Cryptography and Cyber Law

Assignment

Shusmita Ghosh Shoili

IT-21006

** Modes of operation and RC5 block-diagram and java implementation and output.

⟹ Modes of operation:

The block ciphers take a fixed size input block and produces a fixed size output block using a transformation that depends on a key. Modes of operation are used to securely process large data by using a

block cipher repeatedly.

Common modes:

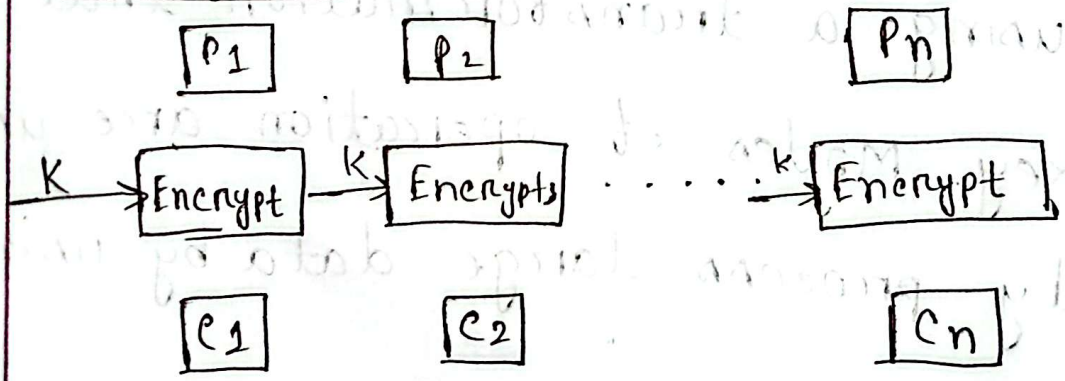
(i) ECB
(ii) CBC
(iii) CFB
(iv) OFB
(v) CTR

Description:-

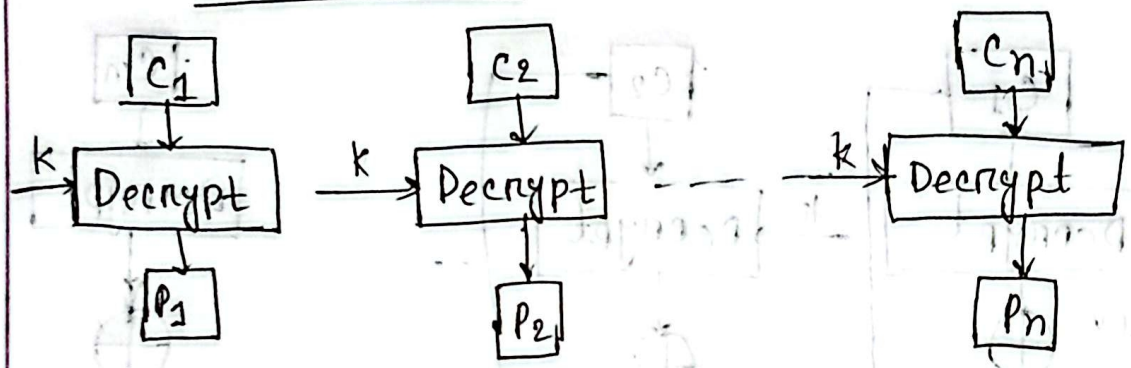
(i) **ECB:** Each block is encrypted independently. Not secure for patterns.

Procedure:

Encryption:



