Assignment topic:

Mode of operational and RC5 - block diagram and java implementation and output.

Mode of operation:

Block ciphers encrypt data in fixed sized blocks (64 or 128 bits). But in real application data is often much longer. So, we use modes of operation to sequrly process longer data by using a block cipher repeatedly

Common modes -

- ECB — Electronic Codebook
- CBC — Cipher Block chainnig
- CFB — Cipher 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 – Convert block cipher into a self-synchronizing stream cipher.

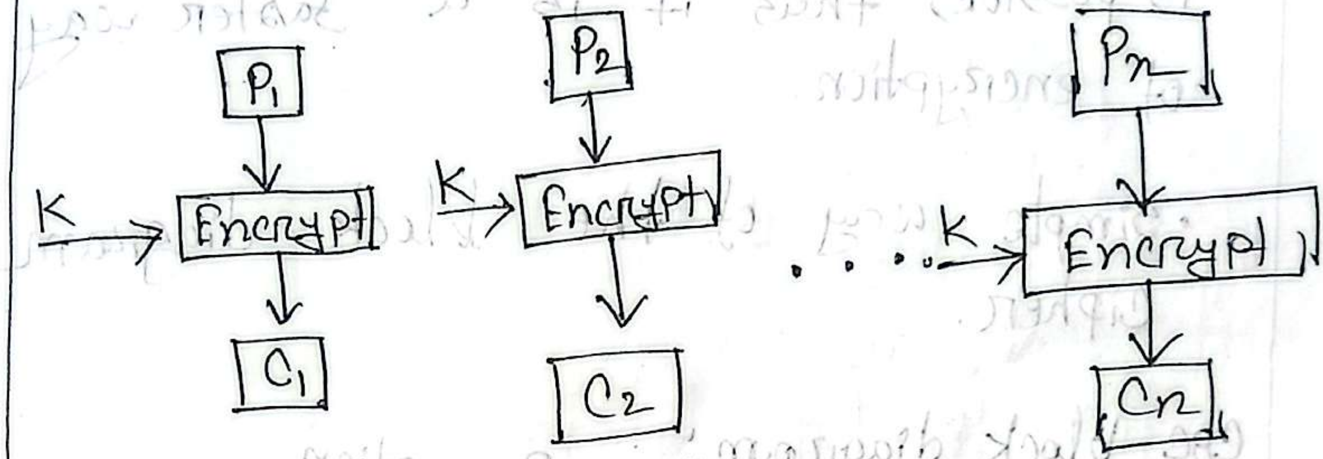
OFB:- Turns blocks cipher into a synchronous stream cipher.

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

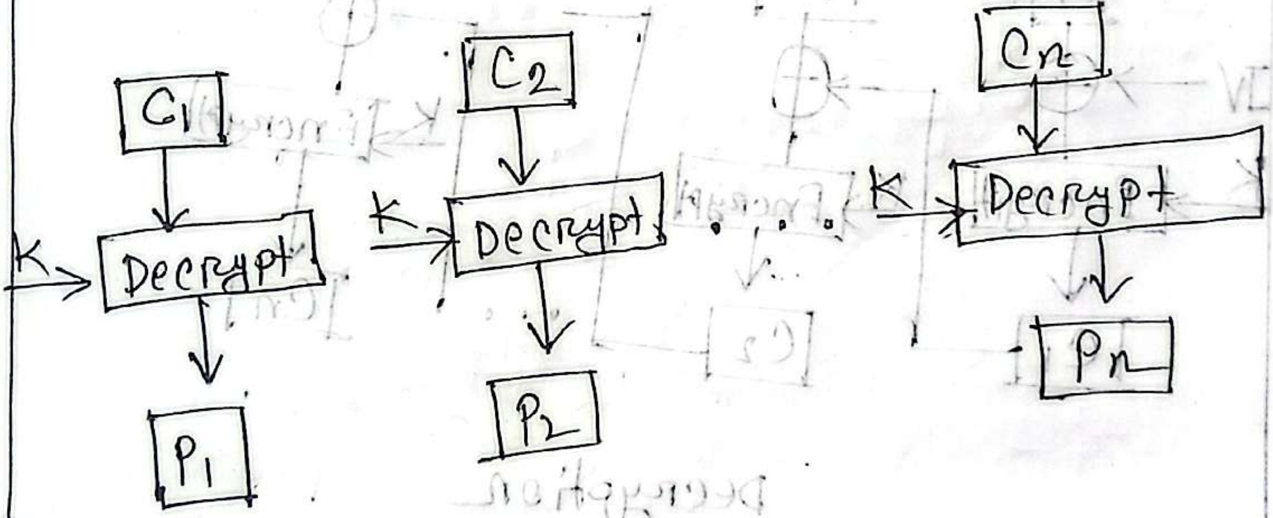
Note:- Among then, CBC and CTR are the most widely used due to their security and efficency.

