4th Year
1st Semester

Abdus Salam
IT-21016
Session: 2020-21
Dept of ICT, MBSTU

Cryptography and Cyber Law

Assignment on: Modes of Operation and RC5- Block Diagram and Java Implementation and output.

Modes Of Operation:

Block Cipher Modes of Operation define how to securely encrypt and decrypt large amounts of data using block cipher. A block cipher is an encryption algorithm that processes data in fixed-size blocks (eg, 128 bits) rather than one bit at a time.

Here are a few common modes:

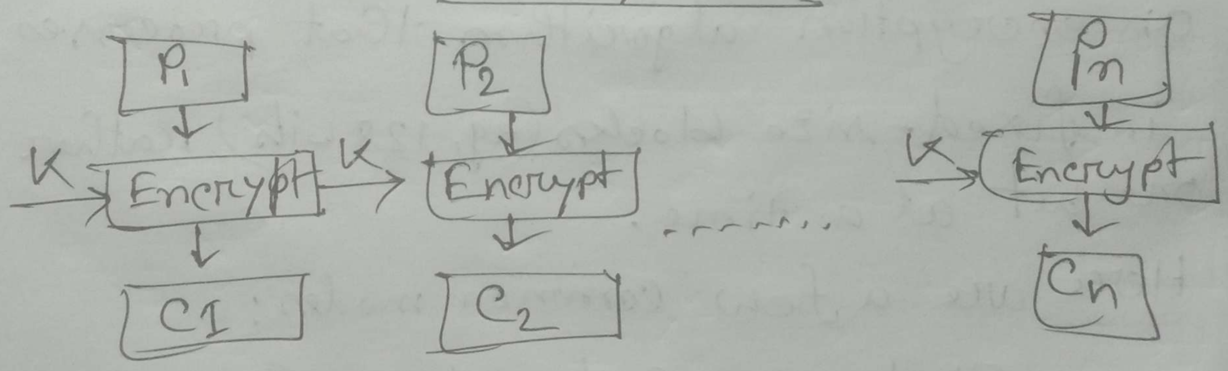
- Electronic Code Block (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)

Abdus Salam
IT-21016
2020-21

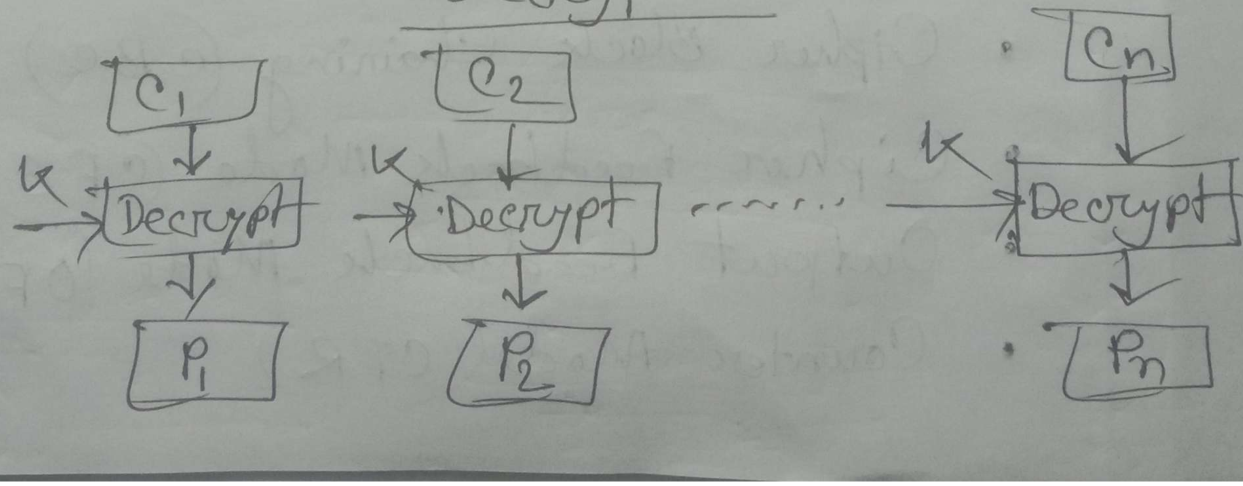
Electronic Code Block (ECB):

The electronic code block is the easiest block cipher mode of functioning. It is easier because of the direct encryption Of each block of input plaintext and output is in the form of blocks of encrypted ciphertext.

