AES kriptográfiai algoritmus

Smidla József

Rendszer- és Számítástudományi Tanszék
Pannon Egyetem

2012. 2. 28.

Tartalom

Bevezetés: Élet az AES előtt

Elől: DES (Data Encryption System)

1. IBM szakemberei fejlesztették ki
2. Blokk kódoló
3. 56 bites kulcs
4. Bit alapú
5. S-dobozok és P-dobozok építik fel

Problémák

1. Elavult, gyenge
2. Nehezen implementálható
3. Sokan nem bíztak benne

Az AES születése

Az amerikai kormánynak új titkosítási szabványra volt szüksége, amely biztonságosabb, és mindenki megbízik benne.

1. 1997-ben a NIST (National Institute of Standards and Technology) kriptográfiai versenyt ír ki
2. Elvárások az új szabvánnyal szemben:
   - Szimmetrikus blokk-kódoló
   - Minden részlete legyen nyilvános
   - 128, 192 és 256 bites kulcsok támogatása
   - Hardveresen és szoftveresen hatékonyan megvalósítható
   - Bárki használhassa
3. 2000-ben bejelentették, hogy a Rijndael nevű algoritmus nyert, alkotói: Joan Daemen és Vincent Rijmen

Alapműveletek

XOR

Kizáró vagy: A XOR B = C

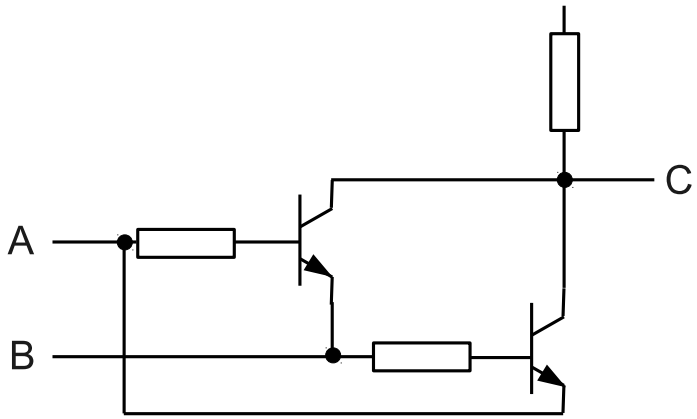
C akkor és csak akkor igaz, ha A és B nem egyenlőek

Igazságtábla

A	B	A XOR B = C
0	0	0
0	1	1
1	0	1
1	1	0

$\rightarrow$

A	B	A XOR B = C	C XOR B $\equiv$ A
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1



Alapműveletek: Összeadás, kivonás

Alapegység: polinomokat reprezentáló bájtok
0x53 = 01010011 = $x^6 + x^4 + x + 1$
A műveleteket ilyen polinomok között végezzük, GF(2^8) algebra szerint.

Összeadás, kivonás

A $\oplus$ B = A $\ominus$ B = A XOR B
Példa:
0x53 $\oplus$ 0xAB = 0x53 $\ominus$ 0xAB = 01010011 $\oplus$ 10101011

```
01010011
10101011
--------
```

11111000 = 0xF8

$$(x^6 + x^4 + x + 1) \oplus (x^7 + x^5 + x^3 + x + 1) = x^7 + x^6 + x^5 + x^4 + x^3$$

Alapműveletek: Szorzás

Szorozzuk össze az 0x53 és 0xAB által reprezentált polinomokat GF(2^8) algebrában:

$$(x^6 + x^4 + x + 1) \circ (x^7 + x^5 + x^3 + x + 1) =$$

$$[(x^{13} + \cancel{x^{11}} + x^8 + x^7) \oplus (\cancel{x^{11}} + x^9 + x^6 + x^5)] \oplus [(x^9 + \cancel{x^7} + x^4 + x^3) \oplus (\cancel{x^7} + x^5 + x^2 + x)] \oplus (x^6 + x^4 + x + 1) =$$

$$(x^{13} + \cancel{x^9} + x^8 + x^7 + x^6 + \cancel{x^5}) \oplus (\cancel{x^9} + \cancel{x^5} + x^4 + x^3 + x^2 + x) \oplus (x^6 + x^4 + x + 1) =$$

$$(x^{13} + x^8 + x^7 + \cancel{x^6} + \cancel{x^4} + x^3 + x^2 + \cancel{x}) \oplus (\cancel{x^6} + \cancel{x^4} + \cancel{x} + 1) =$$