The procedure of ECB is illustrated below:

Encryption



Decryption



Advantages of ECB:

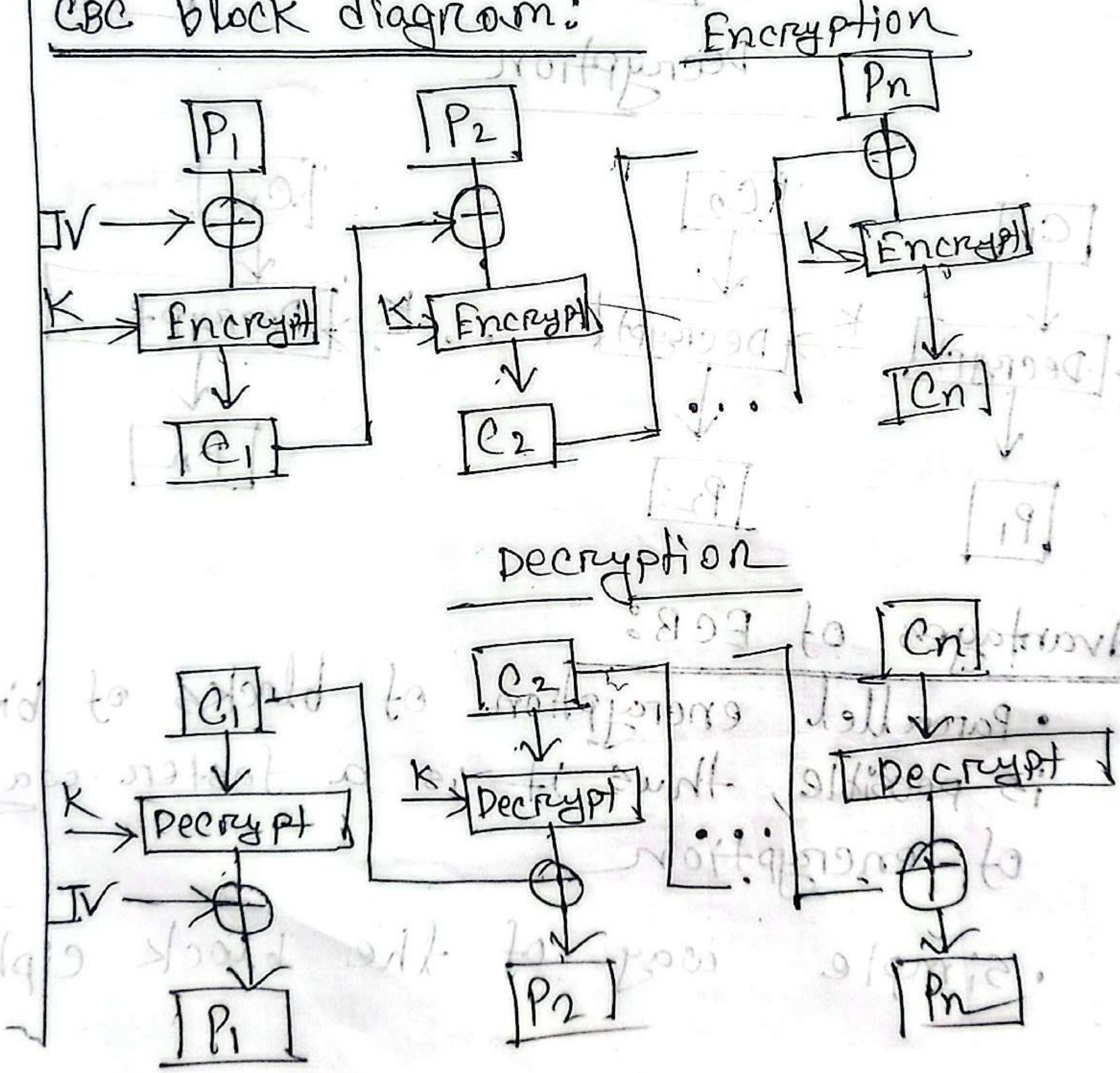
- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption
- simple way of the block cipher