Encryption



Decryption

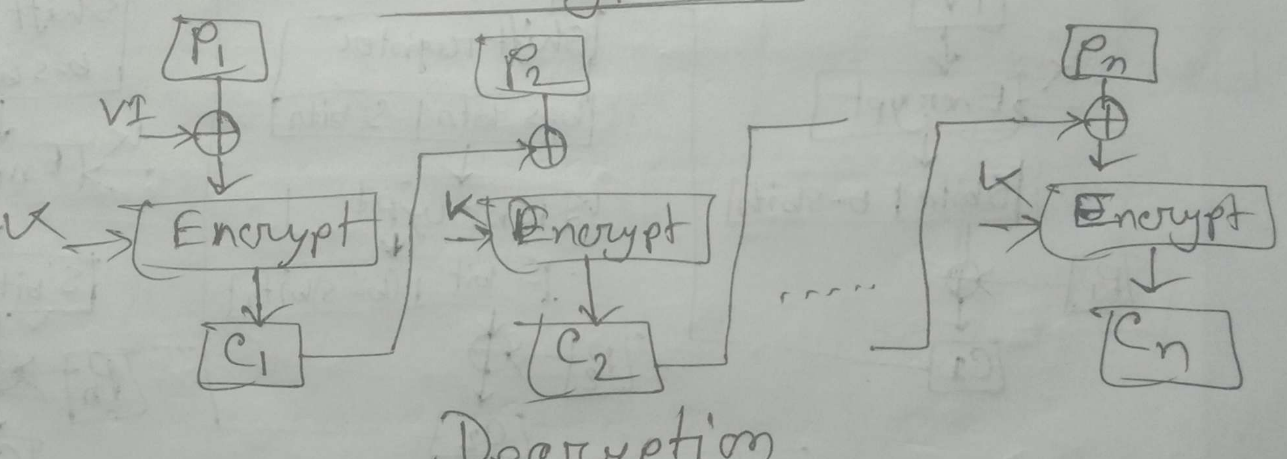


Abdus Salam
IT-21016
2020-21

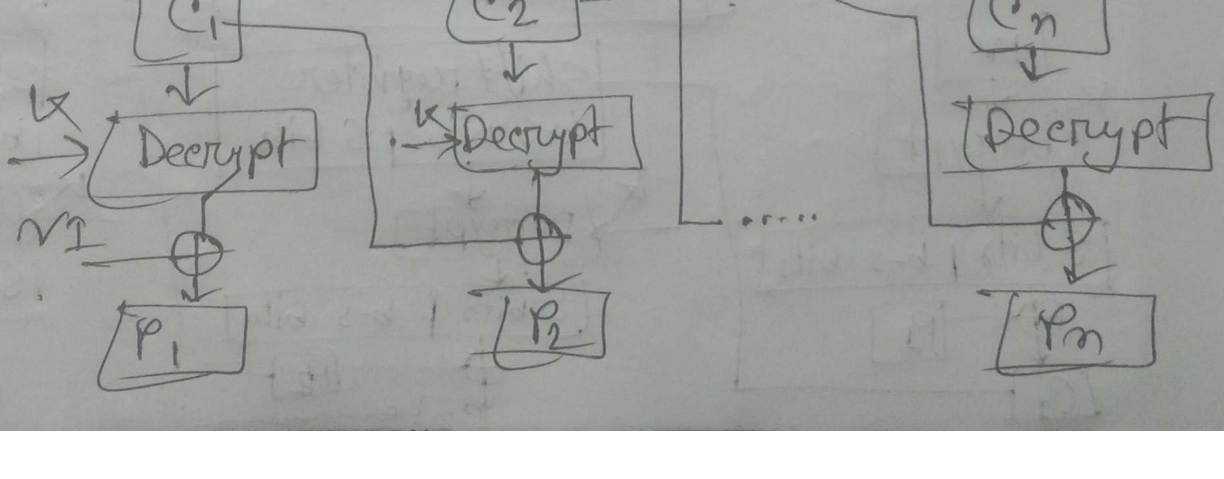
Cipher Block Chaining (CBC):

Cipher block Chaining or CBC is an advancement Made on ECB since ECB compromise some security requirements. In CBC, the privous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext ~~block~~ block.

