IT-21004

Cryptography and Cyber Law

Assignment

Afsana Akter Mim

IT-21004

Modes of operation and RC5 - Block Diagram and Java Implementation and output.

Modes of operation :-

Block cypher encrypt data in fixed size blocks (64 or 128 bits). But in real application data in often much larger. So we use modes of operations to securely process large data by using a block cipher repeatedly.

Afsana
IT-21004

Common modes:-

ECB - Electronic Codebook
CBC - Chipher Block chaining
CFB - chipher feedback
OFB - output feedback
CTR - Counter

Description:-

ECB - Each block is encrypted independently not secure for patterns.

CBC :- XORs each plaintext block with previous ciphertext block before encryption.

CFB :- Converts Block cipher into a self synchronizing stream cipher.

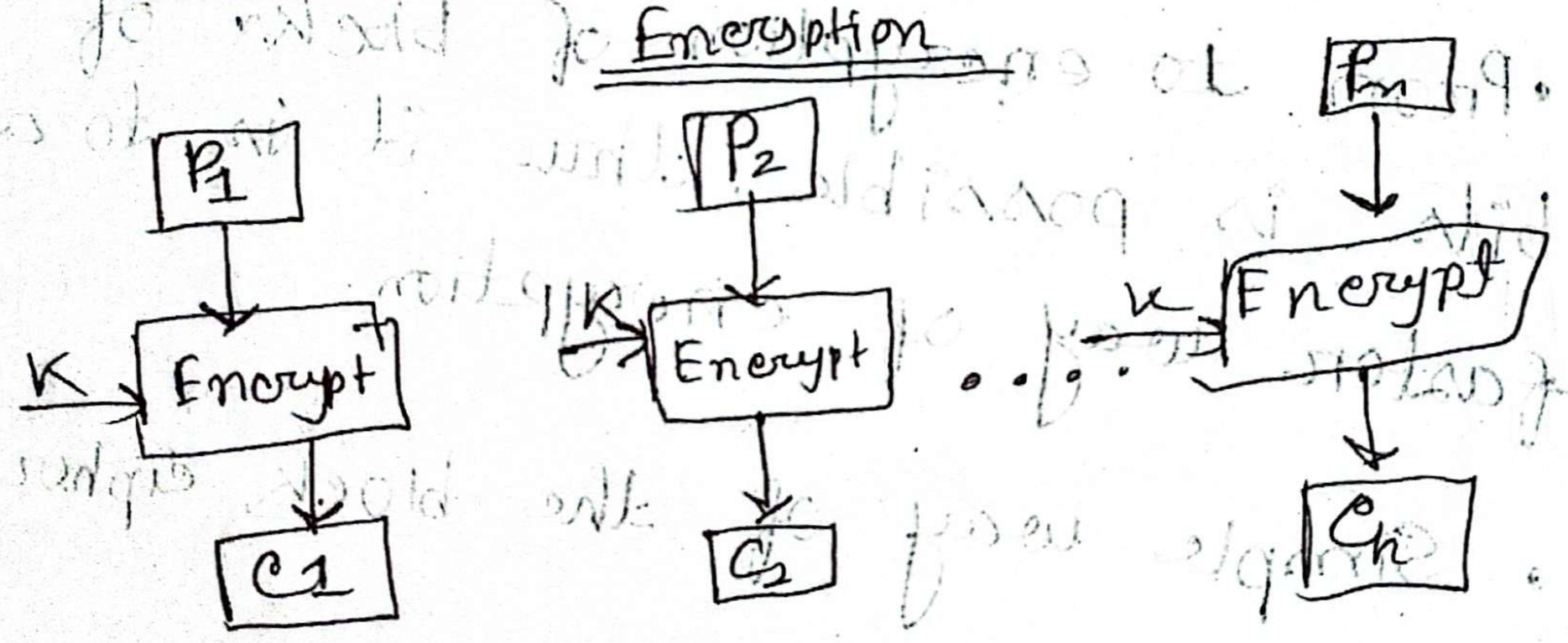
Afsana
IT-21004

OFB:- Turn block cipher into a synchronous stream cipher.