$$\underline{x^{13} + x^8 + x^7 + x^3 + x^2 + 1}$$

Viszont a szorzást modulo aritmetikával végezzük el:

$$(x^6 + x^4 + x + 1) \circ (x^7 + x^5 + x^3 + x + 1) \mod (x^8 + x^4 + x^3 + x + 1)$$

$$x^{13} + x^8 + x^7 + x^3 + x^2 + 1 \mod (x^8 + x^4 + x^3 + x + 1)$$

Alapműveletek: Szorzás

$x^{13} + x^8 + x^7 + x^3 + x^2 + 1 \mod (x^8 + x^4 + x^3 + x + 1)$

1. Szorozzuk be az $x^8 + x^4 + x^3 + x + 1$ polinomot x^5-el, és a kapott polinomot adjuk hozzá az eredetihez:

   $(\cancel{x^{13}} + \cancel{x^8} + x^7 + x^3 + x^2 + 1) \oplus (\cancel{x^{13}} + x^9 + \cancel{x^8} + x^6 + x^5) =$

   $x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$

2. Szorozzuk be az $x^8 + x^4 + x^3 + x + 1$ polinomot x-el, és a kapott polinomot adjuk hozzá az eredményhez:

   $(\cancel{x^9} + x^7 + x^6 + \cancel{x^5} + x^3 + \cancel{x^2} + 1) \oplus (\cancel{x^9} + \cancel{x^5} + x^4 + \cancel{x^2} + x) =$
   $\underline{x^7 + x^6 + x^4 + x^3 + x + 1}$

Tehát:
$(x^6 + x^4 + x + 1) \circ (x^7 + x^5 + x^3 + x + 1) \mod (x^8 + x^4 + x^3 + x + 1) =$

$$\underline{\underline{x^7 + x^6 + x^4 + x^3 + x + 1}}$$

Alapműveletek: Szorzás

Szorzás bitműveletek segítségével:

`0x53 ∘ 0xAB mod 0x11B = 01010011 ∘ 10101011 mod 100011011`

- Végezzük el a szorzást: Az 10101011 bitsorozat 7., 5., 3., 1. és 0. bitje 1 $\longrightarrow$ Toljuk el a 01010011 bitsorozatot 7, 5, 3, 1, és 0 pozícióval, és adjuk össze a keletkezett bitsorozatokat
-

0 1 0 1 0 0 1 1 0 0 0 0 0 0 0	Eltolva 7 bittel
0 1 0 1 0 0 1 1 0 0 0 0 0	Eltolva 5 bittel
0 1 0 1 0 0 1 1 0 0 0	Eltolva 3 bittel
0 1 0 1 0 0 1 1 0	Eltolva 1 bittel
0 1 0 1 0 0 1 1	Eltolva 0 bittel
XOR ----------	
0 1 0 0 0 0 1 1 0 0 0 1 1 0 1	

- 1-esek indexei: 13, 8, 7, 3, 2, 0
  A bitsorozat által reprezentált polinom: $x^{13} + x^8 + x^7 + x^3 + x^2 + 1$

Alapműveletek: Szorzás

- A szorzás első lépéseként kapott bitsorozat: 10000110001101
- Van a 7-esnél nagyobb pozíción 1-es bit $\longrightarrow$ modulo aritmetika
- Toljuk el az 100011011 bitsorozatot úgy, hogy a legmagasabb helyi értékű bitje az előző bitsorozat 1-es bitjeire illeszkedjen, majd a kapott bitsorozatokat adjuk össze az eredetivel

  1 0 0 0 0 1 1 0 0 0 1 1 0 1 Redukálandó bitsorozat

  1 0 0 0 1 1 0 1 1 0 0 0 0 0 5-el eltolt redukáló bitsorozat

  ---------- XOR

  0 0 0 0 1 0 1 1 1 0 1 1 0 1 Legmagasabb 1-es bit: 9.