Encryption



Decryption

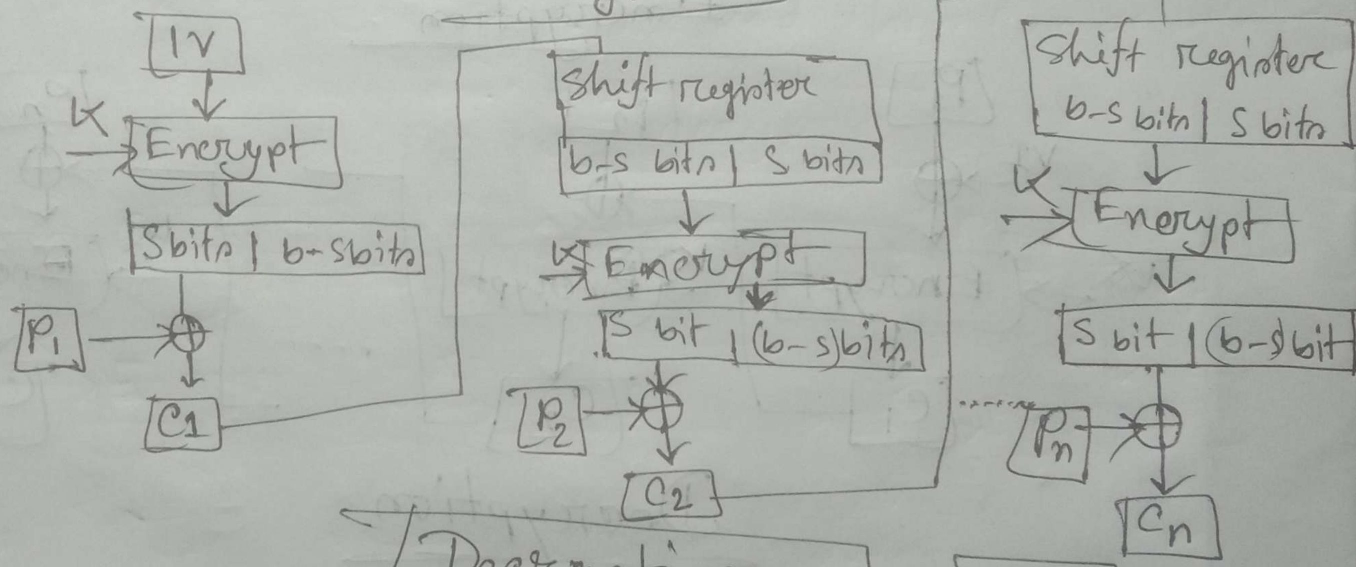


Abdus Salam
IT-21016
2020-21

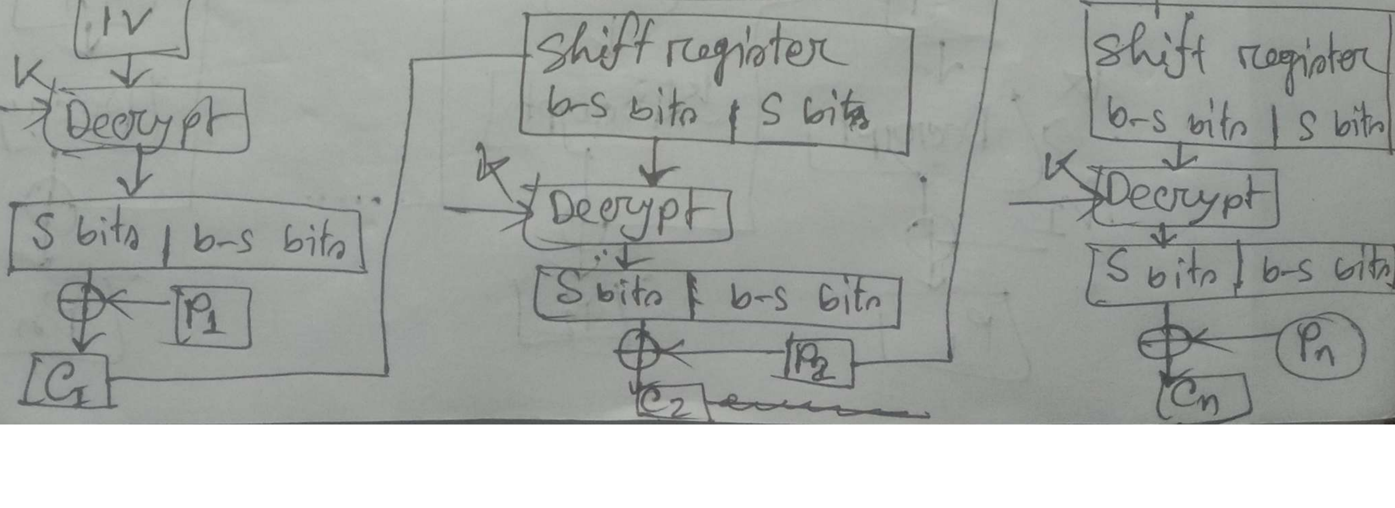
Cipher feedback Mode (CFB):

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector (IV) is used for first encryption and output bits are divided as a set of s and b-s bits.

