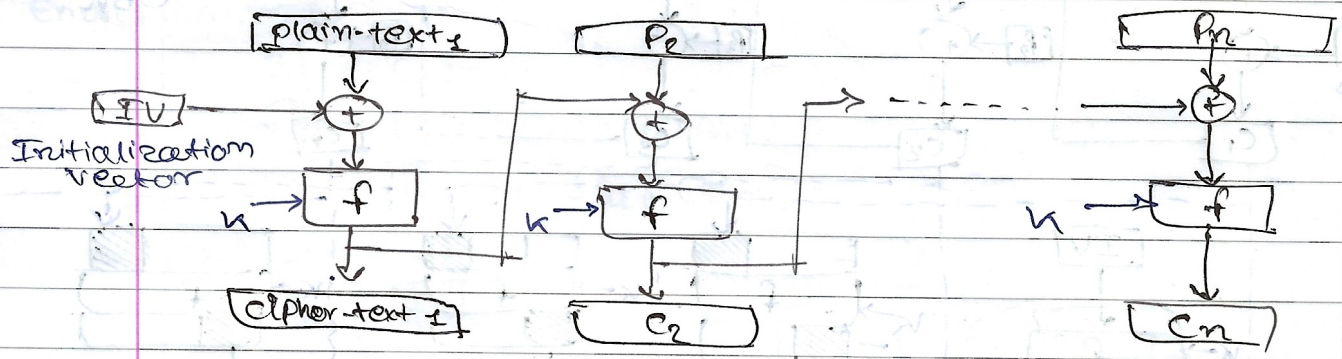
↳ CIPH are generally widely known

↳ So K is comparabely [easy to find]

[Fixed Block Sizes] ⟶ bits < size ⟶ padding required

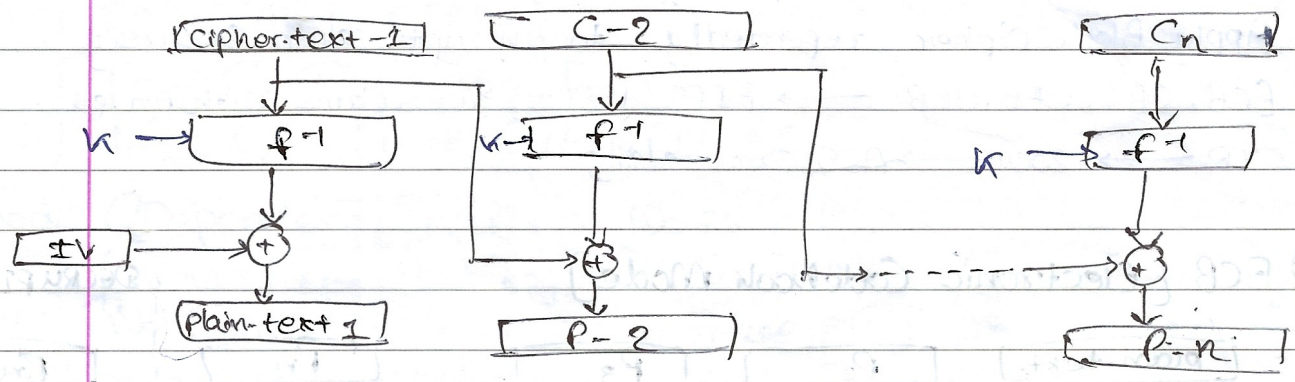
usecase: Small values, Fast processing.

(B) CBC [Cipher Block Chaining Mode]



