1. Introduction:

1T-210A6,000

1+-2104 C

to edoss of Modern energiption objectitions like RCE one used to RC5 is a fast symmetrie block exphere noteable

for itis simplicity and variable parameters:

· Rlock Size, key size, numbers of rounds)

This assignment focuses on:

- -> Understanding mode of operation
- -> Exploring the Res algorithm.
- -> Implementing Res in Java using Java FX
- -> Proesenting the output through a GUI streom ciphen.

# Modes of operations:

1. ECB-(Electronie codebook mode)

Simplest mode; encrypts each block independen

2. CBC- (Ciphen Block Chaining Modu):

Fach plaintext block is xoped with the previous eigher tent block before encryption.

3. CFB - (Ciphen Feedback mode):

-> Convent a block eigher into a self-Synchronizing stream eigher.

4. OFBI- (Output Feedback mode)

-> convert a block eigher into a sychronous Stream ciphen.

5-CRT- (counter mode):

> Uses a counter that is enerypted to produce a Keystreom for XOPing with plaintext.

6. GCM - (Galois/counter mode):

-> Combine CTR mode with authentication using Gralois field multiplication.

7. XTS- [XEX-based Tweaked CodeBook mode with eighentext stealing):

common in disk eneryption, protects data even if blocks one moved on copied.

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

> A variation of eBC where both plaintent and eighentent one xoped with the next block.

IT-210A615-11. # Resultation d'in mitalinand puil and Imput: | Plaintext (64-bits) | Split into 2 halves (sois based (32-bits) | this loning sites of minit Toha mi Hymos (ans) + P = 5 (12 eneryption Round)

(12 eneryption Round)

(14 DBm) <<< B + S[2i]

(B = 1 DDD)

(B = 1 DDD) (B = (B) A) <<< A + 5[21+1]) output: Cipheratext (64 bit)

IT- 21046 / S-11 # Jova Implementation with Jaya FX GUIC: 11 > This JavaFX application energypts text using Res. Important part of the code: Private statie final int W = 32 " int R = 12 (word size) [1] 2. [0] 3 Exercises bb/ (Number of round) 11 11 int C = 4 (Key length in byte) 11 " int P= 0x87 F15163 [[::]2 + 8 >> (Number of word in Kex)

u int G=0x E3779B9

([:::]2 + A>>> (ABB) = 8) 11 (tid to) tocstorodoro tugtuo

9 bold = 1.1 17-21046 James

Ky Setup :

-> Convent Key into world (ILEH): tuan!

-> Initilizes subter among (SEI):

Mixes L and & through 34 max (2nt2, e) iterations.

Pribleg box 100 aproved. to 300 starts.

Eneryption Function:

> Takes 64-bit (2x32bit) block)

-7 Perform 12 round using shift and toR operation.

JavaFX GUI;

> Accep user input

> Enerypt using RCS

> Pisplay ciphentext in her format.

# Sampler output: : gold. Input: Hello Res du la francis Output: (sees yours vidus essibilial. Note: Out changes on and padding. Takes 64-10th (2×32bit) block) Personn 12 round using shiff and 2008 openation. : TUD X Tal trans mous quost i nearpy using RCS Prince Proposition in book elegion volges