Encryption



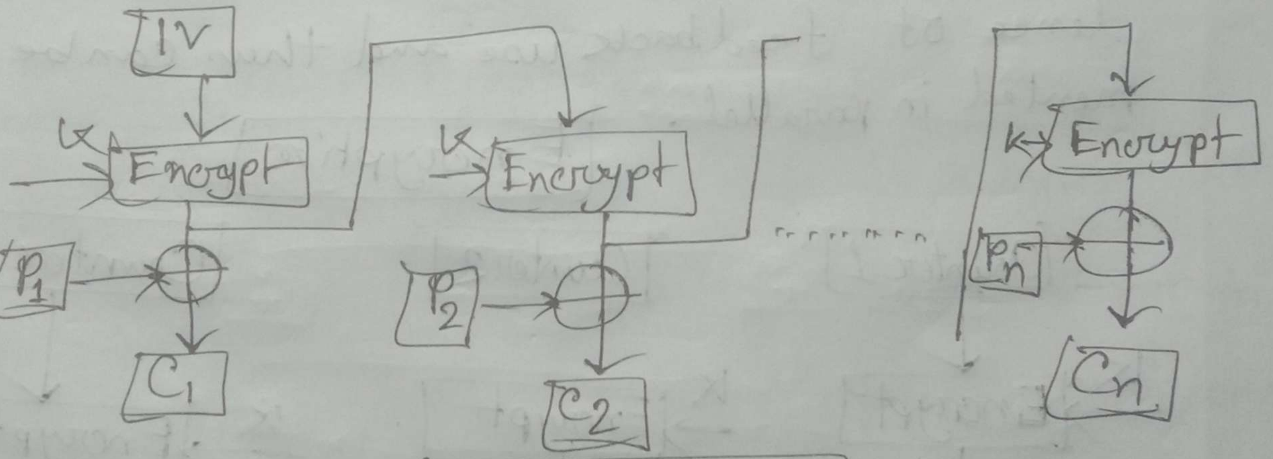
Decryption



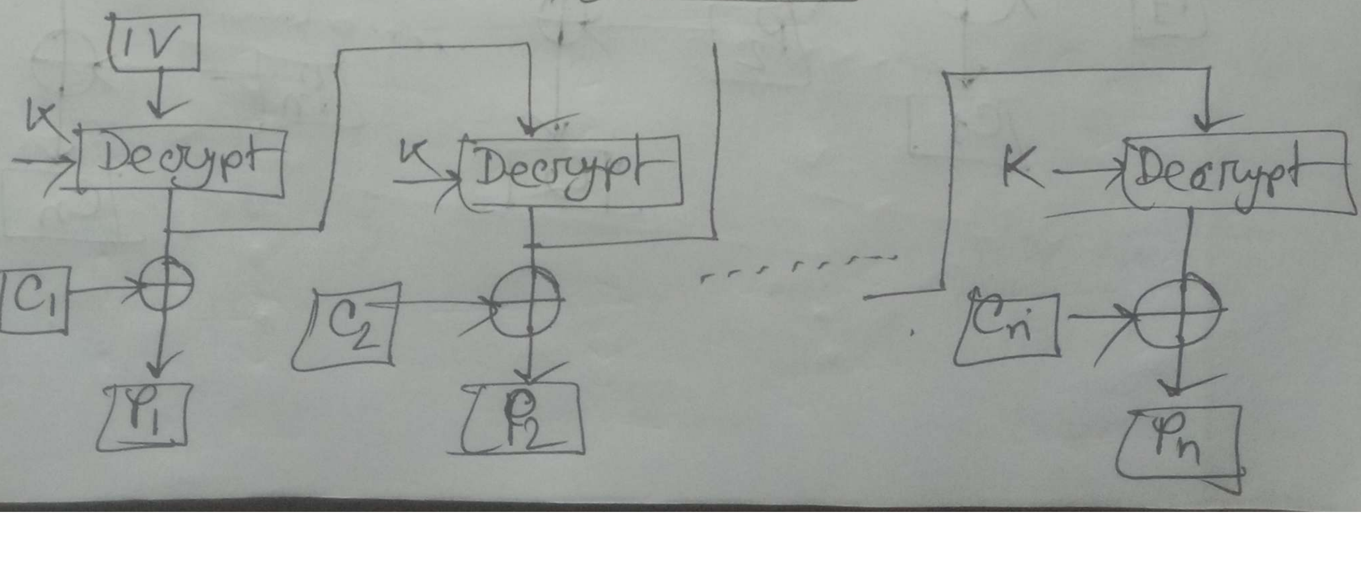
Abdus Salam
IT-21016
2020-21

Output feedbac Mode (OFB): The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual ciphere which is XOR output.