Encryption: $C_n = CIPH_K(P_n \oplus C_{n-1})$ for $n = 1, 2, \ldots, n$

DECRYPTION



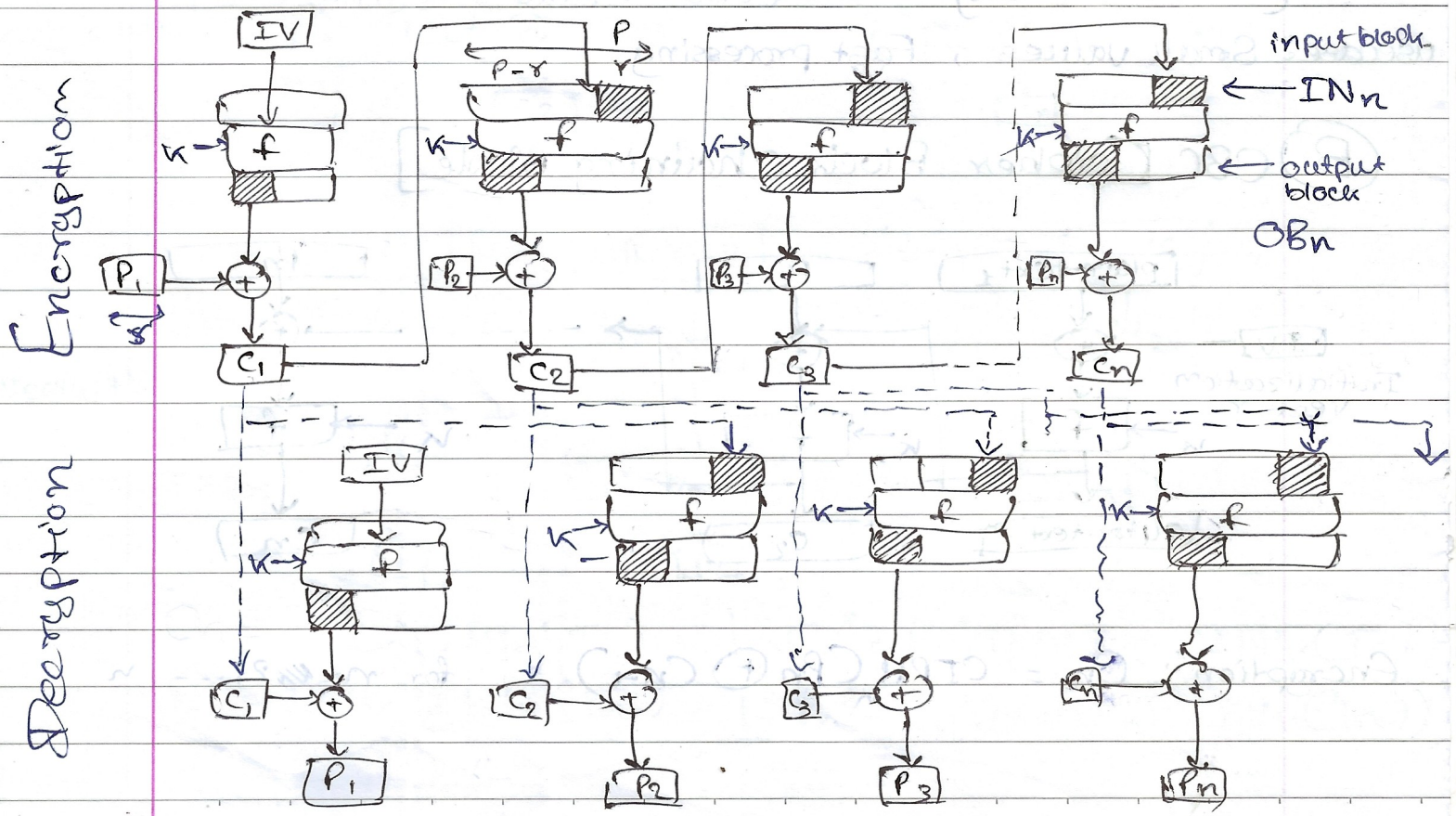
Decryption: $P = CIPH_K^{-1}(C_n) \oplus C_{n-1}$ $\quad n = 2, \ldots, n$

Good: Ciphertext depend on all prior plaintext [Dependency] Ciphers are deferent in each block so decryption is more difficult for attacker.

Bad: [Non-Parallel] cuait for one to finish before other can come [Error-Spreads], [Fixed Block Sizes]

Usecase: Secracy is important and longer processing time is not a concern.

(C) CFB [Cipher Feedback Mode]