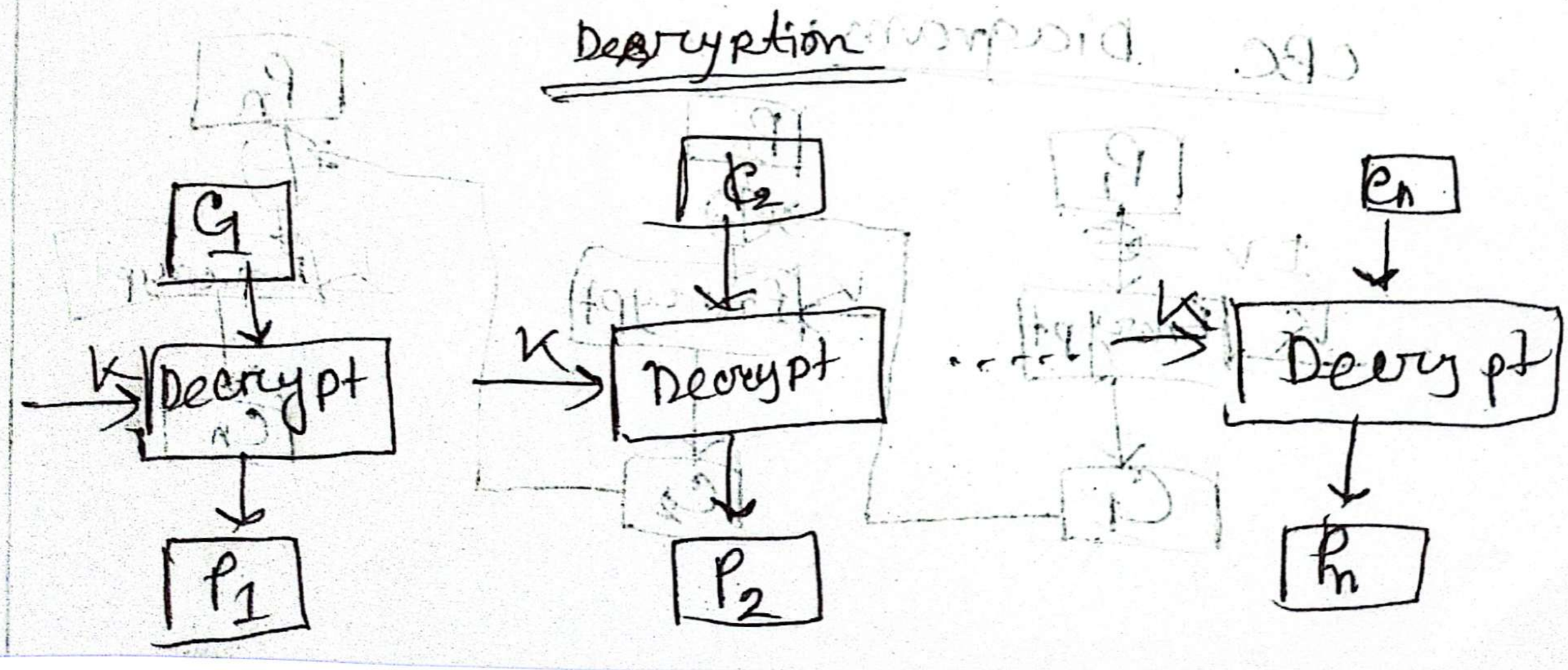
CTR:- Uses a counter that gets encrypted and XORed with plaintext. Fast and parallel.