Encryption



Decryption

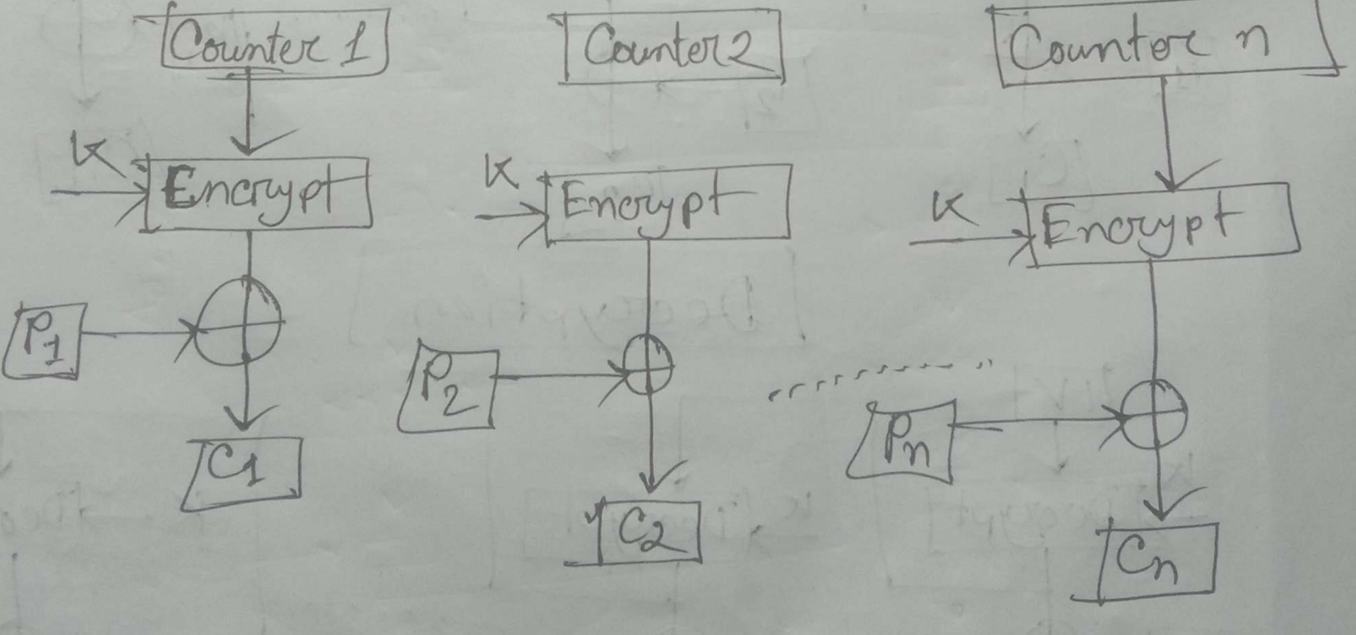


Abdus Salam
IT-21016
2020-21

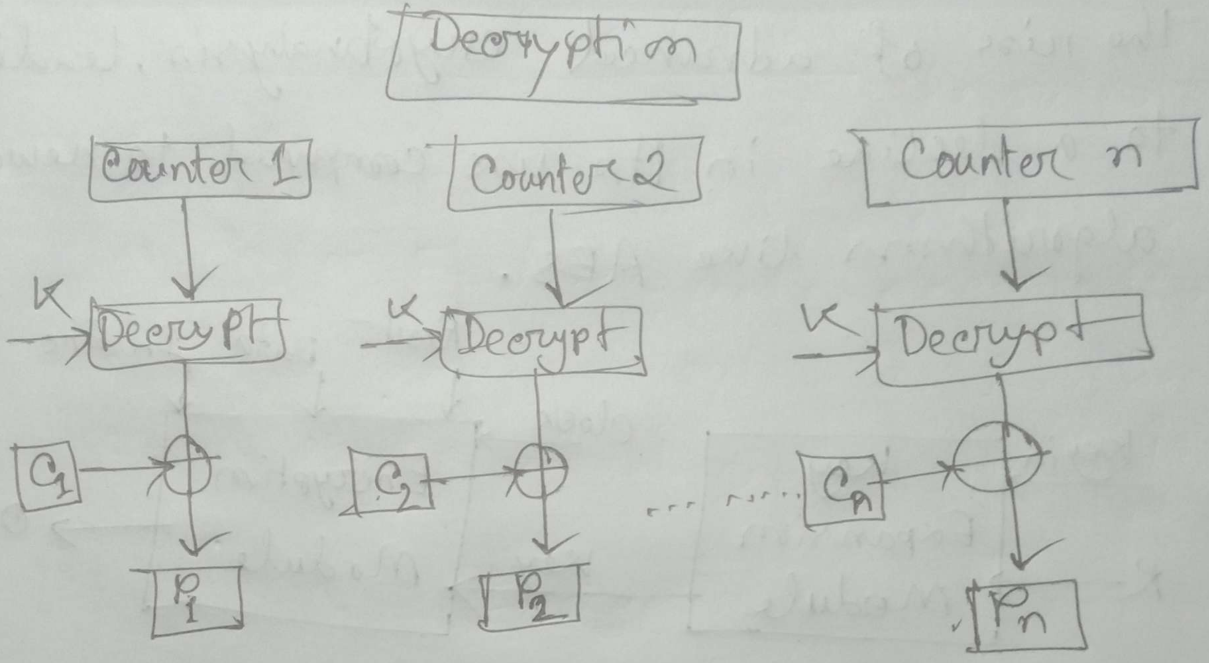
Counter Mode:(CTR)

The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independence of feedback use and thus canbe implemented in parallel.

