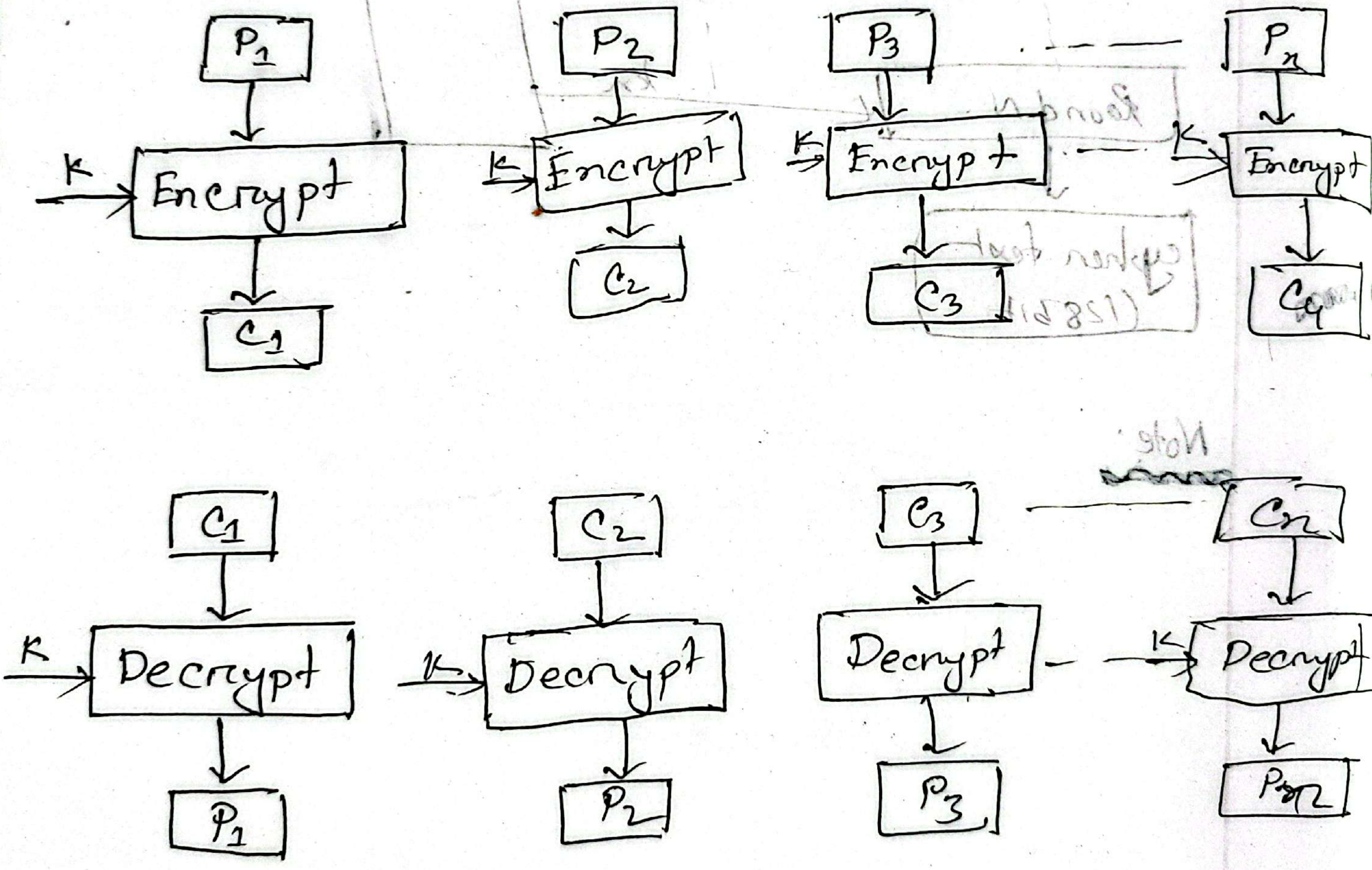
Assignment

ECB (Electric codebook) : In an, electric codebook each block of bits of plain text is encoded independently with the same key.

