

Tema: ” Algoritmul de criptare/decriptare TEA”

Mesajul: **ETHERNET** 01000101 01010100 01001000 01000101 01010010 01001110 01000101 01010100

01000101 01010100 01001000 01000101- stânga

01010010 01001110 01000101 01010100 - dreapta

Cheia K0: **tree** 01110100 01110010 01100101 01100101

Cheia K1: **funs** 01100110 01110101 01101110 01110011

Cheia K2: **time** 01110100 01101001 01101101 01100101

Cheia K3: **data** 01100100 01100001 01110100 01100001

**Partea impara**

1. Partea dreapta se deplasează la stânga cu 4 biti

<<4 01010010 01001110 01000101 01010100 = 0010 01001110 01000101 010101000000

1. La rezultatul (1) se adaugă valoarea K0 mod 2^32=

(0010 01001110 01000101 010101000000

+ 01110100 01110010 01100101 01100101)mod 2^32 = **10011001010101101011101010100101**

1. Partea dreapta se aduna cu I\* delta 01010010 01001110 01000101 01010100 +1\*10011110001101110111100110111001 mod2^32= **11110000100001011011111100001101**
2. Rezultatul de la p (2) XOR Rezultatul de la p (3) **10011001010101101011101010100101**XOR**11110000100001011011111100001101**

**= 1101001110100110000010110101000**

1. Partea dreapta se deplasează la dreapta cu 5 biti

>>5 01010010 01001110 01000101 01010100 = 0000001010010 01001110 01000101 010

1. La rezultatul (5) se adaugă valoarea K1 mod 2^32

0000001010010 01001110 01000101 010+ 01110100 01110010 01100101 01100101 2^32=1101001000001111110000010011101

1. Rezultatul de la p (4) XOR Rezultatul de la p (6)

**1101001110100110000010110101000**XOR 1101001000001111110000010011101=110101001110010100110101

1. Partea stângă se aduna cu rezultatul p(7) mod 2^32

01000101 01010100 01001000 01000101+110101001110010100110101 mod 2^32=1000110001010010010110101111010

**Partea para**

1. Partea stanga se deplasează la stânga cu 4 biti

01000101 01010100 01001000 01000101<<4 0101 01010100 01001000 010001010000

2)La rezultatul (1) se adaugă valoarea K2 mod 2^32

(0101 01010100 01001000 010001010000+ 01110100 01101001 01101101 01100101)

mod 2^32=11001001101011011111000110110101

3)Partea stanga se aduna cu I\* ɓDELTA

01000101 01010100 01001000 01000101+1\*10011110001101110111100110111001mod2^32= 11100011100010111100000111111110

4) Rezultatul de la p (2) XOR Rezultatul de la p (3)

11001001101011011111000110110101XOR11100011100010111100000111111110 = 101010001001100011000001001011

5)Partea stanga se deplasează la dreapta cu 5 biti

01000101 01010100 01001000 01000101=0000 001000101 01010100 01001000 010

1. La rezultatul (5) se adaugăvaloarea K3 mod 2^32

0000 001000101 01010100 01001000 010+01100100 01100001 01110100 01100001mod 2^32=1100110100011000001011010100011

7)Rezultatul de la p (4) XOR Rezultatul de la p (6)

101010001001100011000001001011 XOR1100110100011000001011010100011=1001100101010100010011011101000

8)Partea dreapta se aduna cu rezultatul p(7) mod 2^32

01010010 01001110 01000101 01010100 +1001100101010100010011011101000

mod 2^32=10011110111110000110110000111100

**Rezultatul:** 10011110111110000110110000111100= øl<

**Decriptarea**

**Partea para**

1. Partea dreaptă e deplasează la stânga cu 4 biti :

01010110011001010111001001101111<<4 01100110010101110010011011110000

1. La rezultatul (1) se adaugă valoarea cheie k2mod 2^32

01010010010001000011010111111101+ 01100001 01101110 01110101 01101100 mod 2^32=11001100010111111001011111100101

3. Parteadreapta se aduna cu I\*ɓ

01101110011010010110001101100001+1\*10011110001101110111100110111001mod2^32= 10000110010100000110111010001101

4.Rezultatul de la p (2) XOR Rezultatul de la p (3)

11001100010111111001011111100101XOR10000110010100000110111010001101 = 1001010000011111111100101101000

5.Partea dreapta se deplasează la dreapta cu 5 biți

01101110011010010110001101100001=0000011011100110100101100011011

6.La rezultatul (5) se adaugăvaloarea K3 mod 2^32

0000011011100110100101100011011+00110001001101110011000100110010mod 2^32=00110100101010100111110001001101

7.Rezultatul de la p (3) XOR Rezultatul de la p (6)

10000110010100000110111010001101 XOR00110100101010100111110001001101=10101001111100110011111101110

8. Parteastângă se aduna cu rezultatul p(7) mod 2^32

01000101 01010100 01001000 01000101+10101001111100110011111101110mod 2^32= 01010010010011100100010101010100

01010010010011100100010101010100**→ RNET**

**Partea impara**

1. Parteadreaptase deplasează la stânga cu 4 biți

<<4 01101110011010010110001101100001 = 11100110100101100011011000010000

1. La rezultatul (1) se adaugă valoarea K0 mod 2^32=

11100110100101100011011000010000 + 01100001 01101110 01110101 01101100 mod 2^32= 1100000101100011001011111111000

1. Parteadreaptase aduna cu I\*ɓ

01101110011010010110001101100001+1\*10011110001101110111100110111001mod2^32= 10000110010100000110111010001101

1. Rezultatul de la p (2) XOR Rezultatul de la p (3)

1100000101100011001011111111000 XOR 10000110010100000110111010001101 = 100011100110011010000010110010

1. Parteadreapta se deplasează la dreapta cu 5 biți

01101110011010010110001101100001=0000011011100110100101100011011

1. La rezultatul (5) se adaugă valoarea K0 mod 2^32

0000011011100110100101100011011+ 01100001 01101110 01110101 01101100 mod 2^32=01111101100011101010110100000011

1. Rezultatul de la p (3) XOR Rezultatul de la p (6)

10000110010100000110111010001101XOR 01111101100011101010110100000011= 01000101010101000100100001000101

01000101010101000100100001000101 **→ETHE**