The procedure of ECB is illustrated below

Encryption



Decryption



Afsana
IT-21004

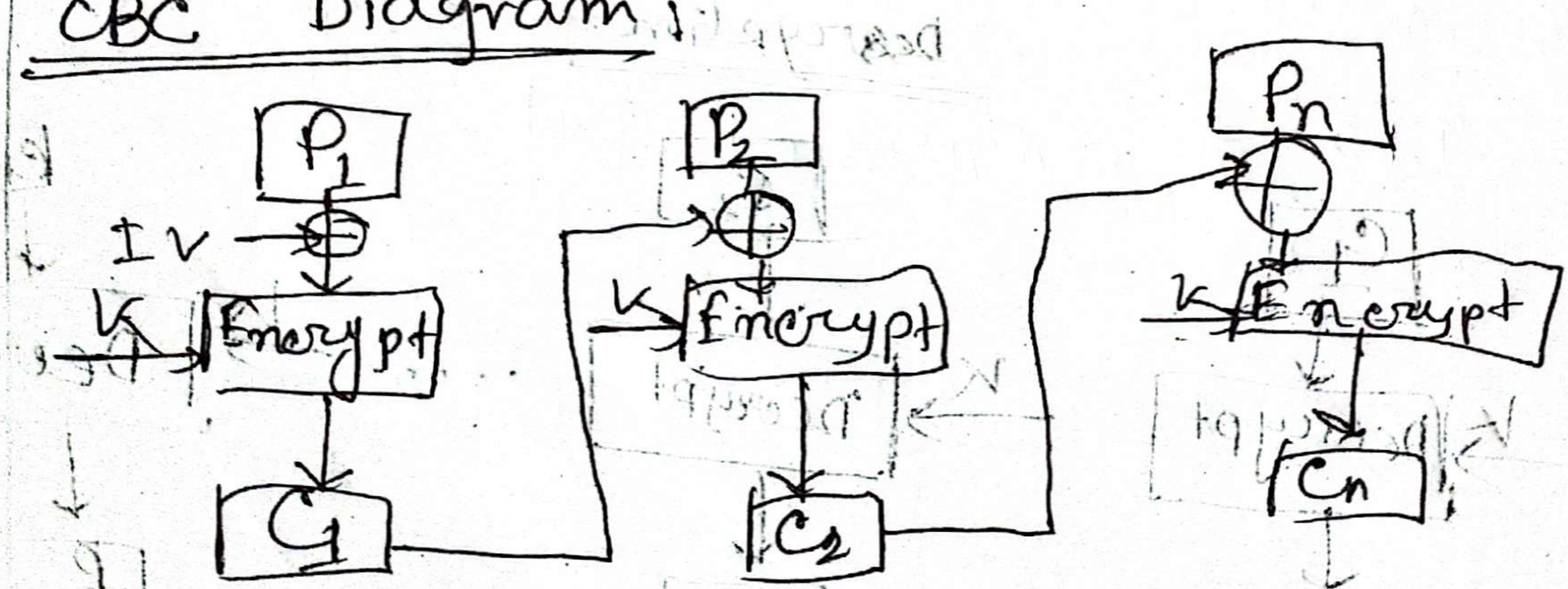
Advantages of ECB

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of ECB

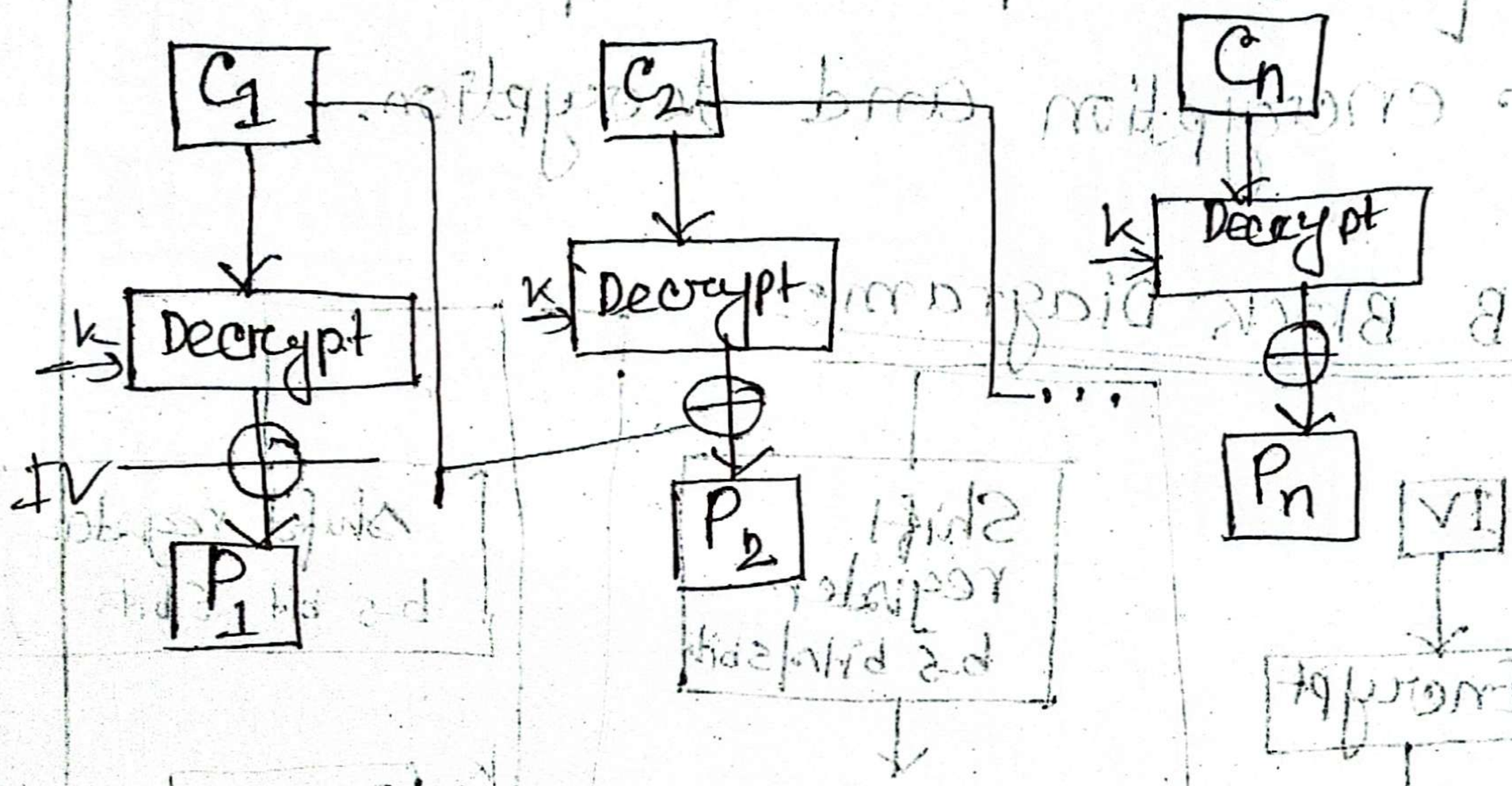
- Prom to encryption of blocks of bits is possible, thus it is to a faster way of encryption.
- Simple way of the block cipher.

CBC Diagram:



IT-21004
Afsana

Decryption:-



Advantages of CBC :-

- CBC works well for input greater than b bits.
- CBC is a good authentication mechanism
- Better resistive nature towards cryptanalysis than ECB
- More secure than ECB as it hides patterns.

Afsana
IT-21004

Disadvantages:-

- Requires the previous ciphertext block for encryption and decryption.

