**Tema: Симетричная система шифрования (Sistemul simetric ) -RC2 .**

**Scopul lucrării:**

Criptarea unui mesaj folosind sistemul de criptare bazat pe blocuri Rivest Code2.

**Sarcinile lucrării:**

Mesajul de criptare trebuie să fie un cuvânt tehnic ce conține 8 caractere.

MODEL.

Realizati Algoritmul RIVEST CODE 2 Conform Schemei de mai jos.

Mesajul de criptare m= “hedgehog” Subkey FV este keia ce consta din initialele Nume Prenume: Fomenco Vasile FV, Mesajul din 8 simboluri obligatoriu la alegere. Fiecare student utilizeaza strict cheile corespunzatoare.

**Tools pentru convertire:**

wolfram alpha<enter>

<https://www.rapidtables.com/convert/number/ascii-to-binary.html>

Tools pentru convertire binary to decimal:

<https://www.rapidtables.com/convert/number/binary-to-decimal.html>

Tools pentru operatii logice: <http://www.ambrsoft.com/MathCalc/LogicCalc/LogicOperations.htm>

Tools pentru operatii de deplasament -смещение

<https://onlinetoolz.net/bitshift>

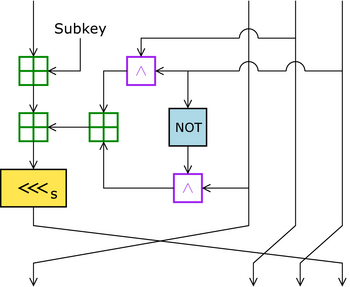
Convert binary to decimal

<https://www.rapidtables.com/convert/number/binary-to-decimal.html>

Convert decimal to binary

https://www.rapidtables.com/convert/number/decimal-to-binary.html

**hedgehog** 01101000 01100101 01100100 01100111 01100101 01101000 01101111 01100111

**CRIPTARE**

**01101000 01100101 01100100 01100111**

**01100101 01101000 01101111 01100111**

a => (01101000 01100101) b => (01100100 01100111)

c => (01100101 01101000) d => (**01101111 01100111**)

Subkey =FV=>(**01000110 01010110**)

1. a + subkey=>(01101000 01100101+01000110 01010110) mod 2^32=

(26725 +18006) mod 2^32 = 44731 = 10101110 10111011.

1. c^d=> **01100101 01101000** &

**01101111 01100111** =

**0**1100101 01100000

1. (not d) ^ b= 10010000 10011000 &

01100100 01100111 =

00000000 00000000

1. (c ^d) + (not d ^b) => (01100101 01100000 +

00000000 00000000)mod2^32 =>

(25952+0)mod2^32=>( 01100101 01100000)

1. (pt1)+(pt4) (10101110 10111011 +01100101 01100000) mod2^32 =>

(44731+ 25952) mod 2^32 =>70683 => (100010100 00011011)

1. Deplasament la stanga cu 4 (<<<4): 0000 00000001 00010100 00011011 0000

NOTA: Замечание:{ 110110**10** <<<2---- 0110**10** 11}

NOTA1: Замечание1:{ 110110**10** <<2---- 0110**10** 00}

1. b => (01100100 01100111) c => (01100101 01101000)

d => (01101111 01100111) a=>(0000 00000000 100010100 00011011 0000)

1. Concatenare b,c,d,a => (01100100 01100111 01100101 01101000 01101111 01100111 0000 00000000 100010100 00011011 0000) “dgehog” „1141B0”

**DECRIPTARE**

1. Deplasamentul a la dreapta cu 4 (>>>4):

0000 00000000 100010100 00011011 0000 (>>>4):

100010100 00011011

1. c^d=> 01100101 01101000 &

01101111 01100111 =

01100101 01100000

1. (not d) ^ b= 10010000 10011000 &

01100100 01100111 =

00000000 00000000

1. (c ^d) + (not d ^b) => (01100101 01100000 +

00000000 00000000) mod 2^32 =>

(25952+0)mod2^32 =>

01100101 01100000

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

( 0000 00000000 100010100 00011011 0000 –

01100101 01100000) mod2^32=>

(70683 - 25952)mod2^32=>  
 44731=> (1010111010111011)

1. a - FV=>(1010111010111011 - 01000110 01010110) mod 2^32 =>(44731-18006) mod2^32=26725=>

0110100001100101

Concatenare a ,b,c,d => (**01101000 01100101 01100100 01100111**

**01100101 01101000 01101111 01100111**

“ hedgehog”