Encryption



Abdus salam
IT-21016
2020-21

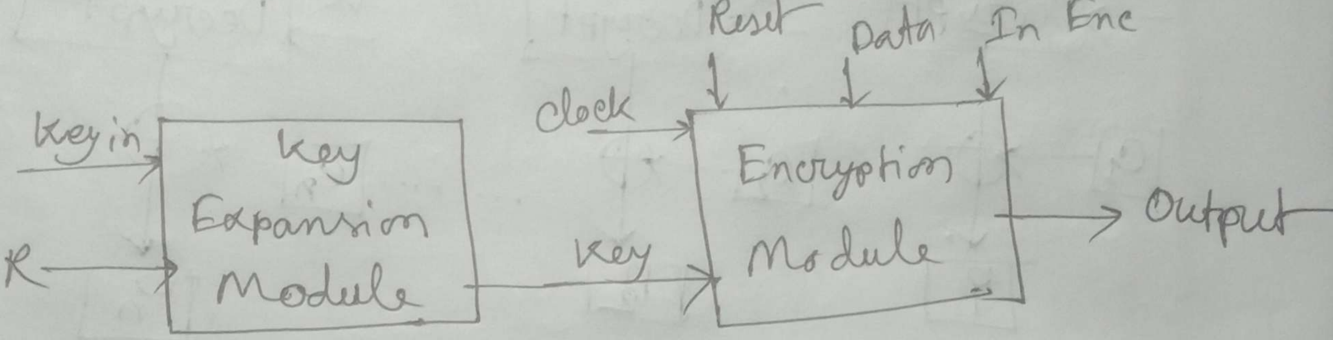


RC5- Block Deigram:

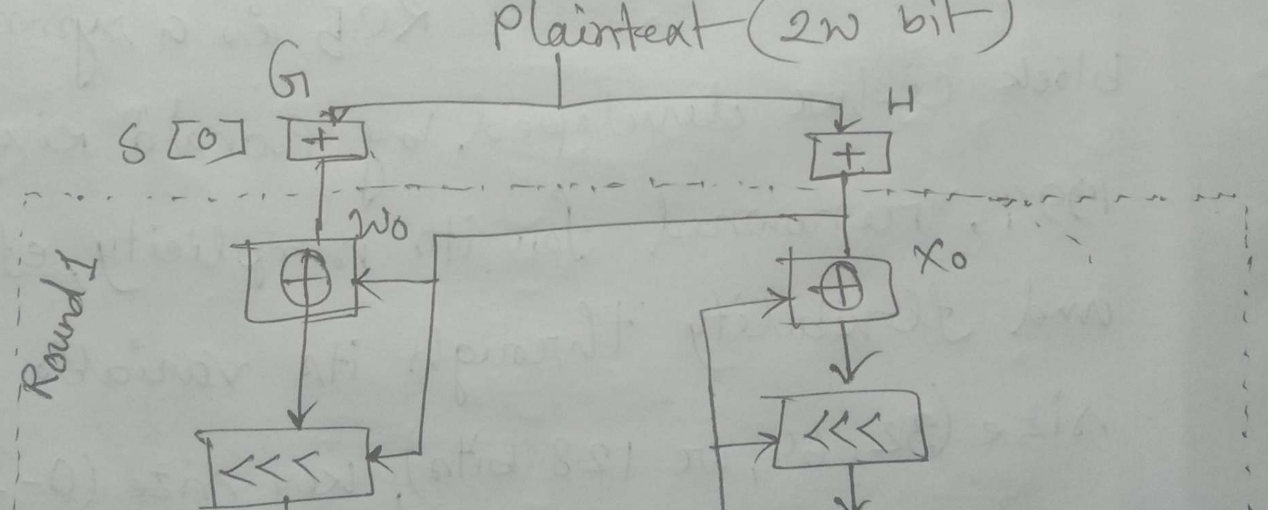
RC5 is a symmetric-key block cipher developed by Ronald Rivest in 1994, renowned for its simplicity, efficiency, and flexibility through its variable block size (32, 64, or 128 bits), key size (0-2040 bits) and number of rounds. While RC5 offers adaptability for tailoring security and performance, it's important to note that it's security has been a concern with

Abdus Salam
IT-21016
2020-21

The rise of advanced cryptanalysis, leading to a decline in its use compared to newer algorithms like AES.