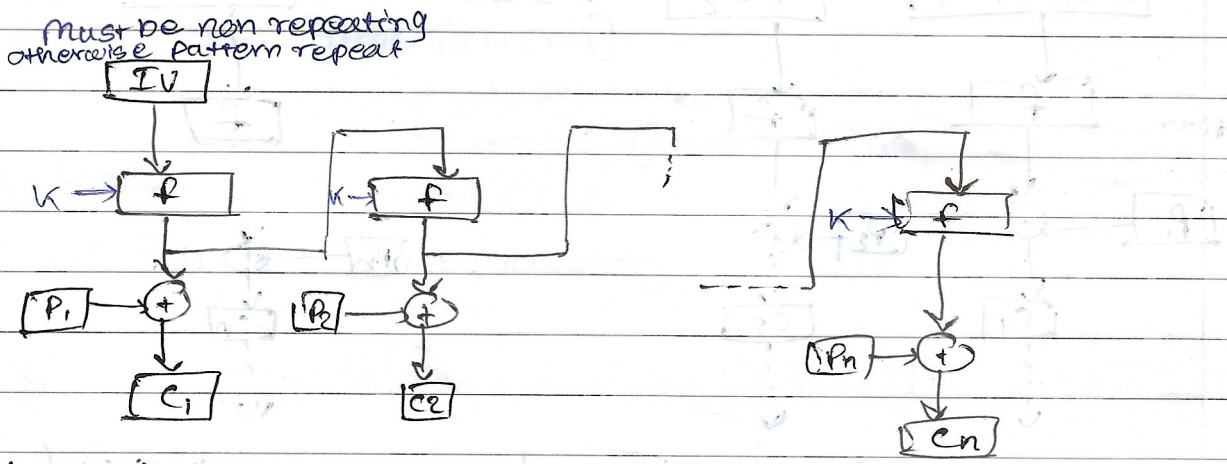


Enc
$IN_1 = IV$
$IN_n = LSB_{p-r}(IN_{n-1})$ or $C^{\#}_{n-1}$ $\quad n = 2 \text{ to } n$
$OB_n = CIPH_K(IN_n)$ $\quad \}\ n = 1 \text{ to } n$
$C^{\#}_n = P^{\#}_n \oplus MSB_r(OB_n)$

Dec
$IN_1 = IV$
$IN_n = LSB_{p-r}(IN_{n-1})$ or $C^{\#}_{n-1}$ $\quad n = 2 \text{ to } n$
$OB_n = CIPH_K(IN_n)$ $\quad \}\ n = 1 \text{ to } n$
$P^{\#}_n = C^{\#}_n \oplus MSB_r(OB_n)$

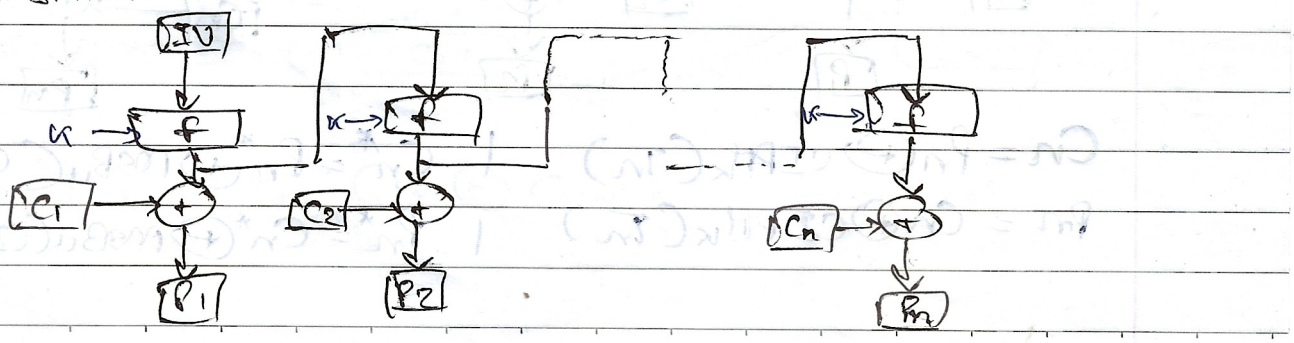
Good: [Dependency] [Difficult to decrypt in comparision]
No need for full blocksize length text to encrypt [No padding as well]
Bad: [Non-Parallel (slow)] [Error spreads]
Usecase: Same as CBC but also encrypts $r < p$ blocks

(D) OFB [Output Feedback Mode]



Encryption: $IN_1 = IV$
$IN_n = OB_{n-1}$
$C_n = P_n \oplus CIPH_K(IN_n)$
$C^*_n = P_n \oplus MSB_u(OB_n)$

DECRYPTION



$IN_1 = IV$

$IN_n = CIPH_k(IN_{n-1})$.

$P_n = C_n \oplus CIPH_k(IN_n)$.

