Algoritm Twofish, abifail

võtmete laiendus

Olgu meie võtmeks:

11110011 11001111 10100011 10110011 11110011 11001100 10110011 11110011
11001100 11110011 11001111 10100011

Pikendame kuni standardse pikkuseni 128:

11110011 11001111 10100011 10110011 11110011 11001100 10110011 11110011
11001100 11110011 11001111 10100011 00000000 00000000 00000000 00000000

K=N/64=128/64=2

Baitide massiivina:

m0=00000000
m1=00000000
m2=00000000
m3=00000000
m4=10100011
m5=11001111
m6=11110011
m7=11001100
m8=11110011
m9=10110011
m10=11001100
m11=11110011
m12=10110011
m13=10100011
m14=11001111
m15=11110011

Samuti Mi massiivina:

M0=m0*2^{8*0} +m1*2^{8*1} +m2*2^{8*2} +m3*2^{8*3} = m0=00000000*2^{8*0} +00000000*2^{8*1}
+00000000*2^{8*2} +00000000*2^{8*3}=00000000*00000001+00000000*100000000+
+00000000*1000000000000000+00000000*100000000000000000000000=00000000
00000000 00000000 00000000

M1=m4*2^{8*0} +m5*2^{8*1} +m6*2^{8*2} +m7*2^{8*3} =11001100*2^{8*0} +11110011*2^{8*1}
+11001111*2^{8*2} +10100011*2^{8*3} =
=11001100*00000001+11110011*100000000+11001111*1000000000000000+
+10100011*100000000000000000000000=
=11001100+1111001100000000+1100111100000000000000000+
+10100011000000000000000000000000=10100011 11001111 11110011 11001100

M2= 11110011*00000001+10110011*100000000+11001100*1000000000000000+
+11110011*100000000000000000000000=11110011+1011001100000000+
+1100110000000000000000+111100110000000000000000000000=
=11110011 11001100 10110011 11110011

Jne

Me=(M0, M2)=
=(00000000 00000000 00000000 00000000, 11110011 11001100 10110011 11110011)

Teisendus q

Sisendsõna arvutus. X=2iρ, $\rho=2^{24}+2^{16}+2^{8}+1$

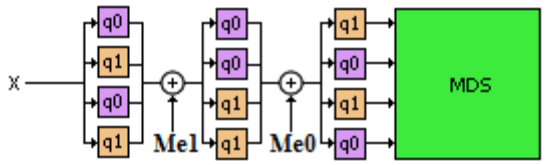
Olgu arvutamisel k2

$$k_{2i} = A_i + B_i \bmod 2^{32};$$
$$k_{2i+1} = (A_i + 2B_i \bmod 2^{32}) <<< 9.$$

$$A_i = h(2i\rho, M_e);$$
$$B_i = h((2i+1)\rho, M_o) <<< 8.$$

X=2*1*(224+216+28+1)=00000010*00000001*10000000100000000100000001=
=00000010 00000010 00000010 00000010

A1=h(00000010 00000010 00000010 00000010, Me)



k = 2

Me0=00000000 00000000 00000000 00000000 –esimene element Me-st

Me1=11110011 11001100 10110011 11110011- teine element Me-st

Jagame X neljaks osaks:

x1=00000010

x2=00000010

x3=00000010

x4=00000010

$$a_0 = \lfloor x/16 \rfloor;$$
$$b_0 = x \bmod 16;$$

Võtame x1, selle jaoks kasutame q0

a0=00000010/16=00000010/10000=0000

b0= x1 mod 16=00000010 mod 10000=0010

$$
\begin{aligned}
a_1 &= a_0 \oplus b_0;\\
b_1 &= a_0 \oplus (b_0 >>>_4 1) \oplus 8a_0 \bmod 16;\\
a_2 &= t_0(a_1);\\
b_2 &= t_1(b_1);\\
a_3 &= a_2 \oplus b_2;\\
b_3 &= a_2 \oplus (b_2 >>>_4 1) \oplus 8a_2 \bmod 16;\\
a_4 &= t_2(a_3);\\
b_4 &= t_3(b_3);\\
y &= 16b_4 + a_4.
\end{aligned}
$$

a1=a0 xor b0=0000 xor 0010=0010

b1=0000 xor (0010>>>1) xor 8*0000 mod 10000=0000 xor (0001) xor 0000= 0001

a2=t0(0010)=0111 – see on kahendkood arvust hex 7

b2=t1(0001)= 1100– see on kahendkood arvust hex C

a3= a2 xor b2=1100 xor 1110 = 0010

b3=0111 xor (1110>>>1) xor 8*0111 mod 10000=0111 xor 0111 xor 1000=1000

a4=t2(0010)= 0101

b4=t3(1000)= 1001

y=16*1001+0101=10000*1001+0101=10010101