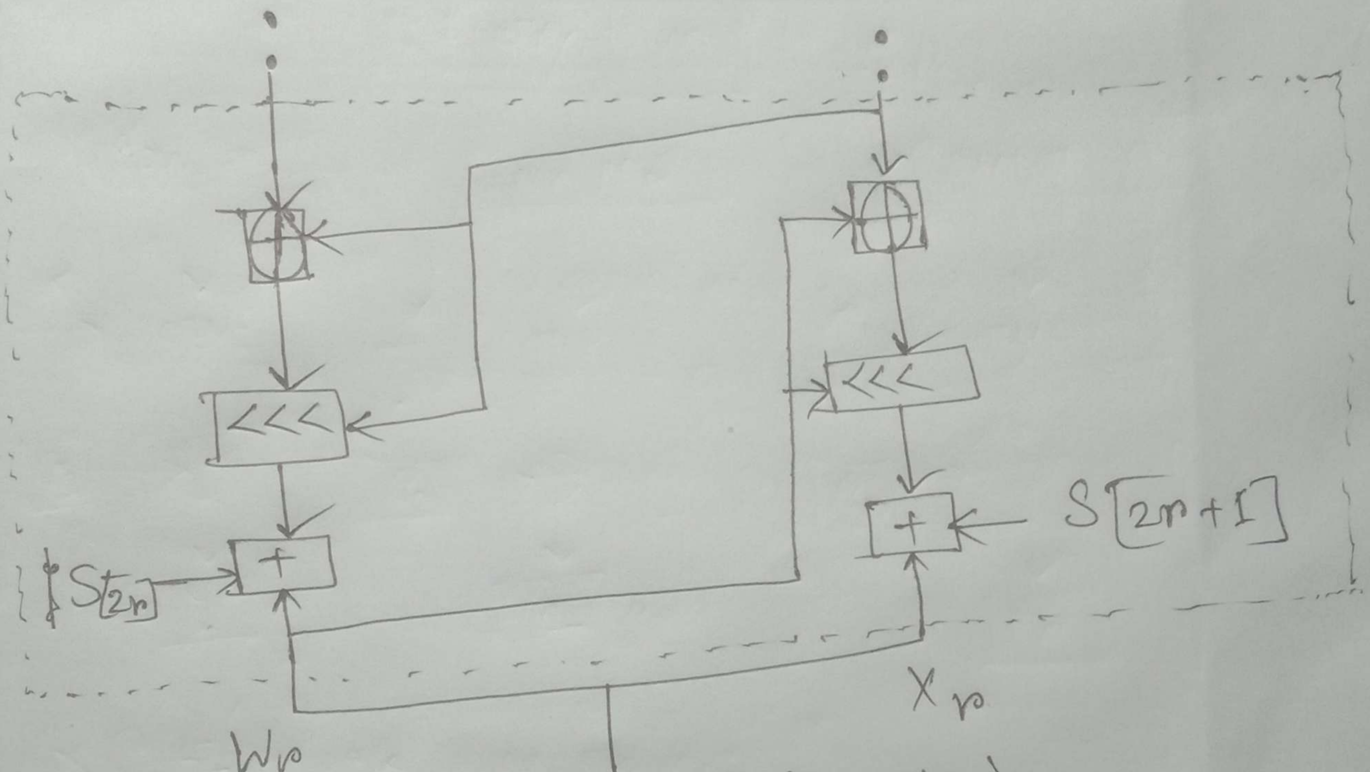
Block Diagram:



Abdus Salam

IT-21016

2020-21; Dept of ICT, MBSTU



Ciphertext (2w bits)