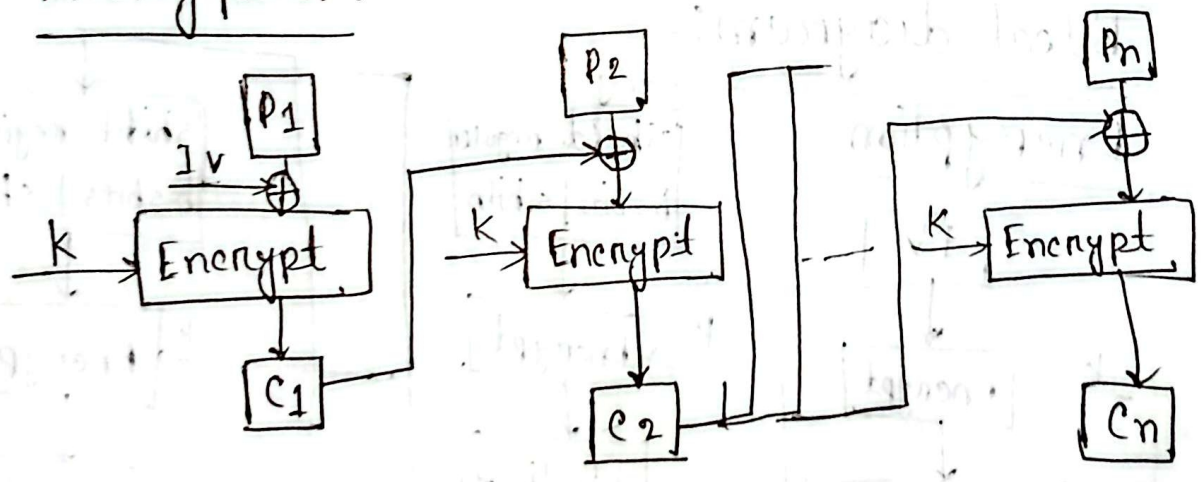
Decryption:



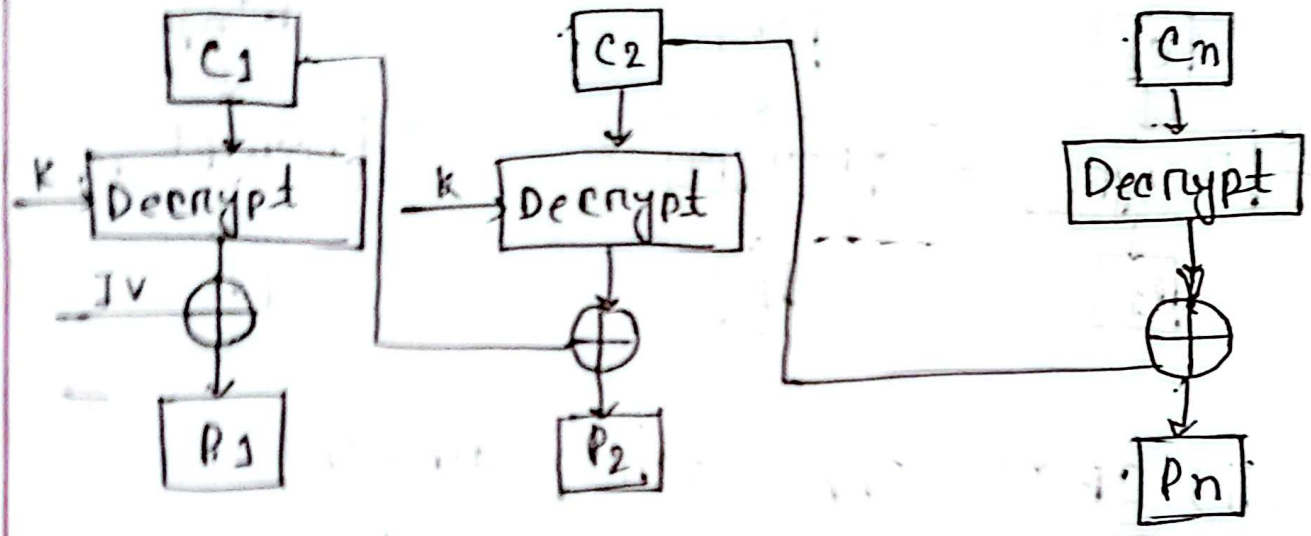
(ii) CBC: XORs each plaintext block with previous ciphertext block before encryption.

Procedure:

Encryption:



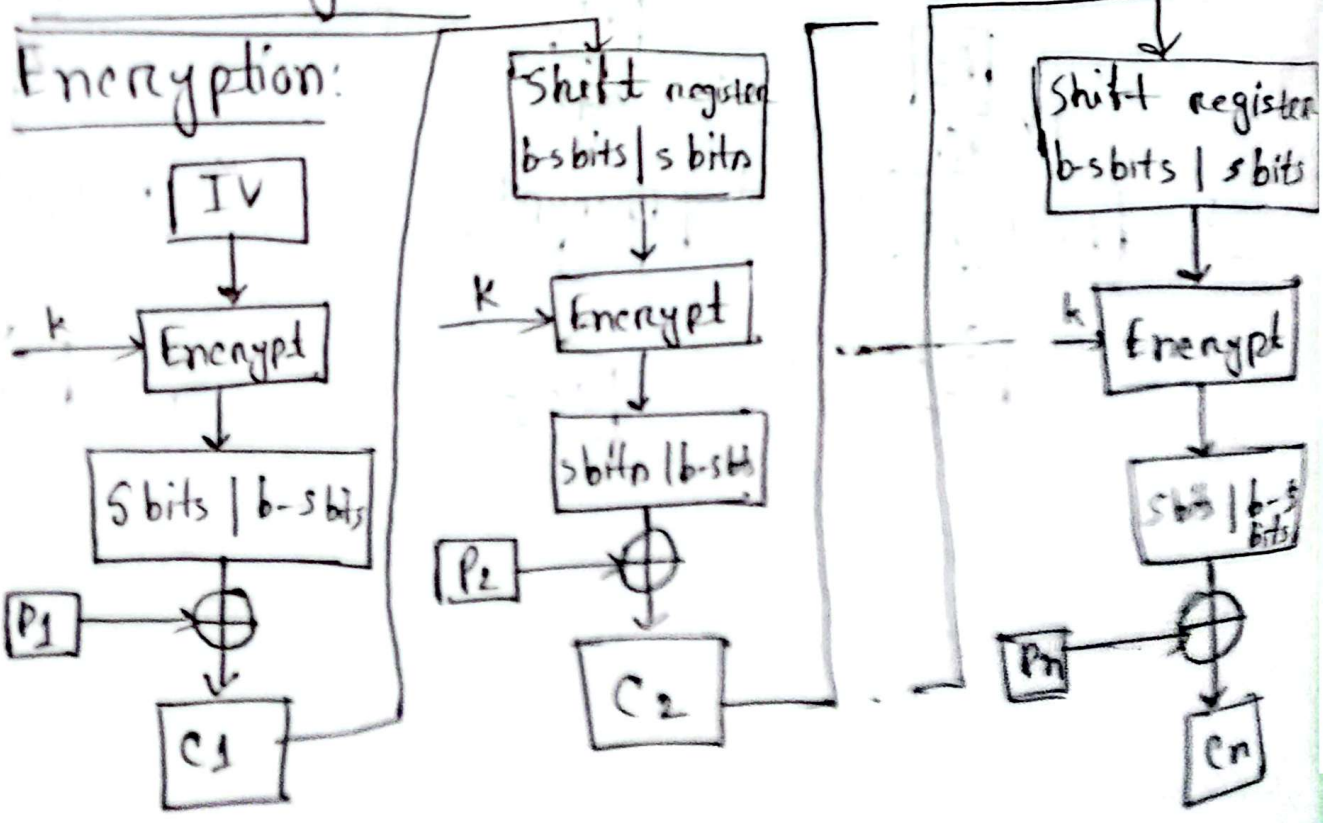
Decryption



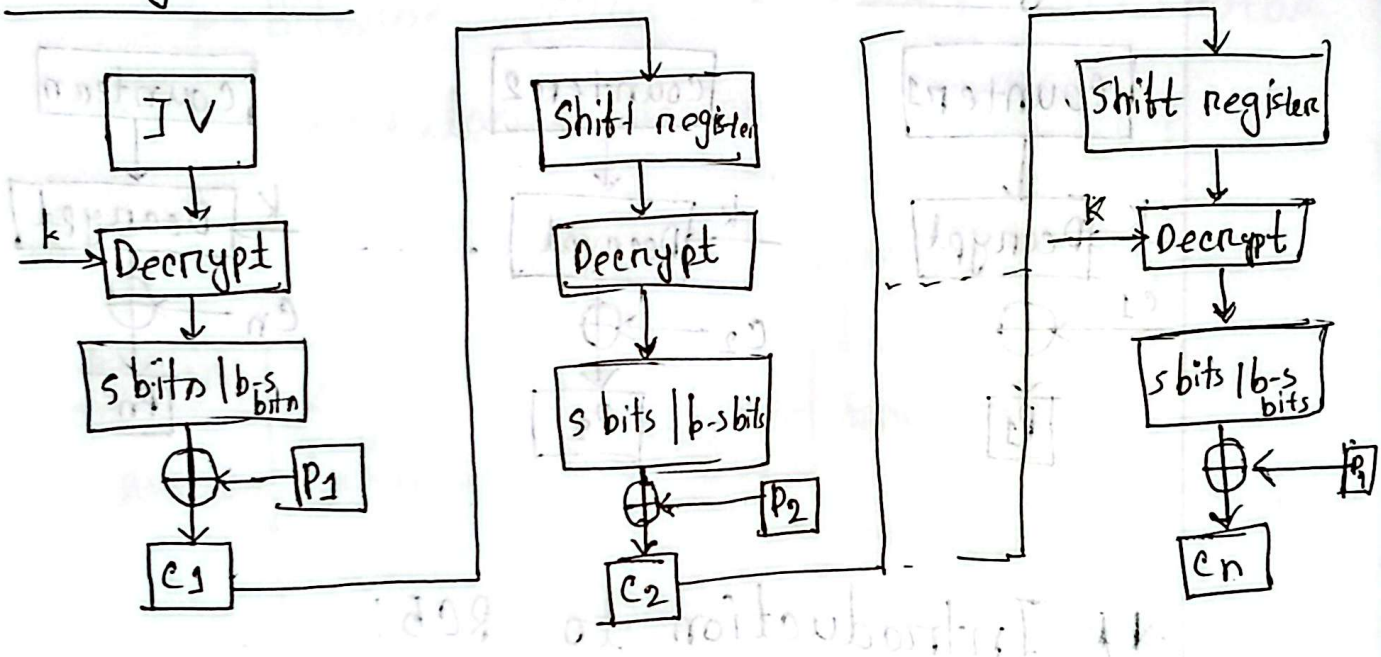
(iii) CFB: Converts block cipher into a self synchronized stream cipher.