CFB Block Diagram:-

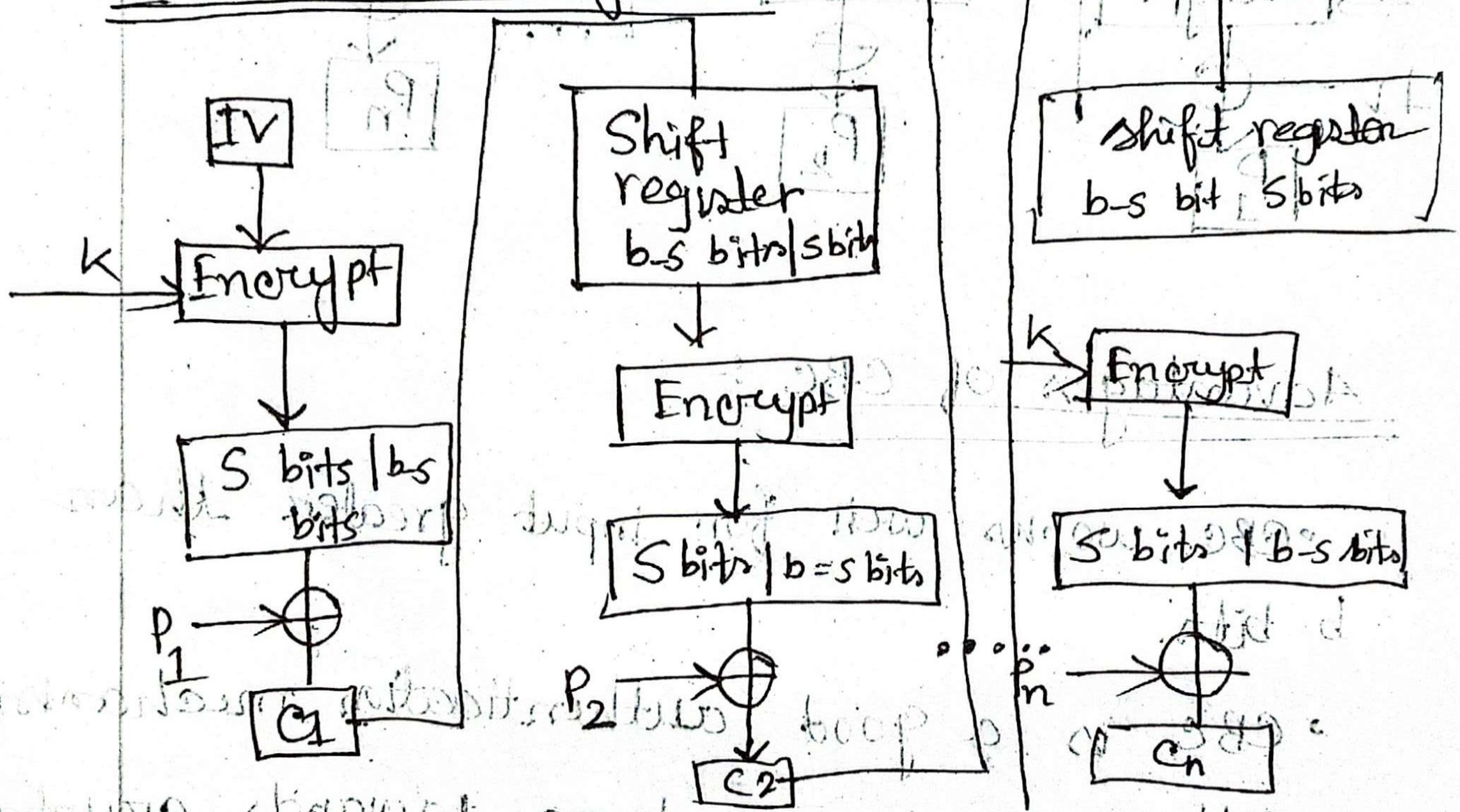
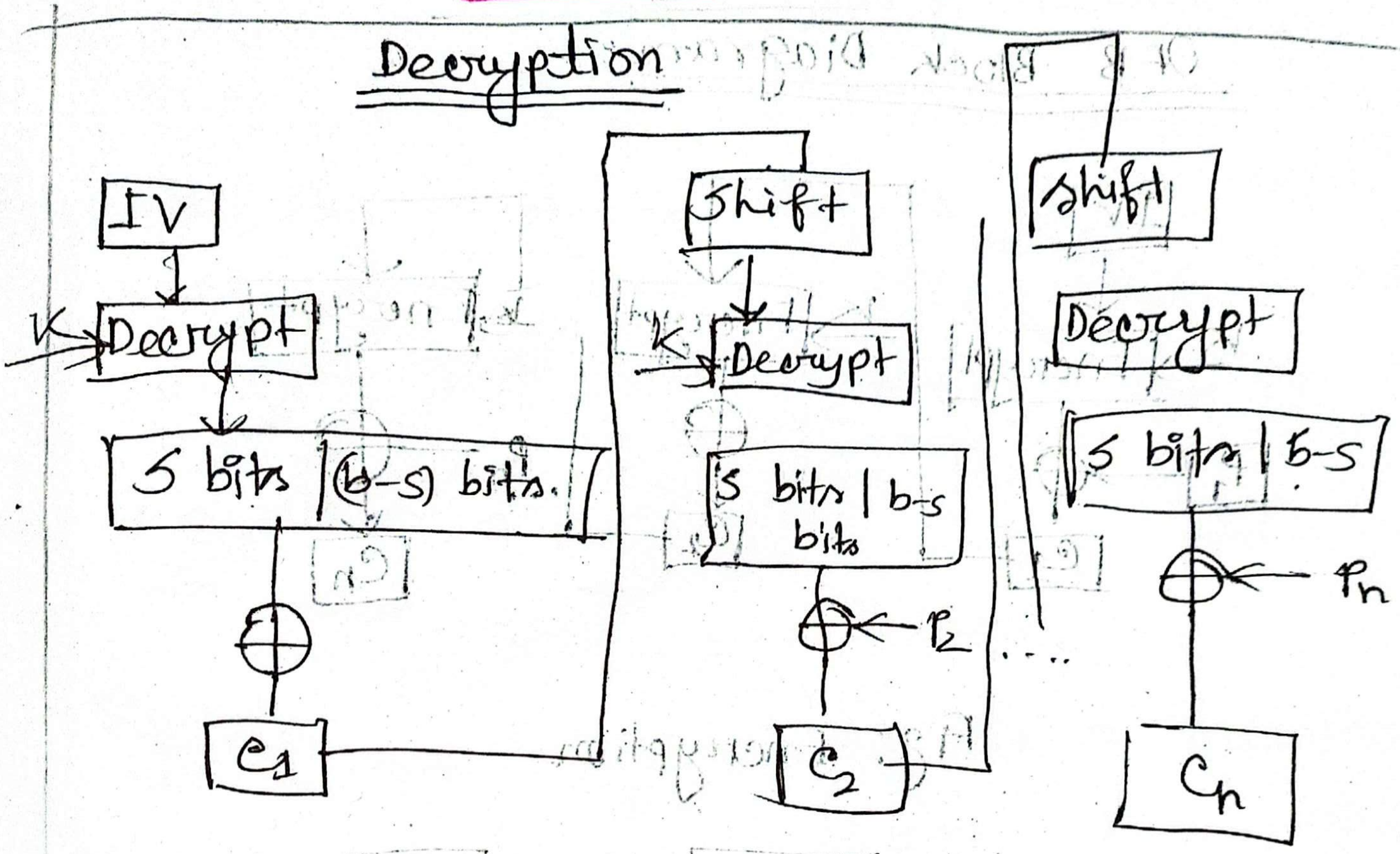


Fig: Encryption of CFB

Afsana
IT-21004

Decryption



Advantages of CFB :-

- Since there is some data loss due to the case of shift register, thus it is difficult for applying cryptanalysis.