Block Diagram:



Java Implement'

```
import javax.crypto.cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.secret key;
import javax.crypto.spec.secretkey spec;
import javax.util.Base64;
public class ECBMode Example{
 //Generate a sample AES key (128 bit)
  public static Secretkey generateAE
```

Advantages of ECB:

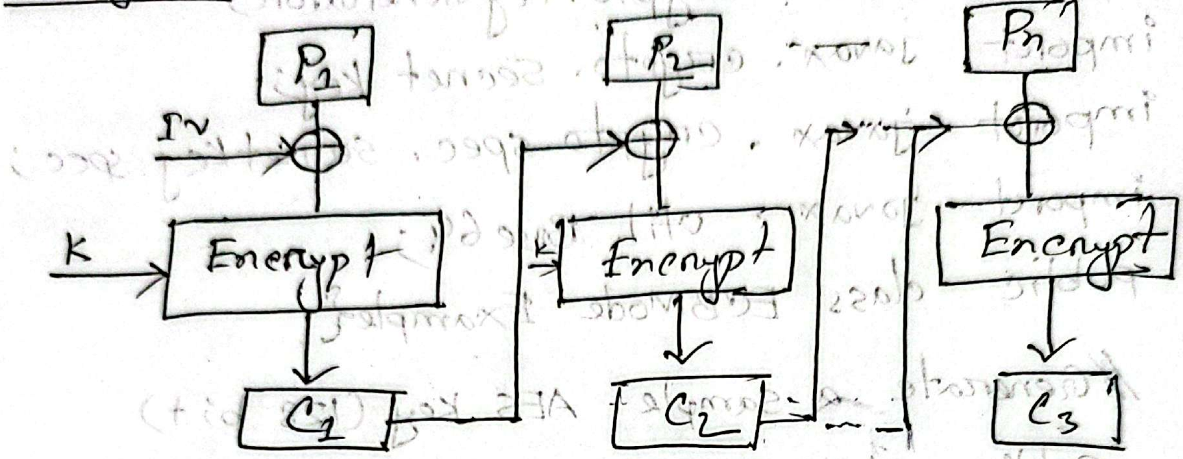
- Parallel encryption of block bits is possible.
- Simple way of the block cipher.

Disadvantages of ECB:

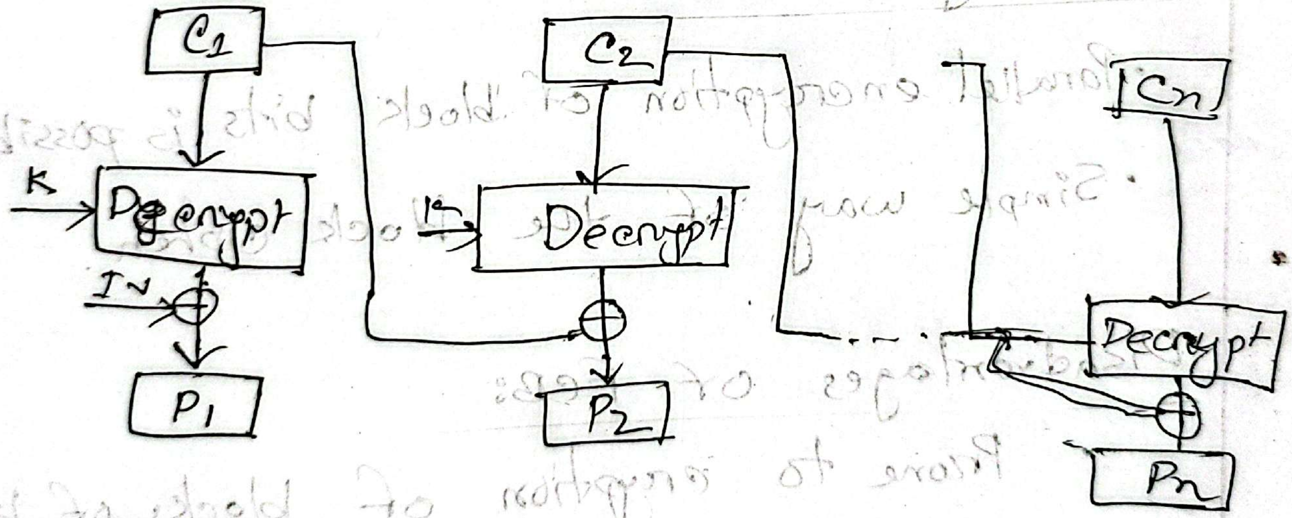
- Prone to encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

CBC - Block Diagram:

Encryption:



Decryption:



Advantages of CBC:

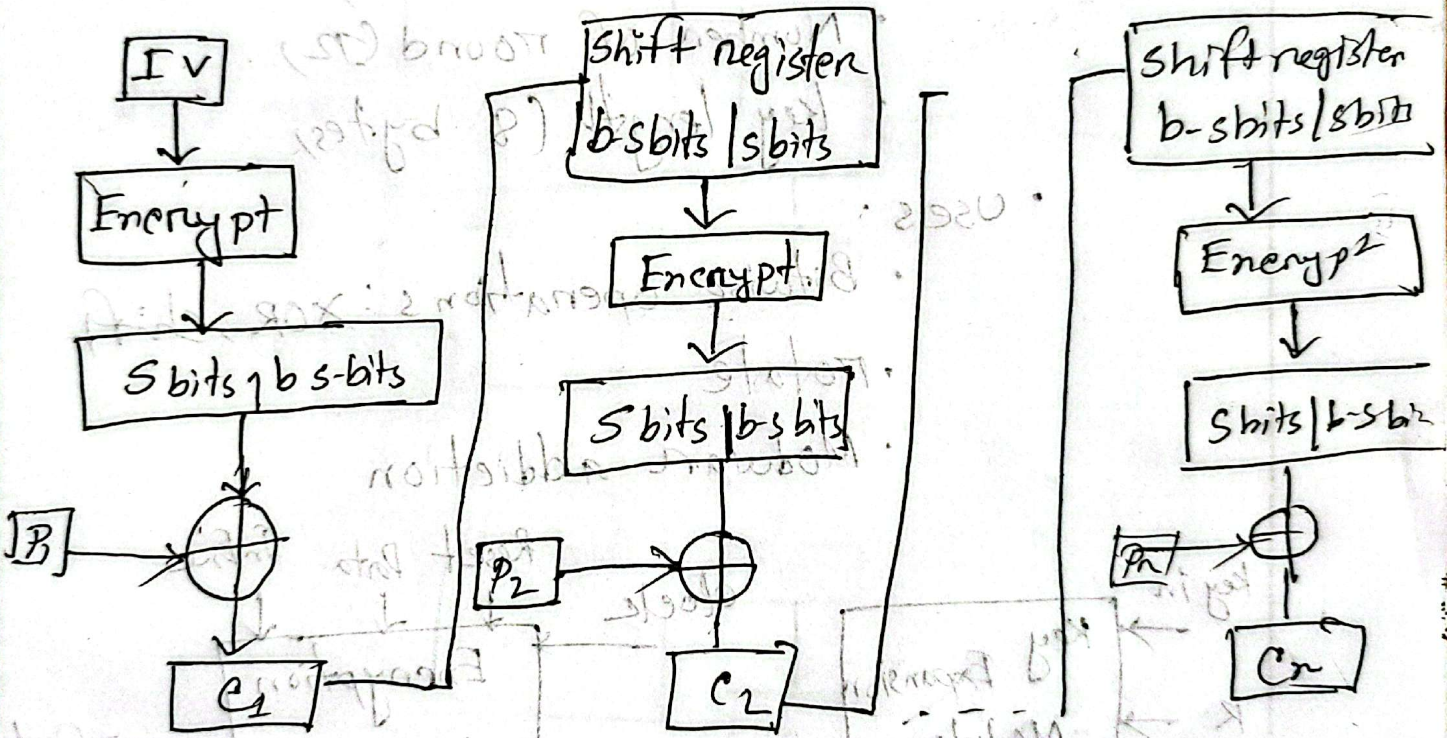
- CBC works well for input greater than b bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptoanalysis than ECB

Disadvantages:

- Requires the previous ciphertext book for encryption and decryption

CFB Block Diagram!

Encryption



De.

Introduction of RC5.

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

Key feature:

- Parameterizable
  - word size (32-bits)
  - Number of round (R)
  - key length (8 bytes)
- Uses:
  - Bitwise operations: XOR, shift
  - rotate
  - Modular addiction

