1. Introduction : IT-21046

Modern encryption algorithms like RC5 are used to ensure data confidentiality in software applications. RC5 is a fast symmetric block cypher noteable for it's simplicity and variable parameters:

(Block size, key size, numbers of rounds)

This assignment focuses on:

→ Understanding mode of operation

→ Exploring the RC5 algorithm.

→ Implementing RC5 in Java using JavaFX

→ Presenting the output through a GUI

IT-21046

Modes of operations:

1. ECB-(Electronic codebook Mode):

→ Simplest mode; encrypts each block independen

2. CBC-(Cipher Block Chaining Mode):

→ Each plaintext block is XORed with the previous cipher text block before encryption.

3. CFB-(Cipher Feedback mode):

→ Convert a block cipher into a self-synchronizing stream cipher.

4. OFB-(Output Feedback mode):

→ Convert a block cipher into a sychronous stream cipher.

IT-21046

5. CRT- (Counter mode):

→ Uses a counter that is encrypted to produce a keystream for XORing with plaintext.

6. GCM - (Galois/counter Mode):

→ Combine CTR mode with authentication using Galois field multiplication.

7. XTS - (XEX-based Tweaked CodeBook mode with ciphertext stealing):

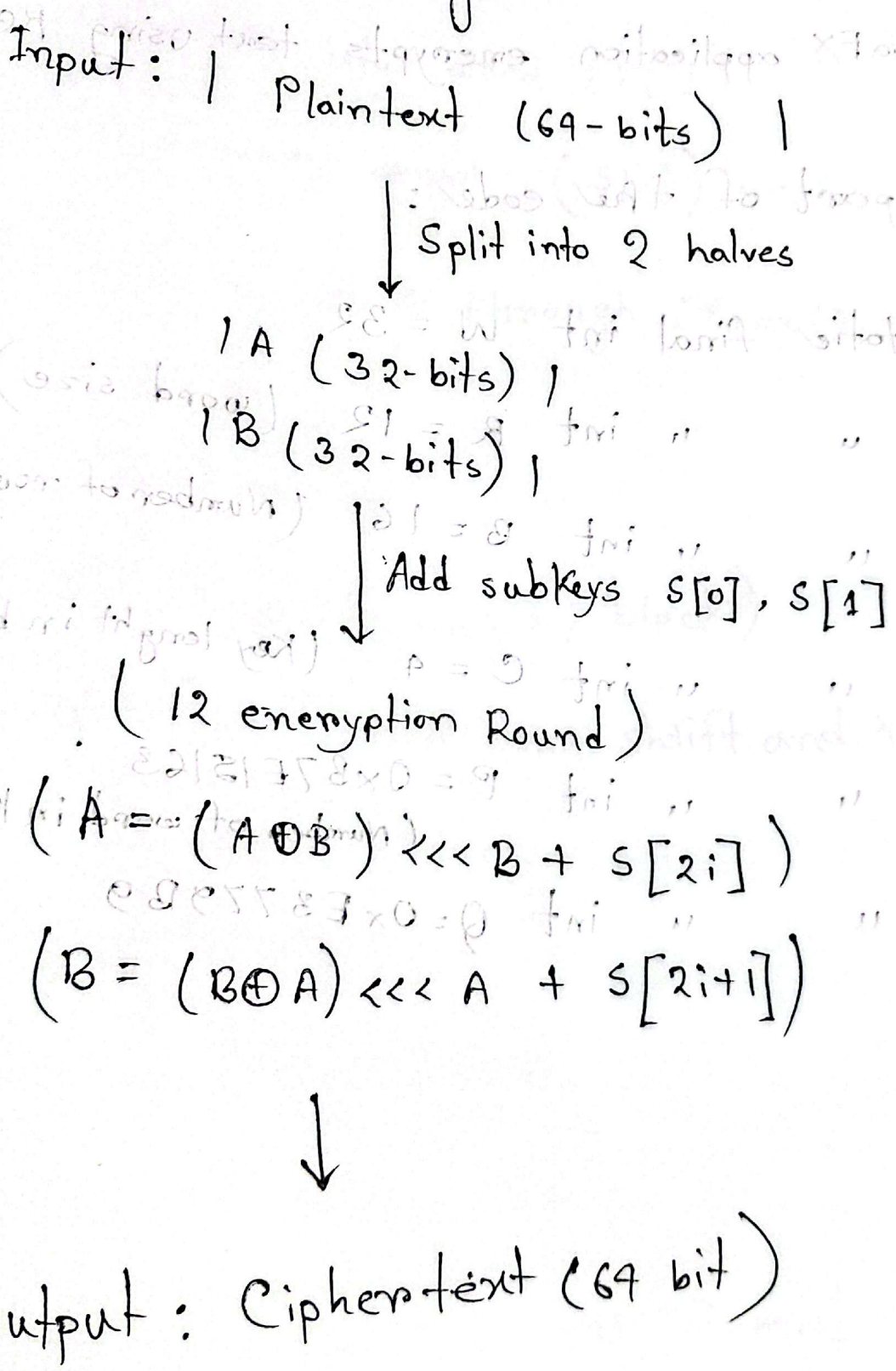
→ Common in disk encryption, protects data even if blocks are moved or copied.

8. PCBC - (Propagating Cipher Block Chaining mode):

→ A variation of CBC where both plaintext and ciphertext are XORed with the next block.

IT-210AG

RC5 Block Diagram:



IT- 21046

Java Implementation with JavaFX GUI:

→ This JavaFX application encrypts text using RC5.

Important part of the code:

Private static final int W = 32

" " " int R = 12 (word size)

" " " int B = 16 (Number of round)

" " " int C = 4 (Key lenght in byte)

" " " int P = 0xB7E15163

" " " int Q = 0xE3779B9 (Number of word in key)

IT-21046

Key Setup :

→ Convert Key into word (L[])

→ Initilizes subKey array (S[])

→ Mixes L and S through 3*max(2r+2, c) iterations

Encryption Function :

→ Takes 64-bit (2x32bit) block)

→ Perform 12 round using shtift and XOR operation.

JavaFX GUI :

→ Accep user input

→ Encrypt using RCS

→ Display ciphertext in hex format.

IT=21096

Sample output:

Input: Hello Res

Output: Sess

Note: Out changes on and padding.