Disadvantages :-

- Slightly more complex and propagate errors.

Afsana
IT-21004

OFB Block Diagram:

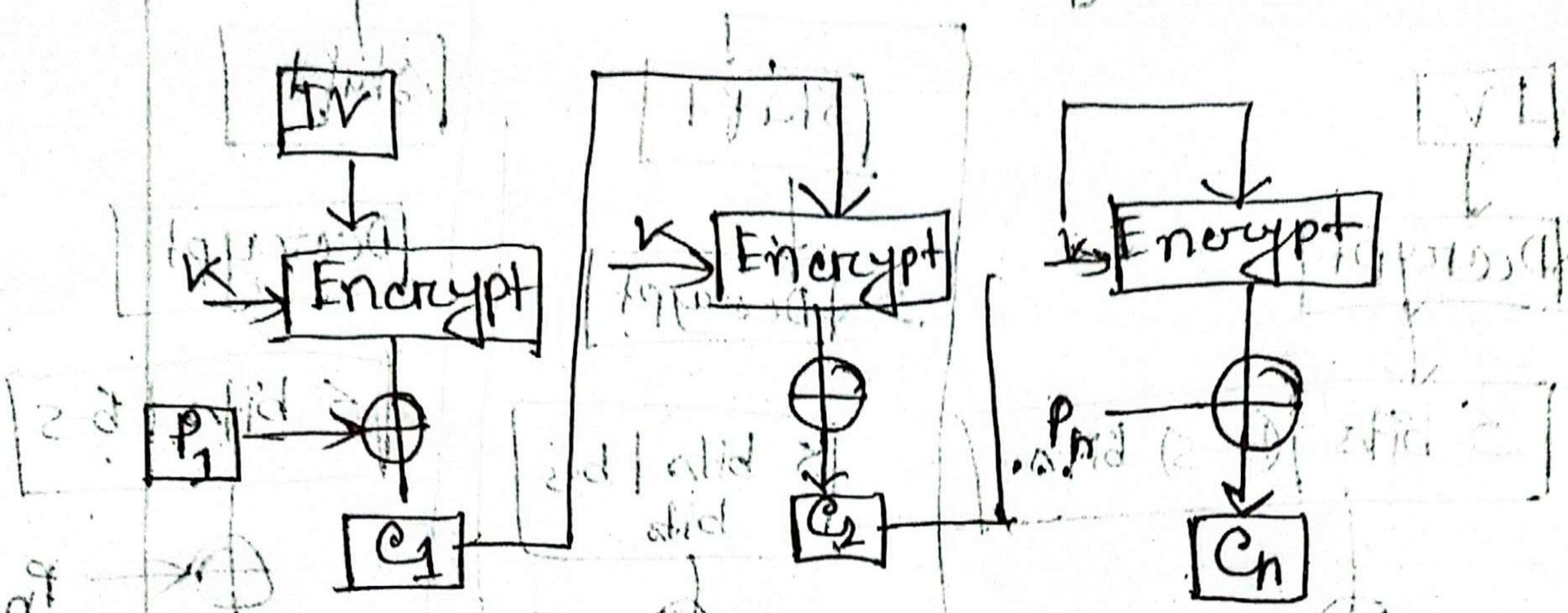


Fig: Encryption

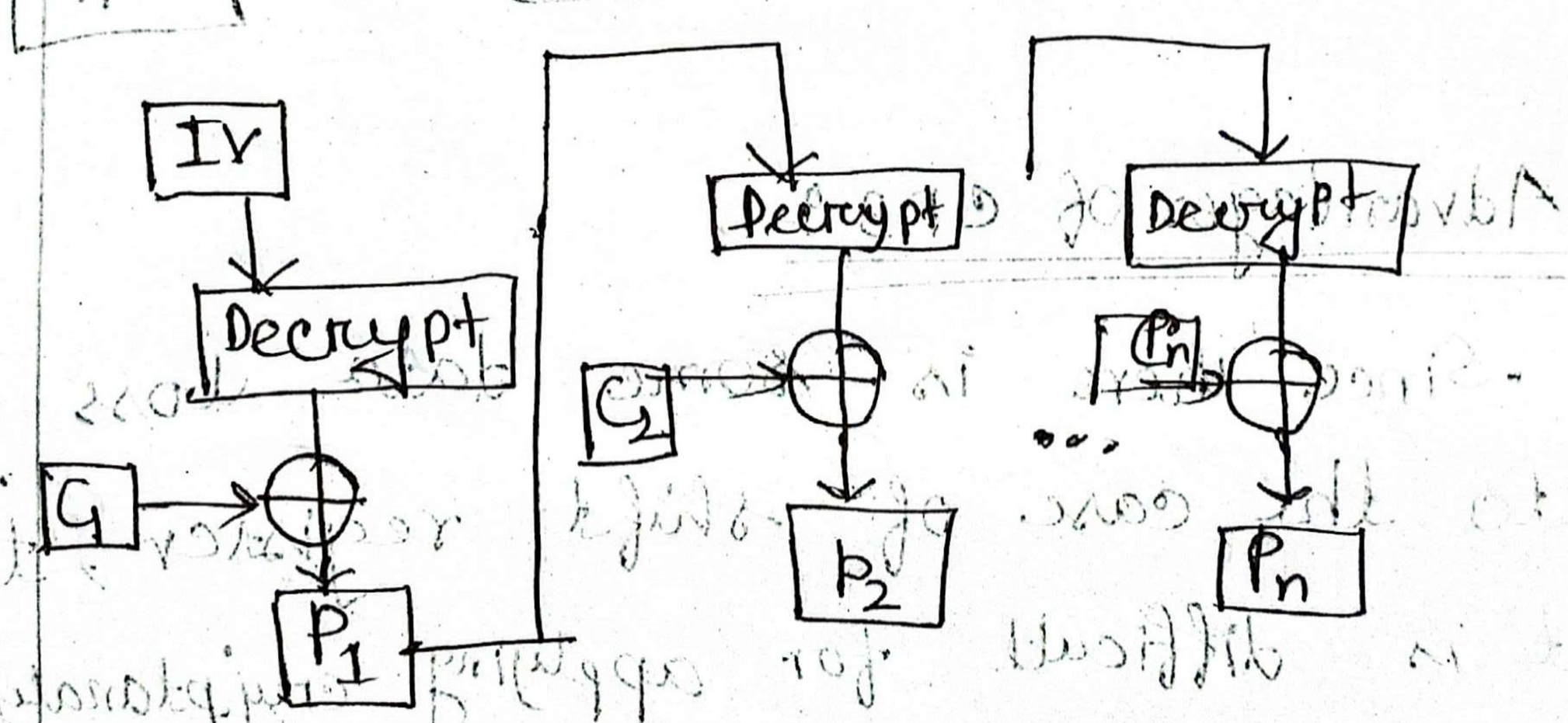


Fig: Decryption.

Afrana
IT-21004

Advantages of OFB:

- In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit error.

Disadvantages of OFB:

- It is more susceptible to a message stream modification attack than CFB
- If the key stream is refused, security is compromised.

Afsana
IT-21004

Block Diagram of CTR:

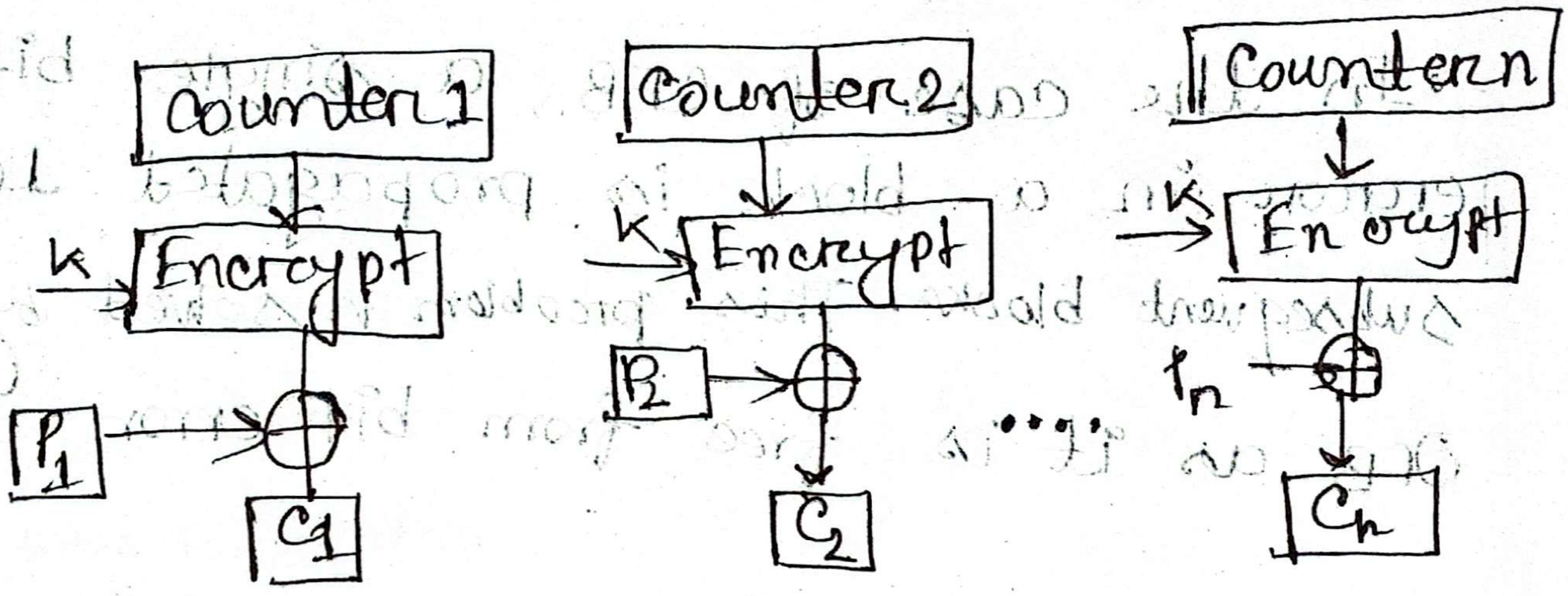


Fig: Encryption

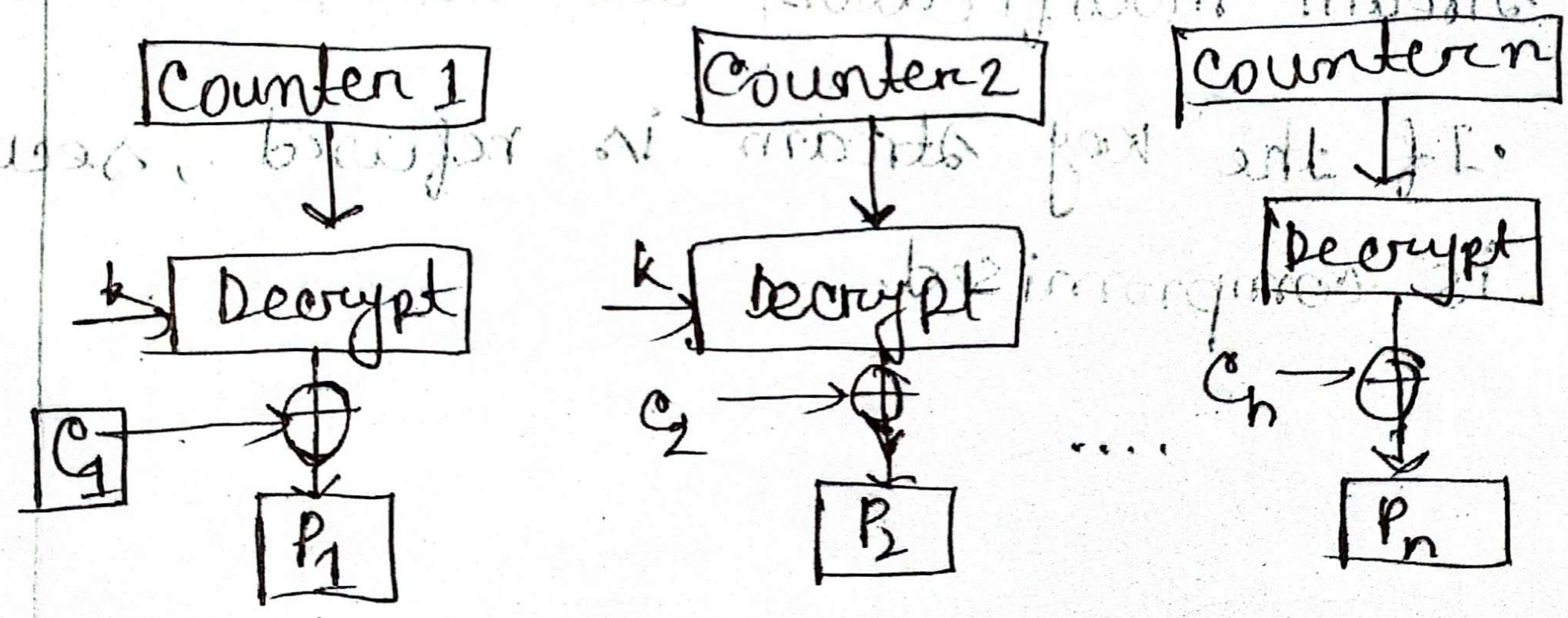


Fig: Decryption

Afsana
IT-21004

Advantages of Counter (CTR):-

- Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plain text can map to different ciphertext.

Disadvantages of counter (CTR):-

- The fact that CTR mode requires a synchronous counter at both the transmitter and the receiver is severe drawback. The recovery of plaintext is inaccurate when synchronous is lost

Afsana
IT-21004

Introduction of RC5

RC5 is a fast, simple and secure symmetric key block cipher designed by Ron Rivest in 1994.

Key Features:

- Parameterizable
  - → Word size (32 bits)
  - → Number of round (12)
  - → Key length (8 bytes)
- Use
  - → Bitwise operation : XOR, shift
  - → Modulation addition

