Государственный Университет Молдовы

Факультет Математики и Информатики

Департамент Информатики

“Криптография и информационная безопасность”

Лабораторная работа №1

Алгоритм “RC2”

Преподаватель: O.Cerbu

Выполнил: Маруневич Николай группа I1902

Кишинев 2022

**Criptarea**

computer to x2

01100011 01101111 = a (co)

01101101 01110000 = b (mp)

01110101 01110100 = c (ut)

01100101 01110010 = d (er)

MN (key) (Marunevici Nicolai)

01001101 01001110

1. a + key

01100011 01101111 + 01001101 01001110 mod 2^32 =

(25455 + 19790) mod 2^32 = 45245 = 1011000010111101

1. c^d => 01110101 01110100 &

01100101 01110010 =

01100101 01110000

3. (not d) ^ b= 0001010 10001011 &

01101101 01110000 = 0001000 00000000

1. ((pt2)+(pt3)) =

(c ^d) + (not d ^b) =>

(01100101 01110000 + 0001000 00000000) mod 2^32 =>

(25968 + 2048) mod 2^32 = 28016 => (110110101110000)

1. (pt1)+(pt4) => (1011000010111101 + 110110101110000) mod2^32 =>

(45245 + 28016) mod2^32 = 73261 = 10001111000101101

1. Deplasament la stanga cu 4 (<<<4)

10001111000101101

00000000000100011110001011010000 = a

1. b => (01101101 01110000) c => (01110101 01110100)

d => (01100101 01110010) a=>(00000000000100011110001011010000)

1. Concatenare b,c,d,a =>

01101101 01110000 01110101 01110100 01100101 01110010 to text UTF-8 => “mputer”

00000000000100011110001011010000) to x16 => 11E2D0

**Decriptare**

computer to x2

01100011 01101111 = a (co)

01101101 01110000 = b (mp)

01110101 01110100 = c (ut)

01100101 01110010 = d (er)

MN (key) (Marunevici Nicolai)

01001101 01001110 = 19790

00000000000100011110001011010000 = a

1. Deplasamentul a la dreapta cu 4 (>>>4) => 10001111000101101
2. c^d => 01110101 01110100 & 01100101 01110010 => 1100101 01110000
3. (not d) ^ b= 0001010 10001011 & 01101101 01110000 = 0001000 00000000
4. ((pt2)+(pt3)) =

(c ^d) + (not d ^b) =>

(01100101 01110000 + 0001000 00000000) mod 2^32 =>

(25968 + 2048) mod 2^32 = 28016 => (110110101110000)

1. (a - (b ^ (not d) + (c ^ d) )) =>

(00000000000100011110001011010000 - 0001000 00000000 + 01110101 01110100) mod 2^32 =>

(73261 – 2048) mod 2^32 = 71213 => 10001011000101101

1. pt5 – key => (71213 – 19790) mod 2^32 = 51 423 => 1100100011011111
2. Concatenare a ,b,c,d => (01100011 01101111 01101101 01110000 01110101 01110100

01100101 01110010) to text UTF-8 =>

“computer”