$P_n^* = C_n^* \oplus MSB_u(CIPH_k(IN_{n-1}))$

Good: (Dependency) (Error Does not spread) (Never Needs Padding) (Hides all pattern - Keystream (pseudo Random))

Bad: (No-Parallel/slow) (cannot reuse IV) (Short cycle if loops)

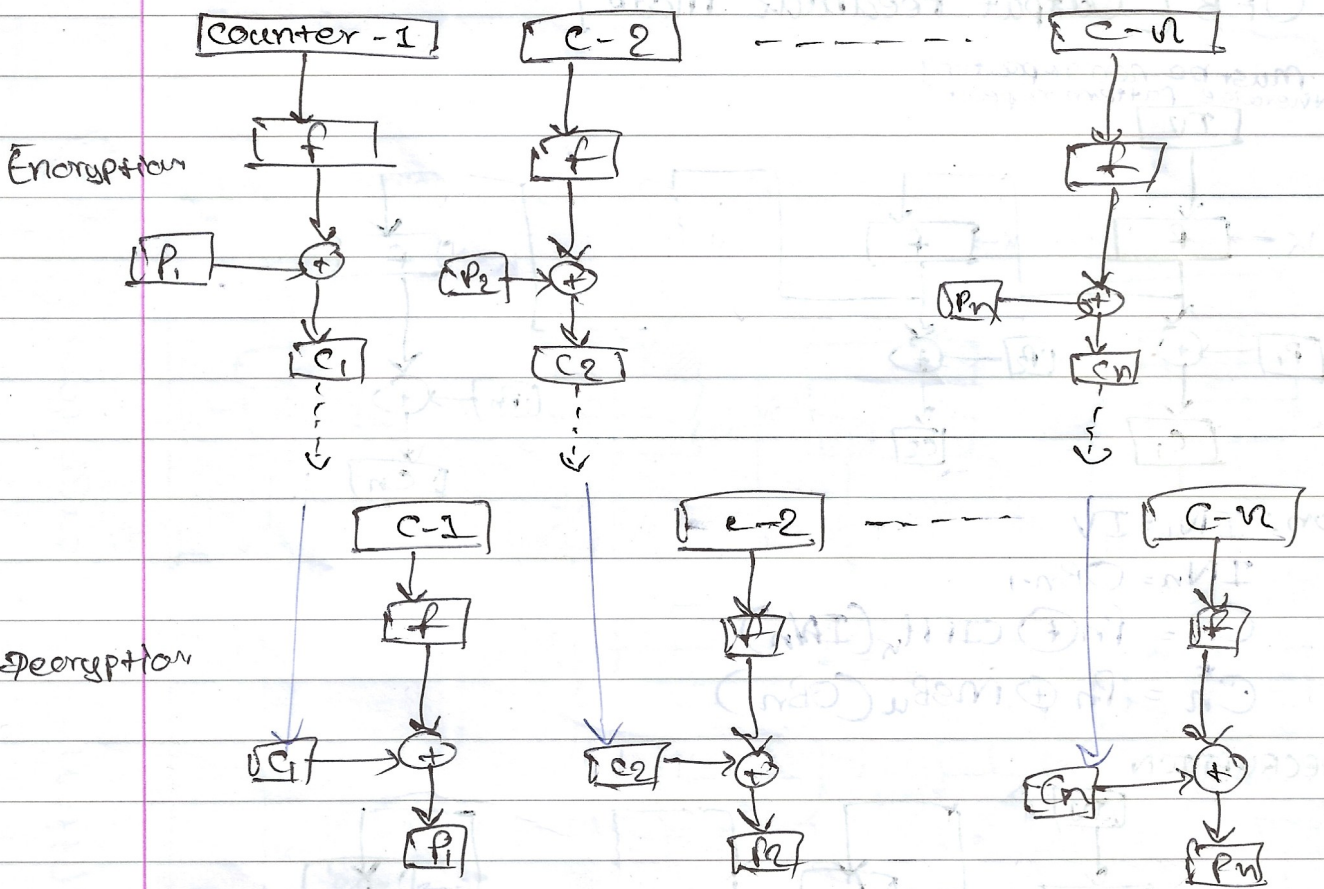
usecase: Noisy Communication channel - large data

(E) CTR [The Counter Mode]

→ Counter ① initialize [counter] value

Block |C| == |P| ② [counter++]