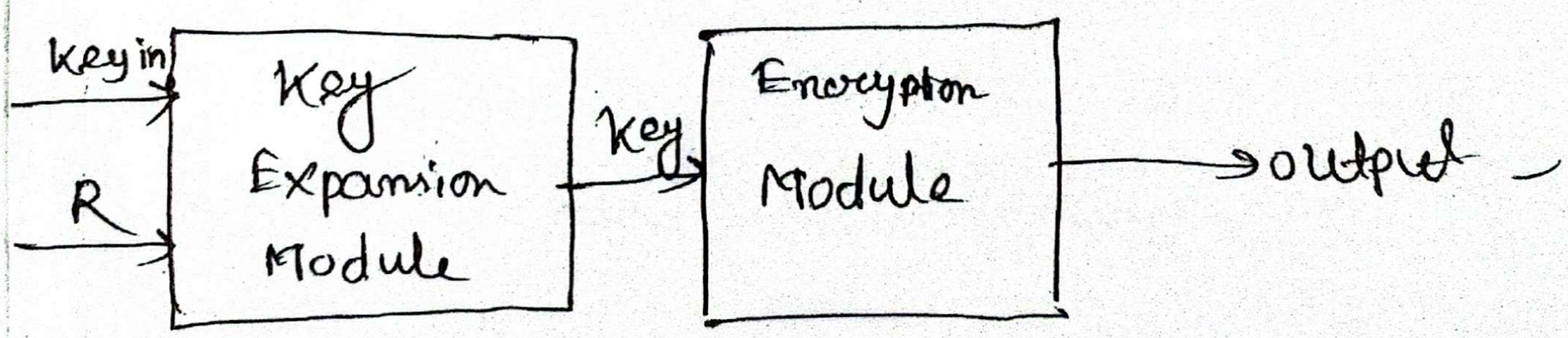
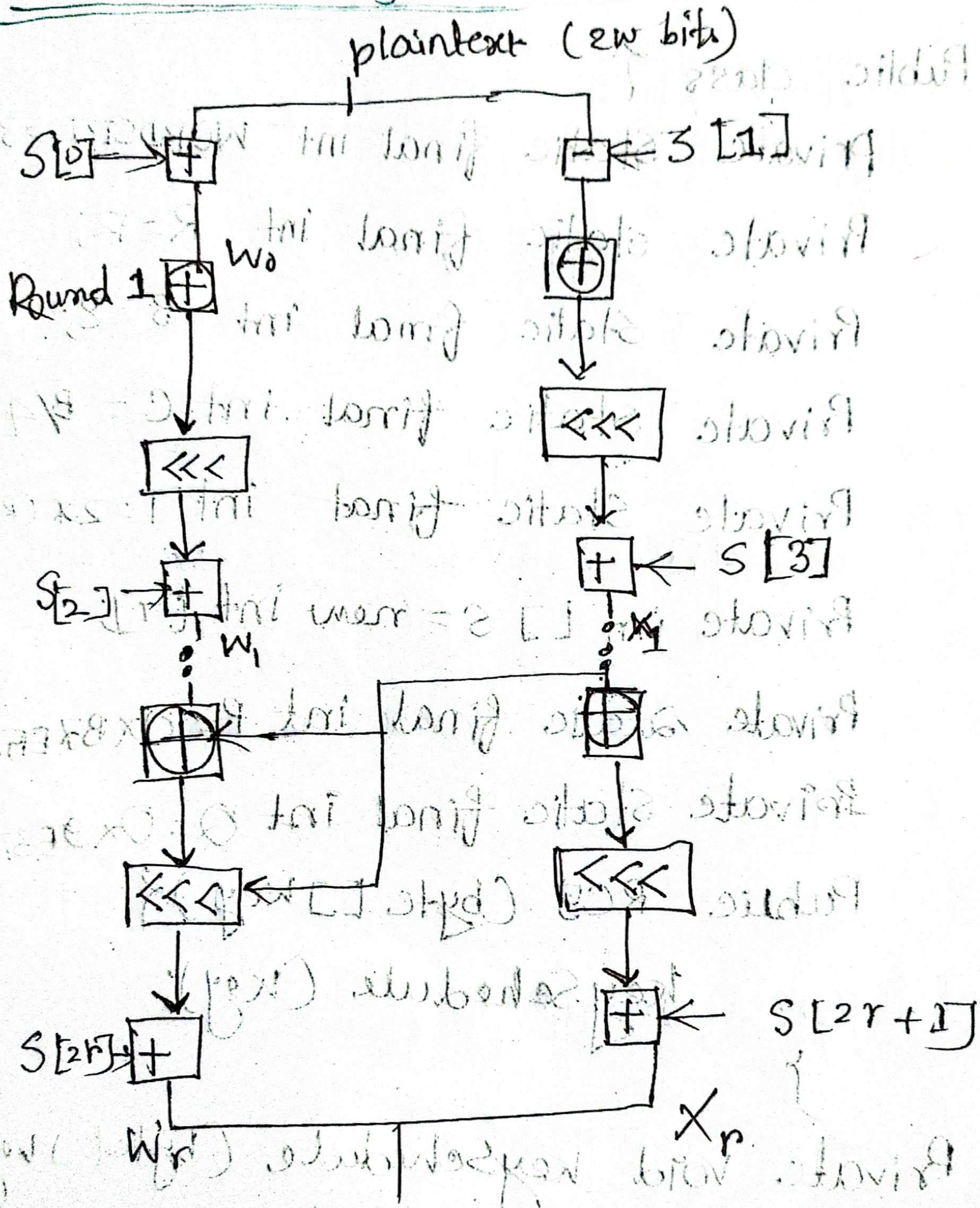


Fig: RC5 Encryption Block Diagram

Afsana
IT-21004

RC5 Block Digram :-



Afsana
21001

Java Implementation

```
Public class {
    private static final int WORDSIZE = 32;
    Private static final int R=12;
    Private static final int B=8;
    Private static final int C = B/4;
    Private static final int T=2x(R+1);
    Private int [] S = new int [T];
    Private static final int P=0xB7E5163;
    Private static final int Q=0x9E3779B9
    Public RC5 (byte [] key){
        keySchedule (key);
    }
    Private void keyschedule (byte[] key){
        int [] L = new int[C];
        for (int i=0; i<B; i++){
            L[i/4] = (L[i/4] << B)+ key [i] 20xFF
    }
```

Afsana
IT-2100A

```
S[0]=P
for (int i=1; i<T; ++i){
  S[i]=S[i-1]+Q;
}
int A=0, B=0, i=0, j=0;
for (int k=0; k<3*T; ++k){
    A=S[i]=Integer.rotateleft(S[i]+A+B),3);
    B=L[j]=Integer.rotateleft(C[j]+A+B,
                                  (A+B));