  1 0 0 0 1 1 0 1 1 0 1-el eltolt redukáló bitsorozat

  ---------- XOR

  0 0 0 0 0 0 1 1 0 1 1 0 1 1 Legmagasabb 1-es bit: 7. ✓
- A kapott polinom: $x^7 + x^6 + x^4 + x^3 + x + 1$

Kulcs kiterjesztés

Kulcs kiterjesztés

A 128 bites kulcsot ki kell terjeszteni, hogy a titkosítás minden iterációjában más kulcs értékeket használjunk
A kulcs: $k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15}$
A kulcs bájtjait 4 sorba rendezzük:

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

Ezt a kulcs táblázatot kiterjesztjük 44 oszlopra
$w[i]$: a kulcs táblázat i. oszlopa, ahol $0 \leq i < 44$

Kulcs kiterjesztés

A kulcs oszlop minden $i \geq 4$ sorszámú oszlopát a következő módon számoljuk ki:

1. Legyen temp $= w[i-1]$
2. Ha i osztható 4-el, akkor:
   a) temp bájtjait forgatjuk: temp $= [w_0, w_1, w_2, w_3] \longrightarrow [w_1, w_2, w_3, w_0]$
   b) temp minden bájtját egy S-doboz segítségével kicseréljük
   c) temp új első bájtjához hozzáadjuk az $x^{i/4-1} \mod (x^8 + x^4 + x^3 + x + 1)$ polinomot reprezentáló bájtot
3. $w[i] = w[i-4]$ XOR temp

Kulcs kiterjesztés példa

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF				
0x15	0xD9	0xB7	0x7F				
0x71	0xE8	0xAD	0x67				
0xC9	0x59	0xD6	0x98				

1. i = 4, temp = [0xAF, 0x7F, 0x67, 0x98], i osztható 4-el
2. temp-et forgatjuk: temp = [0x7F, 0x67, 0x98, 0xAF]
3. temp bájtjait kicseréljük: temp = [0xD2, 0x85, 0x46, 0x79]
4. $x^{i/4-1} = x^0 = 1 =$ 0x01, ezt XOR-oljuk temp első bájtjával: temp = [0xD3, 0x85, 0x46, 0x79]
5. w[4] = w[0] XOR temp = [0xDC, 0x90, 0x37, 0xB0]

Kulcs kiterjesztés példa

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC			
0x15	0xD9	0xB7	0x7F	0x90			
0x71	0xE8	0xAD	0x67	0x37			
0xC9	0x59	0xD6	0x98	0xB0			

1. i = 5, nem osztható 4-el, temp = w[4] = [0xDC, 0x90, 0x37, 0xB0]
2. w[5] = w[1] XOR temp = [0x9B, 0x49, 0xDF, 0xE9]

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC	0x9B		
0x15	0xD9	0xB7	0x7F	0x90	0x49		
0x71	0xE8	0xAD	0x67	0x37	0xDF		
0xC9	0x59	0xD6	0x98	0xB0	0xE9		

Kulcs kiterjesztés példa

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC	0x9B		
0x15	0xD9	0xB7	0x7F	0x90	0x49		
0x71	0xE8	0xAD	0x67	0x37	0xDF		
0xC9	0x59	0xD6	0x98	0xB0	0xE9		

1. i = 6, nem osztható 4-el, temp = w[5] = [0x9B, 0x49, 0xDF, 0xE9]
2. w[6] = w[2] XOR temp = [0x97, 0xFE, 0x72, 0x3F]

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC	0x9B	0x97	
0x15	0xD9	0xB7	0x7F	0x90	0x49	0xFE	
0x71	0xE8	0xAD	0x67	0x37	0xDF	0x72	
0xC9	0x59	0xD6	0x98	0xB0	0xE9	0x3F	

Kulcs kiterjesztés példa

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC	0x9B	0x97	
0x15	0xD9	0xB7	0x7F	0x90	0x49	0xFE	
0x71	0xE8	0xAD	0x67	0x37	0xDF	0x72	
0xC9	0x59	0xD6	0x98	0xB0	0xE9	0x3F	

1. i = 7, nem osztható 4-el, temp = w[6] = [0x97, 0xFE, 0x72, 0x3F]
2. w[7] = w[3] XOR temp = [0x38, 0x81, 0x15, 0xA7]

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC	0x9B	0x97	0x38
0x15	0xD9	0xB7	0x7F	0x90	0x49	0xFE	0x81
0x71	0xE8	0xAD	0x67	0x37	0xDF	0x72	0x15
0xC9	0x59	0xD6	0x98	0xB0	0xE9	0x3F	0xA7

Kódolás

Kódolás

1. Beolvassuk a kódolandó 16 bájtos blokkot az állapot táblázatba
2. Az állapothoz hozzáadjuk a kulcs táblázat [0-3]-as oszlopait
3. Végrehajtunk 9 iterációt, jelölje *i* az aktuális iteráció sorszámát, és *i* értéke 1-től 9-ig halad
   a) Bájt csere
   b) Sorok eltolása
   c) Oszlopok keverése
   d) Az állapothoz hozzáadjuk a kulcs táblázat [i*4, (i+1)*4-1] oszlopait
4. Bájt csere
5. Sorok eltolása
6. Az állapothoz hozzáadjuk a kulcs táblázat [40, 43]-as oszlopait

A kulcs hozzáadása után 10 iterációt hajtunk végre, de az utolsóból kihagyjuk az oszlopok keverését.