Block diagram:-

Encryption:



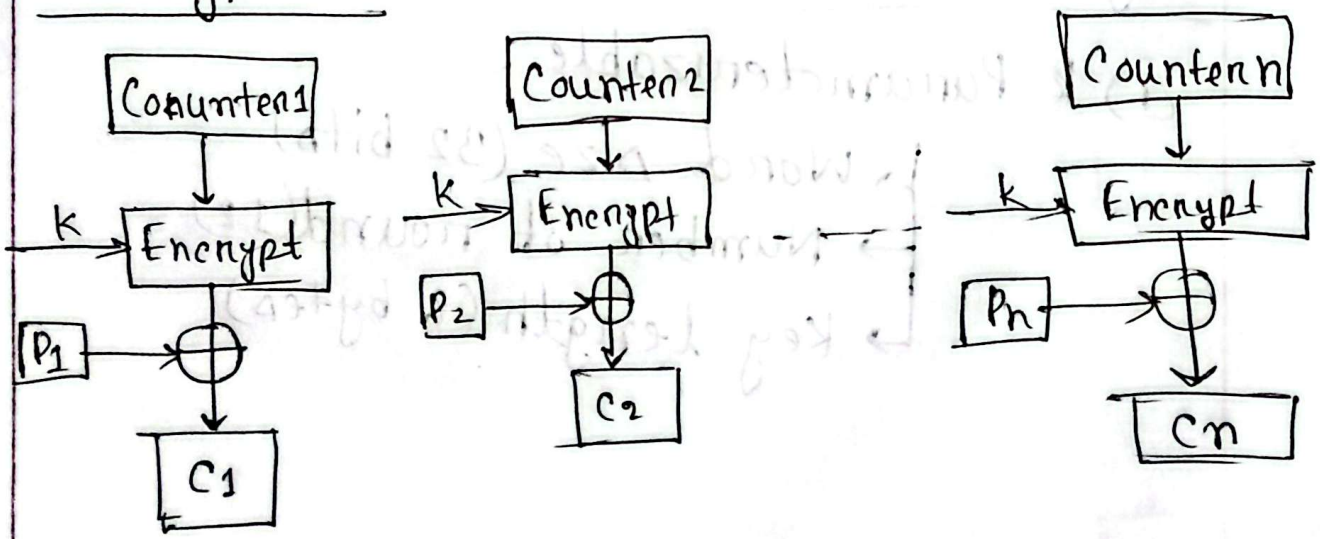
Decryption:



(V) CTR: Uses a counter that gets encrypted and X-ORed with plaintext. Fast and parallelizable.

