1. В симметричной криптосистеме шифрования в которых используется один и тот же ключ для зашифровывания и расшифровывания информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение.

Именно поэтому симметричные криптосистемы называют криптосистемами секретным ключом — ключ шифрования должен быть доступен только тем, кому предназначено сообщение.

1. Поточный или потоковый шифр - это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. Поточный шифр реализует другой подход к симметричному шифрованию, нежели блочные шифры.
2. Криптографические хеш-функции — инструмент, который используется для выполнения целого ряда задач, включая аутентификацию, проверку целостности данных, защиту файлов и обнаружение зловредного ПО.

**Criptosisteme simetrice fluide: RC4**

n=2

2n =22 =4 – flux de biţi

Formăm vectrul S: 0123

m= Nico

Alegem cheia: 6M, K – vectorul cheii

Codul ASCII al cheii este: 1 → 54; M → 77;

Vectorul cheii este:

|  |  |  |  |
| --- | --- | --- | --- |
| 54 | 77 | 54 | 77 |

Depunem valorile codului ASCII al cheii:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **P** | **0** | **1** | **2** | **3** |
| **S** | 0 | 1 | 2 | 3 |
| **K** | 54 | 77 | 54 | 77 |

Efectuăm permutări asupra biţilor vectorului S:

Iniţial i=0, j=**0**.

**j=(j+K[i]+S[j]) mod 8**

1) i=**0**, j=(**0**+K[0]+S[0]) mod 4 = (0+54+0) mod 4 = 54 mod 4 = **2**;

SWAP(S[i],S[j])=SWAP(S[**0**],S[**2**])=2013=56 77 56 77

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P** | **0** | **1** | **2** | **3** |  |  |  |  |
| **S** | 2 | 0 | 1 | 3 |  |  |  |  |
| **K** | 56 | 77 | 56 | 77 |  |  |  |  |

2) i=**1**, j=(**1**+K[1]+S[1]) mod 4 = (1+77+0) mod 4 = 78 mod 4 = 2;

SWAP(S[i],S[j])=SWAP(S[**1**],S[2])=2103=56 56 77 77

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P** | **0** | **1** | **2** | **3** |  |  |  |  |
| **S** | 2 | 1 | 0 | 3 |  |  |  |  |
| **K** | 56 | 56 | 77 | 77 |  |  |  |  |

3) i=**2,** j=(2+K[2]+S[2]) mod 4 = (2+77+0) mod 4 = 79 mod 4 = 3;

SWAP(S[i],S[j])=SWAP(S[2],S[3])=2130= 55 49 49 55

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P** | **0** | **1** | **2** | **3** |  |  |  |  |
| **S** | 2 | 1 | 3 | 0 |  |  |  |  |
| **K** | 56 | 77 | 77 | 56 |  |  |  |  |

4) i=3, j=(3+K[3]+S[3]) mod 4 = (3+55+0) mod 4 = 58 mod 4 = 2;

SWAP(S[i],S[j])=SWAP(S[3],S[2])=12340567=55 49 55 49 49 55 49 55

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P** | **0** | **1** | **2** | **3** |  |  |  |  |
| **S** | 2 | 1 | 0 | 3 |  |  |  |  |
| **K** | 56 | 77 | 56 | 77 |  |  |  |  |

**CRIPTARE**

Alegem un mesaj pentru criptare m = Nico

Iniţial i=0, j=**0**.

i=(i+1) mod 4 = 1 mod 4 = 1.

j=(**j**+S[i]) mod 4 = (j+S[1]) mod 4 = (0+1) mod 4 = 1

Calculam o constanta **t**:

t=(S[i]+S[j]) mod 4 = (S[1]+S[1]) mod 4 = (1+1) mod 4 = 2mod4 = 2

**Criptul r = chr(ord(m)) XOR K[t] (Formula dlea shifrovania)**

, K[t] = K[2] = (56)10 = **(00111000)2** -cheia de criptare

m[0] = N → (78)10 = (01001110)2

m[1] = i → (105)10 = (01101001)2

m[2] = c → (99)10 = (01100011)2

m[3] = o → (111)10 = (01101111)2

1. r[0] = 01001110 XOR **00111000** = (0111 0110)2 = (118)10 → v
2. r[1] = 01101001 XOR **00111000** = (0101 0001)2 = (81)10 → Q
3. r[2] = 01100011 XOR **00111000** = (0101 1011)2 = (91)10 → [
4. r[3] = 01101111 XOR **00111000** = (0101 0111)2 = (87)10 → W

**Deci, mesajul m = „Nico” criptat este „vQ[W”**

**DECRIPTARE** Cript r = **vQ[W**

K=6M;

S= 2103

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **P** | **0** | **1** | **2** | **3** |
| **S** | 2 | 1 | 0 | 3 |
| **K** | 56 | 77 | 56 | 77 |

Iniţial i=0, j=0.

i = (i+1) mod 4 = 1 mod 4 = 1.

j = (j+S[i]) mod 4 = (j+S[1]) mod 4 = (0+1) mod 4 = 1

t=SWAP(S[1],S[1]) mod 4 = (1+1) mod 4 = 2

K[t] = K[2] = (56)10 = (**00111000**)2

**i = chr(ord(r)) XOR K**[t]

r[0] = v → (118)10 = (0111 0110)2

r[1] = Q → (81)10 = (0101 0001)2

r[2] = [ → (91)10 = (0101 1011)2

r[3] = W → (87)10 = (0101 0111)2

1. m[0] = 0111 0110 XOR **00111000** = (01001110)2 = (78)10 → N
2. m[1] = 0101 0001 XOR **00111000**= (01101001)2 = (105)10 → i
3. m[2] = 0101 1011 XOR **00111000**= (01100011)2 = (99)10 → c
4. m[3] = 0101 0111 XOR **00111000**= (01101111)2 = (111)10 → o

**Mesajul criptat r = „vQ[W” decriptat va fi: „Nico”.**