Disadvantages of ECB:

- Prone to eryption of block of bits is possible, thus it is a faster way of encryption.

- Simple way of the block diagram cipher.

CBC block diagram:



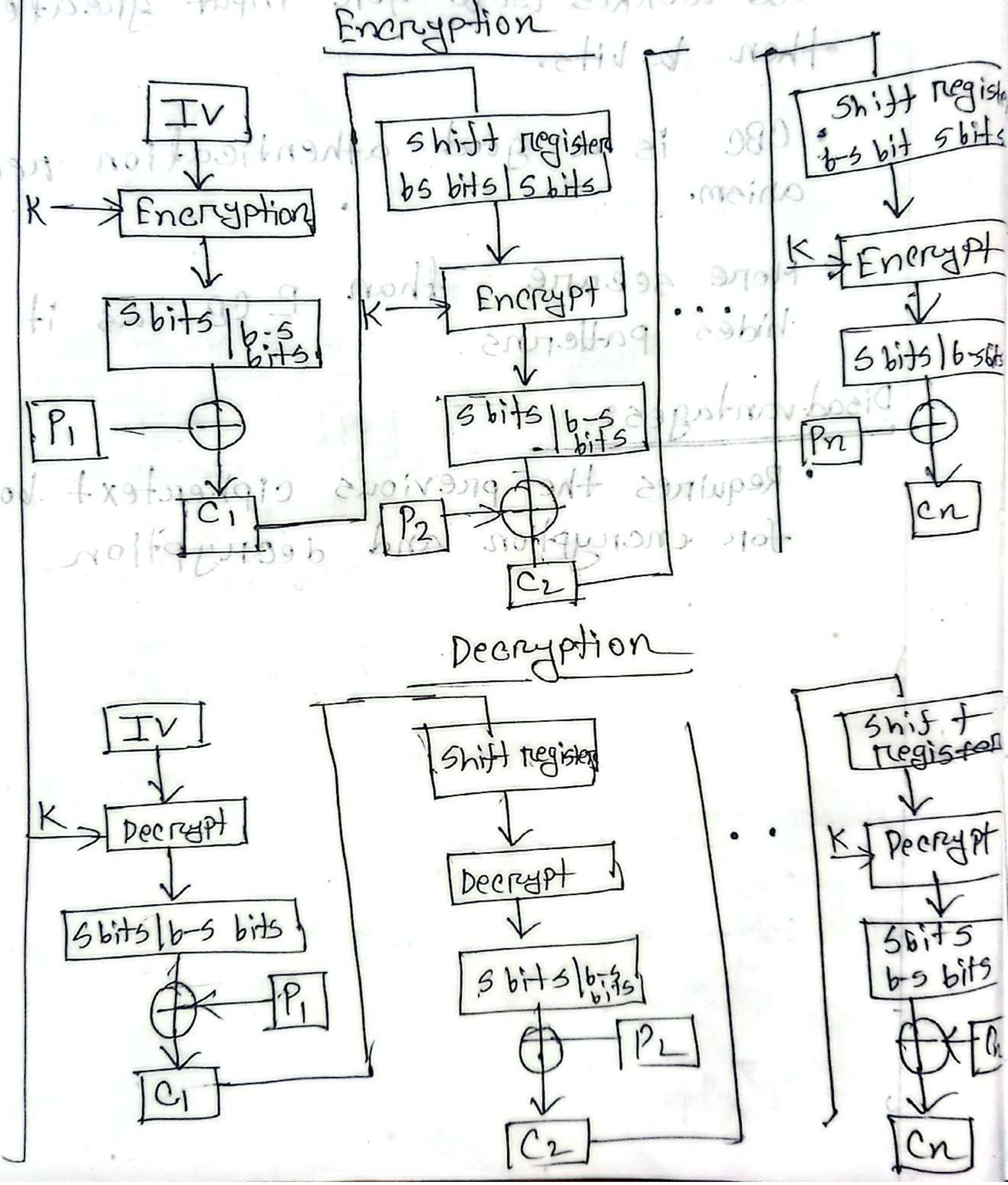
Advantage of CBC:

- CBC workes well for input greater then b-bits.
- CBC is a good athentication mechanism.
- More secure than ECB as it hides patterns.

Disadvantages:

- Requires the previous ciphertext book for encryption and decryption

CFB block diagram:



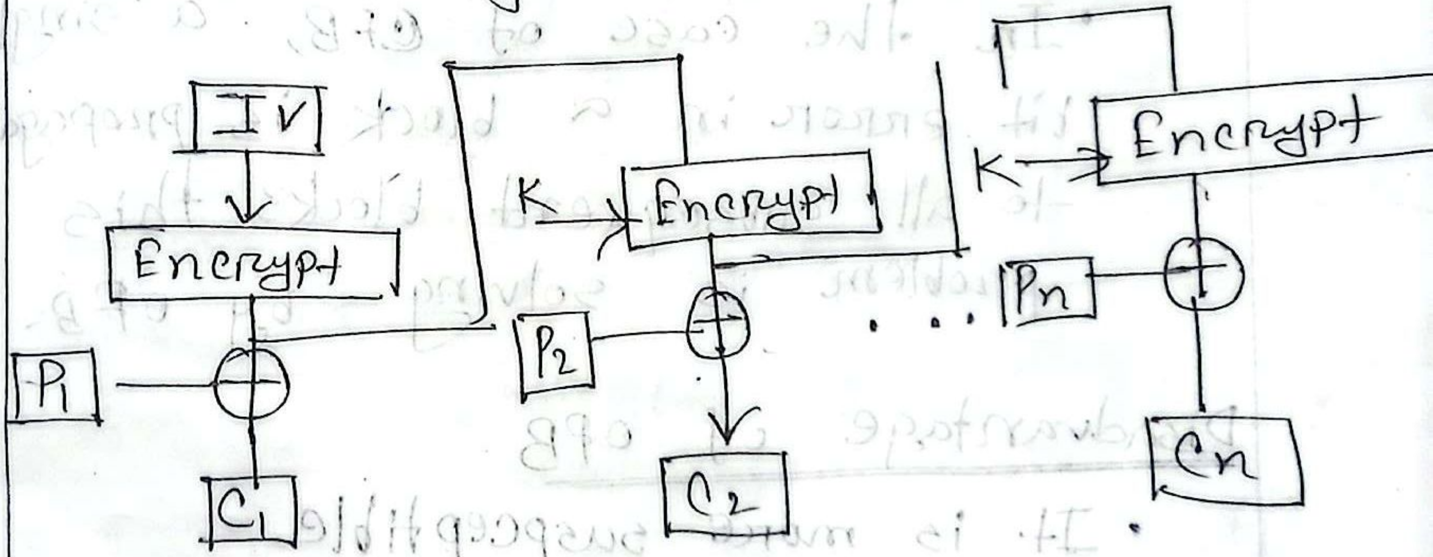
Advantage of CFB:

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

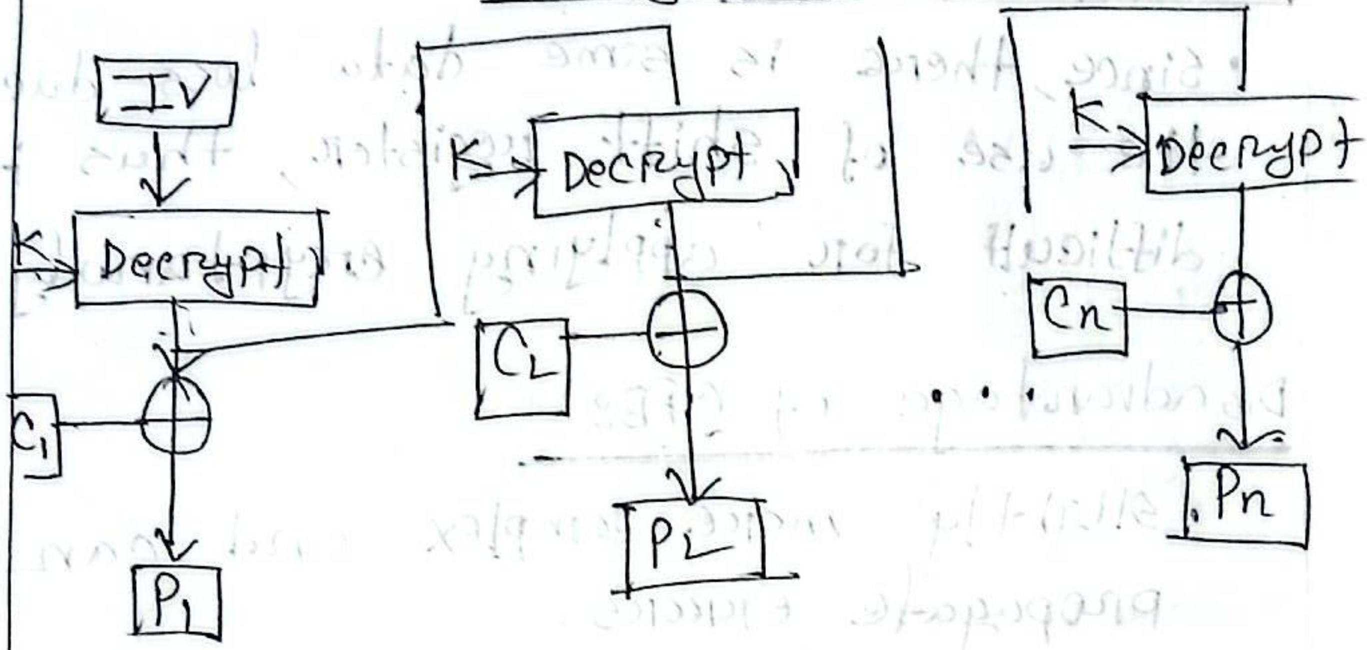
Disadvantage of CFB:

- slightly more complex and can propagate errors.

