Государственный Университет Молдовы

Факультет Математики и Информатики

Департамент Информатики

“Криптография и информационная безопасность”

Аттестационная работа 1

Проверил: Чербу Ольга

Выполнил: Чобану Артём

Кишинев 2021

**Алгоритм RC2**

Шифруемое слово: **language**

Ключ – **ac** (Artiom Ciobanu)

**Шифрование**

Данное слово в бинарном коде:

01101100 01100001 01101110 01100111 01110101 01100001 01100111 01100101

a: 01101100 01100001 b: 01101110 01100111

c: 01110101 01100001 d: 01100111 01100101

Ключ: 01100001 01100011

1. a + subkey:

01101100 01100001 +

01100001 01100011 =

11001101 11000100

1. c & d:

01110101 01100001 &

01100111 01100101 =

01101101 01100001

1. (not d) & b:

10011000 10011010 &

01101110 01100111 =

00001000 00000010

1. (c ^ d) + (not d ^ b) =

01110101 01100001 ^ 01100111 01100101 +

10011000 10011010 ^ 01101110 01100111 =

00010010 00000100 + 11110110 11111101 =

00000001 00001001 00000001

1. pt1 + pt4 =

00000000 11001101 11000100 +

00000001 00001001 00000001 =

00000001 11010110 11000101

1. Сдвиг влево на 4:

00000001 11010110 11000101 <<< 4

0001 11010110 11000101 0000

00011101 01101100 01010000

1. Конкатенация b, c, d, a:

011011100110011101110101011000010110011101100101000111010110110001010000

Результат ascii: **nguagelP**

Результат в hex: **6e67756167651d6c50**

**Расшифровка**

1. Сдвиг вправо на 4:

00011101 01101100 01010000 >>> 4

0001 11010110 11000101 000

1. c & d =

01110101 01100001 &

01100111 01100101 =

01100101 01100001

1. (not d) & b:

10011000 10011010 &

01101110 01100111 =

00001000 00000010

1. (c ^ d) + (not d ^ b) =

01110101 01100001 ^ 01100111 01100101 +

10011000 10011010 ^ 01101110 01100111 =

00010010 00000100 + 11110110 11111101 =

00000001 00001001 00000001

1. a – (b ^ (not d) + (c ^ d)) =

01101100 01100001 - (11110110 11111101 + 01110101 01100001 ^

01100111 01100101) =

01101100 01100001 - (11110110 11111101 + 00010010 00000100) =

01101100 01100001 – 10000100100000001 = 11001110010100000

1. pt5 – CA =

11001110010100000 - 01100001 01100011 = 01101100 01100001

1. Конкатенация a, b, c, d:

01101100 01100001 01101110 01100111 01110101 01100001 01100111 01100101

Результат: language

Результат в hex: 6c616e6775616765