Inicializálás

Bemenet: 16 bájtos blokk, és 16 bájtos kulcs

Bemenet: $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}$

A bemenetet egy 4*4-es táblázatba rendezzük

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

A titkosító algoritmus ezen táblázaton végez el különféle transzformációkat.

Kulcs hozzáadása

A kódolás i. iterációjában a kiterjesztett kulcs $[i * 4, (i + 1) * 4 - 1]$ oszlopait hozzáadjuk a jelenlegi állapot oszlopaihoz.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\oplus$

$w_{0,i}$	$w_{0,i+1}$	$w_{0,i+2}$	$w_{0,i+3}$
$w_{1,i}$	$w_{1,i+1}$	$w_{1,i+2}$	$w_{1,i+3}$
$w_{2,i}$	$w_{2,i+1}$	$w_{2,i+2}$	$w_{2,i+3}$
$w_{3,i}$	$w_{3,i+1}$	$w_{3,i+2}$	$w_{3,i+3}$

$=$

$s_{0,0} \oplus w_{0,i}$	$s_{0,1} \oplus w_{0,i+1}$	$s_{0,2} \oplus w_{0,i+2}$	$s_{0,3} \oplus w_{0,i+3}$
$s_{1,0} \oplus w_{1,i}$	$s_{1,1} \oplus w_{1,i+1}$	$s_{1,2} \oplus w_{1,i+2}$	$s_{1,3} \oplus w_{1,i+3}$
$s_{2,0} \oplus w_{2,i}$	$s_{2,1} \oplus w_{2,i+1}$	$s_{2,2} \oplus w_{2,i+2}$	$s_{2,3} \oplus w_{2,i+3}$
$s_{3,0} \oplus w_{3,i}$	$s_{3,1} \oplus w_{3,i+1}$	$s_{3,2} \oplus w_{3,i+2}$	$s_{3,3} \oplus w_{3,i+3}$

Bájt helyettesítés

Minden bájt értékét lecseréljük egy S-doboz szerint.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\Longrightarrow$

$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

Ahol $s'_{i,j} = \text{S-doboz}(s_{i,j})$

Bájt helyettesítés

S-doboz:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Példa: 0x13-at 0x7D-re helyettesítjük, azaz az 1-es sor és 3-as oszlopában lévő elemre.

Sor forgatás

A második sor elemeit 1-el balra forgatjuk, a harmadik sort 2-vel, a negyediket 3-al:

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\Longrightarrow$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$\mathbf{s_{1,0}}$
$s_{2,2}$	$s_{2,3}$	$\mathbf{s_{2,0}}$	$\mathbf{s_{2,1}}$
$s_{3,3}$	$\mathbf{s_{3,0}}$	$\mathbf{s_{3,1}}$	$\mathbf{s_{3,2}}$

Oszlop keverés

Az állapot táblázat c. oszlopának elemeit az alábbi módon keverjük össze:

$$s'_{0,c} = (0x02 \circ s_{0,c}) \oplus (0x03 \circ s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$
$$s'_{1,c} = s_{0,c} \oplus (0x02 \circ s_{1,c}) \oplus (0x03 \circ s_{2,c}) \oplus s_{3,c}$$
$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (0x02 \circ s_{2,c}) \oplus (0x03 \circ s_{3,c})$$
$$s'_{3,c} = (0x03 \circ s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (0x02 \circ s_{3,c})$$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\Longrightarrow$

$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

Dekódolás

Dekódolás

- Az üzenet dekódolásához a kódolási lépések inverzét kell végrehajtani. Ugyanazt a kiterjesztett kulcs táblázatot használjuk, amit a kódoló is alkalmazott.
- Tudjuk, hogy A XOR B = C, és C XOR B = A, azaz ha egy kulcs bitsorozatot 2x XOR-olunk egy A bitsorozathoz, akkor visszakapjuk az eredeti bitsorozatot $\rightarrow$ A kulcs táblázat sorait visszafele haladva kell hozzáadni az állapothoz.
- A kódolásnál alkalmazott lépések inverzeit fordított sorrendben alkalmazzuk.