    i=(i+1)%T;
    j=(j+1)%c;
}
}
public int[] Encrypt(int[] pt){
  int A=pt[0]+S[0];
  int B=pt[1]+S[1];
  for (int i=1; i<=R; ++i){
    A=integer.rotateleft(A^B, B)+S[2*i];
    B=integer.rotateleft(B^A, A)+S[2*i];
}
```

Afsana
II-21004

```
return new int[] {A, B};
}

Public int[] decrypt(int[] ct) {
    int B = ct[1];
    int A = ct[0];

    for (int i = R; i >= 1; i--) {
        B = Integer.rotateleft(B ^ S[2*i+1], A) ^ A;
        A = Integer.rotateleft(A ^ S[2*i], B) ^ B;
    }

    A = S[0];

    B = S[1];

    return new int[] {A, B};
}
```

Afsana
II-21004

```
Public static void main (String[] args){
byte [] key = "password".getBytes ();
RC5 rc5 = new RC5 (key);
int [] pt = {0x12345678, 0xabcdefg9};
int [] ct = rc5. encrypt (pt);
System.out.printf ("Encrypted: %08x %08x\n",
ct[0] ct [1]);
int [] dt = rc5. decrypt (ct);
System.out.print ("Decrypted: %08x %8x
\n", dt. [0], dt [1]);
}
}
```

Afsana
IT-21007

Sample Output:

Encrypted: 7f93d8c2 1423ba29

Decrypted: 12345678 9abcdefg