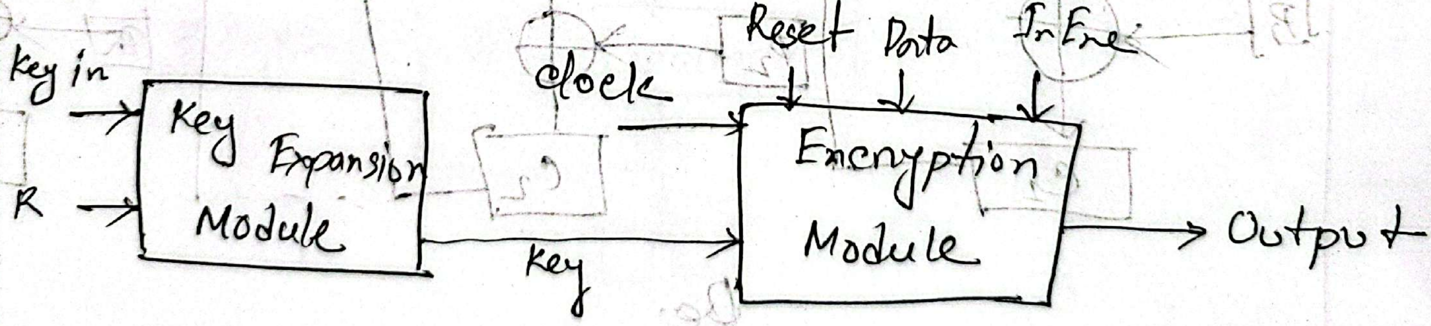
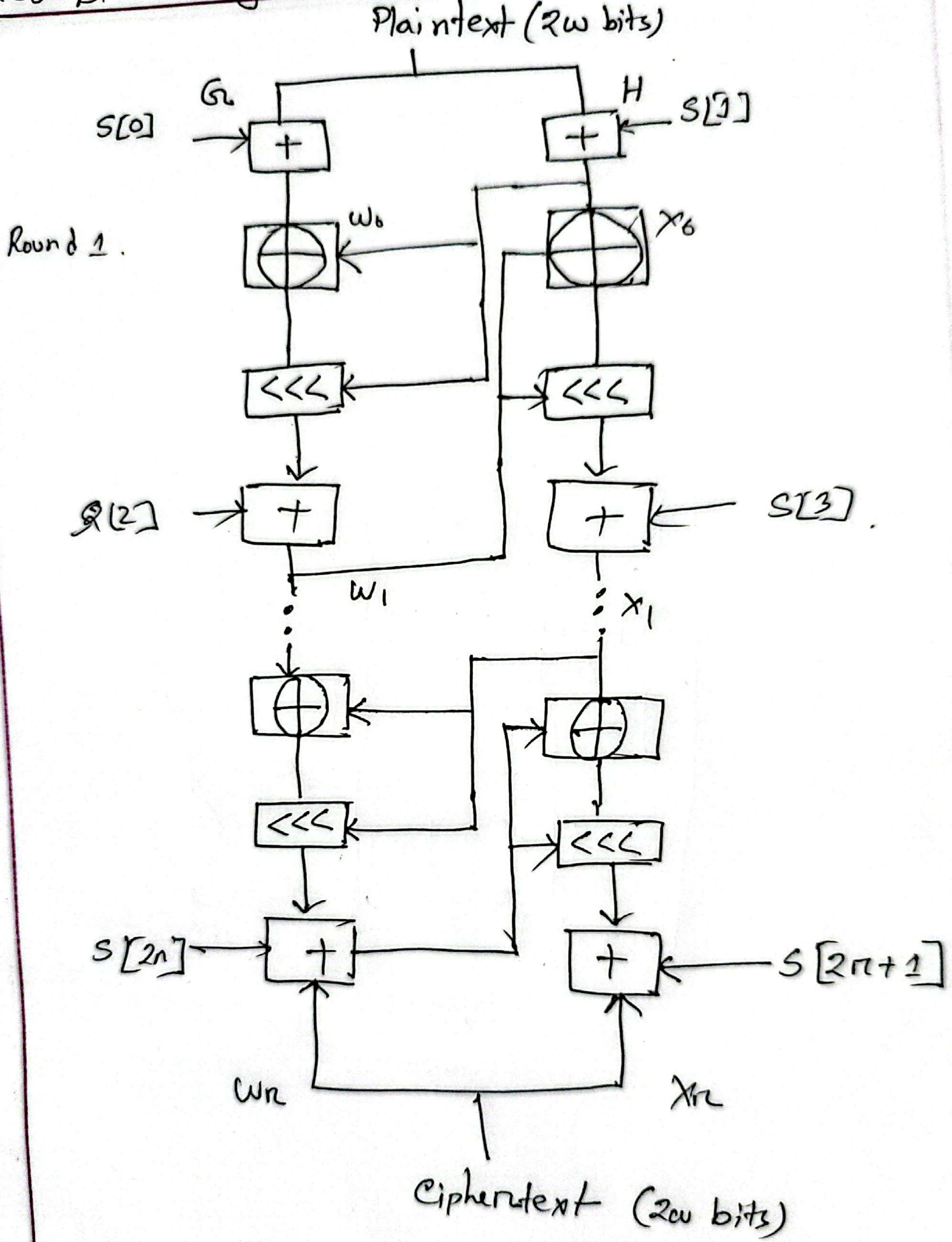


fig: RC5 Encryption Block Diagram.

RC5 Block Diagram


Plaintext (2w bits)
G
H
S[0]
S[1]
Round 1.
w0
x0
<<<
<<<
S[2]
S[3]
W1
x1
<<<
<<<
S[2n]
S[2n+1]
Wn
Xn
Ciphertext (2w bits)