OFB Block diagram: Encryption



Decryption



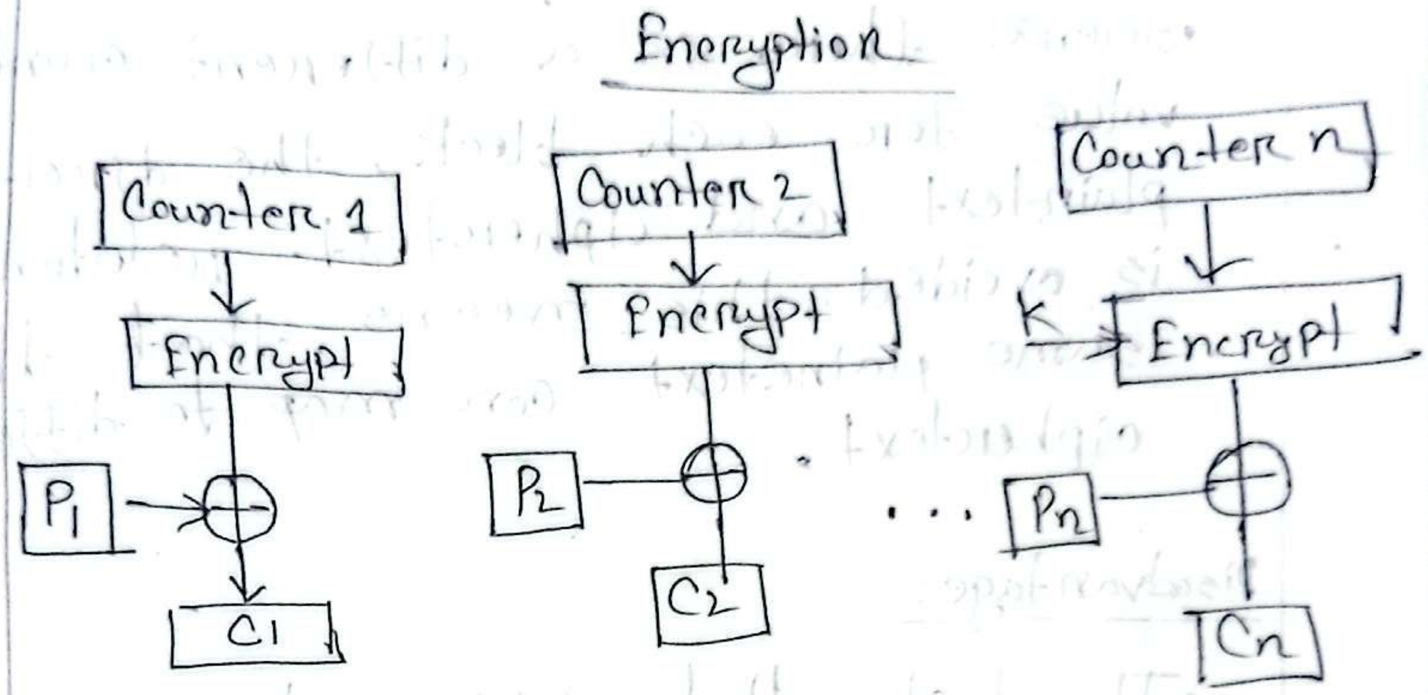
Advantage of OFB:

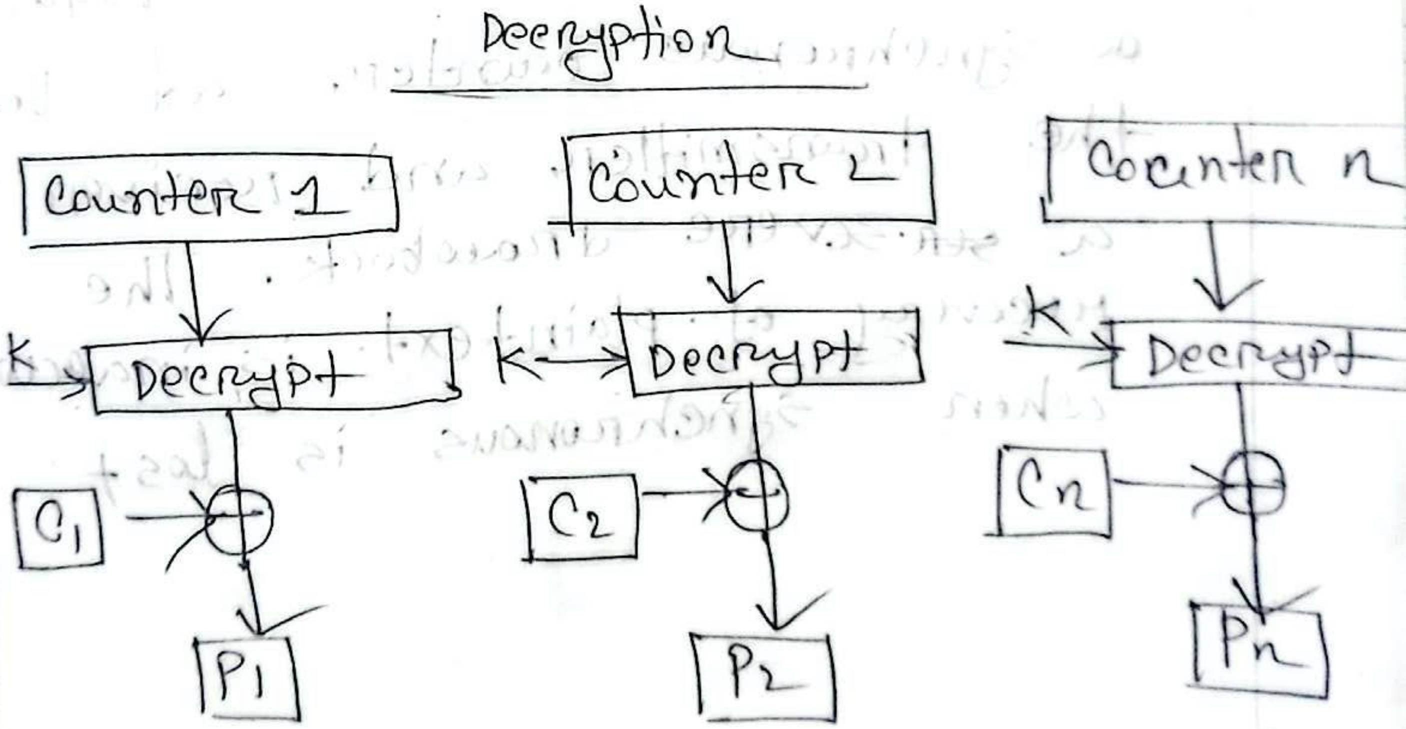
- In the case of OFB, a single bit error in a block is propagate to all subsequent blocks this problem is solving by OFB.

Disadvantage of OFB

- It is more suspceptible
- If the keystream is refused, secueity is compromised

Block diagram of CTR:





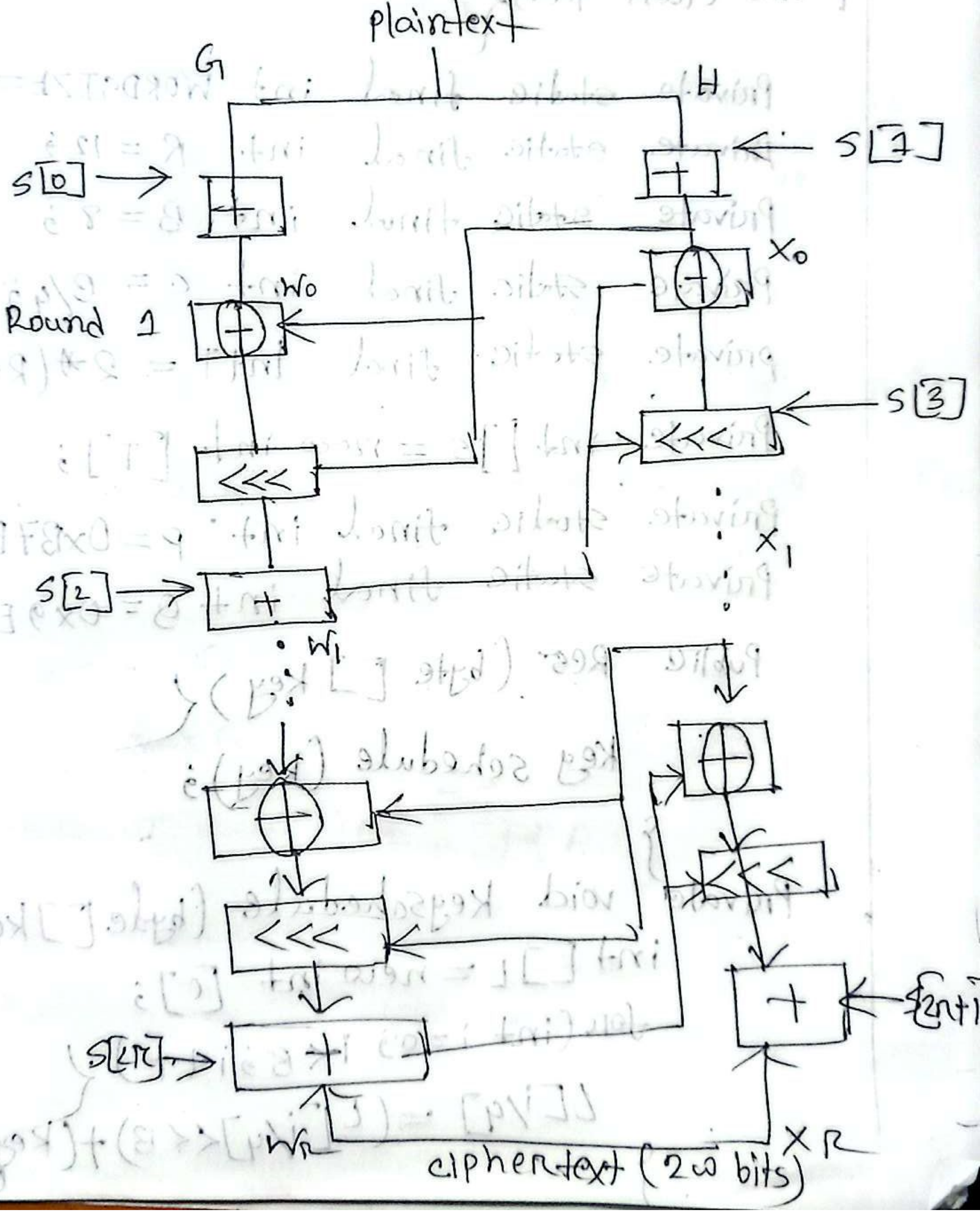
Advantage:

- science there is a different acounter value for each block, the direct plaintext and ciphertext relationship is avoided. this means that the same plainetext can map to differen ciphertext.

Disadvantage:

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

RC5 block diagram:



Java implementation:

```
public class RC5{
    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 IntT = 2*(R+1);
    Private int []s = new int [T];
    Private static final int p = 0xB7E15163;
    Private static final int Q = 0x9E3779B9;
    Public RC5 (byte [] key){
        Key schedule (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]& 0xFF
        }
```

```
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.rotateRight(B-s[2*i+1], A)^A;
        A = Integer.rotateRight(A-s[2*i], B)^B;
        }

A - = s[0];
B - = s[1];
return new int [] {A,B}
}
Public static void main(String [] args)
{
```

```
byte [] key = "Password" get Bytes();
RC5. rc5 = new RC5(key);
int [] pt = {0x 12345978 , 0x9abcdef0};
int [] ct = rc5. encrypt (ef);

Sytem. out. Printf ("Encrypted: %08X
  %08X\n", ct[0], ct[1]);

system. out. print ("Decrypted : %08X
  %08X\n" , dt[0], dt[1]);

}
}
```

Sample Output:

```
Encrypted: 7f93d8c2 1423ba29
decrypted: 12345678 9abcdef0.
```