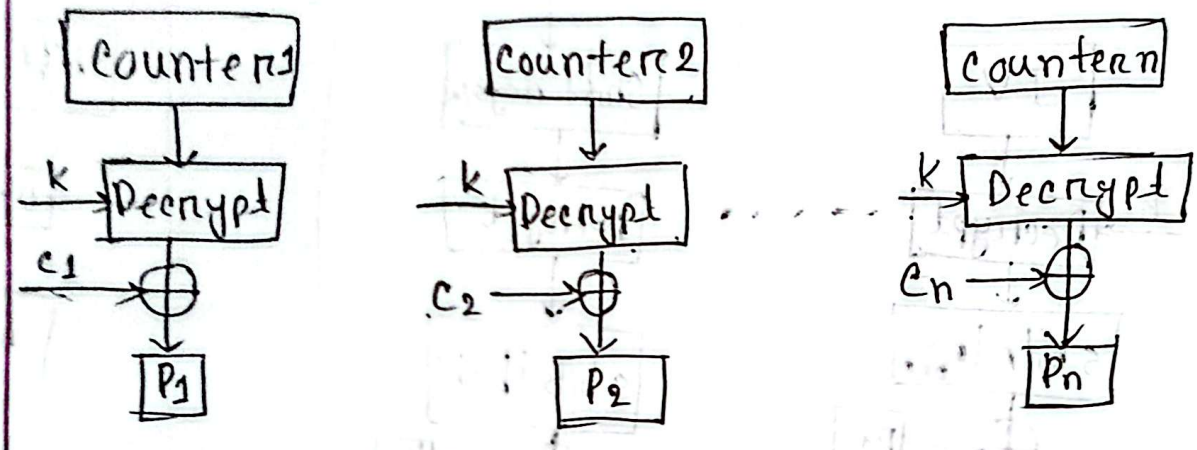
Block diagram:

Encryption:



IT-21006

Decryption:



** Introduction to RC5:

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

Key features:

(i) Parameterizable:

- Word size (32 bits)
- Number of round (12)
- Key length (8 bytes)

(ii) Uses:

- Bitwise operations: X-OR, shift, rotate
- Modular addition

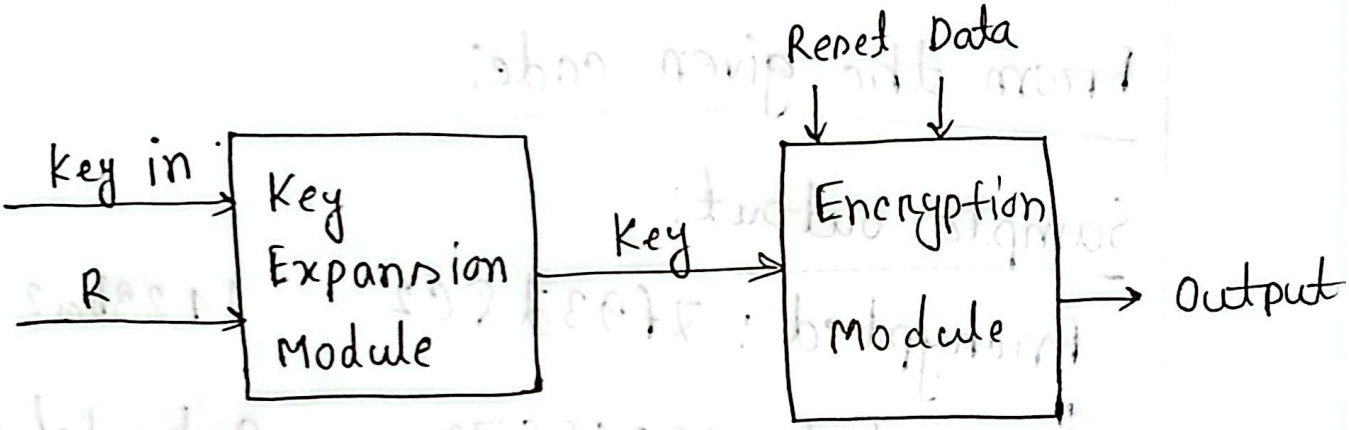
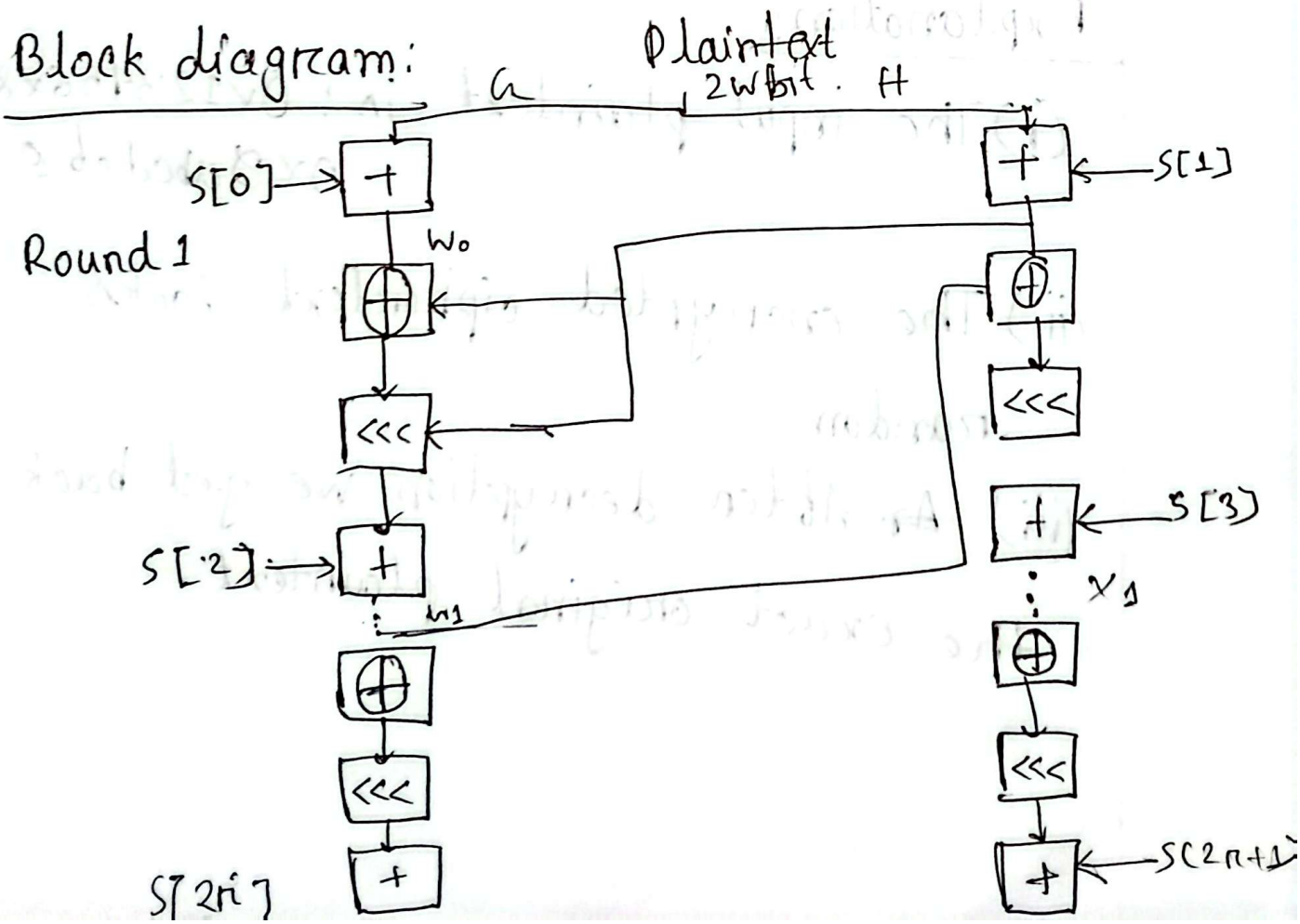


Fig: RC5 Encryption ~~Block diagram~~

Block diagram:



↳ ciphertext (2w bits)

*** Java implementation:

From the given code:

Sample output:

Encrypted : 7f93d8c2 1423ba29

Decrypted : 12345678 9abcdeb0

Explanation:

(i) The input plaintext in : 0x12345678
0x9abcdeb0

(ii) The encrypted ciphertext looks random.

(iii) ~~An~~ After decryption we get back the exact original plaintext.