Last Block - appropriate bits taken



$C_n = P_n \oplus CIPH_k(I_n)$ | $C_n^* = P_n^* \oplus MSB_u(CIPH_k(I_n))$

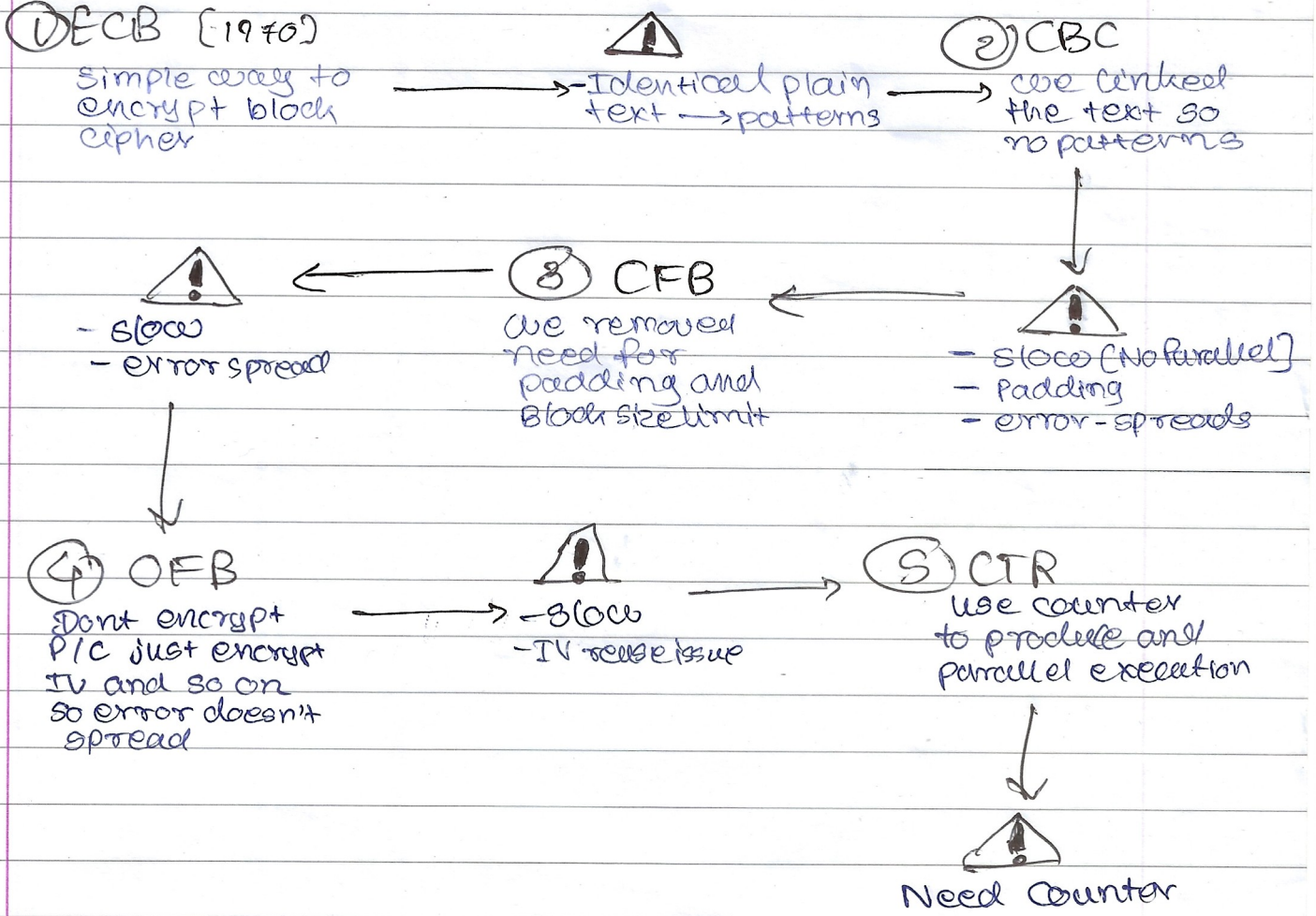
$P_n = C_n \oplus CIPH_k(I_n)$ | $P_n^* = C_n^* \oplus MSB_u(CIPH_k(I_n))$

Good: [Parallel Processing] [Different key] [error doesn't spread] [for Counter Encryption we can pre process] [Random access for any encryption block]

Bad: [Internal dependency missing]

Usecase: ATM, IPsec . most usefull outof all modes.

→ Growth Path & Differentiation



Paper:

- NIST SP 800-38A Recommendation for Block Cipher modes of operation: Methods and Techniques