Dekódolás

1. Beolvassuk a dekódolandó 16 bájtos blokkot az állapot táblázatba
2. Az állapothoz hozzáadjuk a kulcs táblázat [40-43]-as oszlopait
3. Végrehajtunk 9 iterációt, jelölje *i* az aktuális iteráció sorszámát, és *i* értéke 9-től visszafele halad 1-ig
   a) Inverz sor forgatás
   b) Inverz bájt csere
   c) Az állapothoz hozzáadjuk a kulcs táblázat [i*4, (i+1)*4-1] oszlopait
   d) Inverz oszlop keverés
4. Inverz sor forgatás
5. Inverz bájt csere
6. Az állapothoz hozzáadjuk a kulcs táblázat [0, 3]-as oszlopait

Inverz sor forgatás

A kódolásnál használt sor forgatás inverze: A sorokat a másik irányba kell forgatni.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\Longrightarrow$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$\mathbf{s_{1,3}}$	$s_{1,0}$	$s_{1,1}$	$s_{1,2}$
$\mathbf{s_{2,2}}$	$\mathbf{s_{2,3}}$	$s_{2,0}$	$s_{2,1}$
$\mathbf{s_{3,1}}$	$\mathbf{s_{3,2}}$	$\mathbf{s_{3,3}}$	$s_{3,0}$

Inverz bájt helyettesítés

Az állapot bájtjait az inverz S-doboz alapján cseréljük ki.
Inverz S-doboz:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Inverz oszlop keverés

Az állapot táblázat c. oszlopának elemeit az alábbi módon keverjük össze:

$$s'_{0,c} = (0x0E \circ s_{0,c}) \oplus (0x0B \circ s_{1,c}) \oplus (0x0D \circ s_{2,c}) \oplus (0x09 \circ s_{3,c})$$
$$s'_{1,c} = (0x09 \circ s_{0,c}) \oplus (0x0E \circ s_{1,c}) \oplus (0x0B \circ s_{2,c}) \oplus (0x0D \circ s_{3,c})$$
$$s'_{2,c} = (0x0D \circ s_{0,c}) \oplus (0x09 \circ s_{1,c}) \oplus (0x0E \circ s_{2,c}) \oplus (0x0B \circ s_{3,c})$$
$$s'_{3,c} = (0x0B \circ s_{0,c}) \oplus (0x0D \circ s_{1,c}) \oplus (0x09 \circ s_{2,c}) \oplus (0x0E \circ s_{3,c})$$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\Longrightarrow$

$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

Példa

Példa

Kódoljuk a (61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70) üzenetet a
(0F 15 71 C9 47 D9 E8 59 0C B7 AD D6 AF 7F 67 98) kulcs segítségével!

1. A kezdő állapot táblázat:

0x61	0x65	0x69	0x6D
0x62	0x66	0x6A	0x6E
0x63	0x67	0x6B	0x6F
0x64	0x68	0x6C	0x70

2. A kulcs táblázat első 4 oszlopa:

0x0F	0x47	0x0C	0xAF
0x15	0xD9	0xB7	0x7F
0x71	0xE8	0xAD	0x67
0xC9	0x59	0xD6	0x98

Példa: kulcs kiterjesztés

1. temp = w[3] = (0xAF 0x7F 0x67 0x98)
2. temp forgatása: temp = (0x7F 0x67 0x98 0xAF)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0xD2 0x85 0x46 0x79)
4. temp[0]-hoz hozzáadunk 0x01-et: temp = (0xD3 0x85 0x46 0x79)
5. w[4] = w[0] XOR temp, w[5] = w[1] XOR w[4], w[6] = w[2] XOR w[5], w[7] = w[3] XOR w[6]

A kulcs táblázat első 8 oszlopa:

w[0]	w[1]	w[2]	w[3]	w[4]	w[5]	w[6]	w[7]
0x0F	0x47	0x0C	0xAF	0xDC	0x9B	0x97	0x38
0x15	0xD9	0xB7	0x7F	0x90	0x49	0xFE	0x81
0x71	0xE8	0xAD	0x67	0x37	0xDF	0x72	0x15
0xC9	0x59	0xD6	0x98	0xB0	0xE9	0x3F	0xA7

Példa: kulcs kiterjesztés

1. temp = w[7] = (0x38 0x81 0x15 0xA7)
2. temp forgatása: temp = (0x81 0x15 0xA7 0x38)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0x0C 0x59 0x5C 0x07)
4. temp[0]-hoz hozzáadunk 0x02-t: temp = (0x0E 0x59 0x5C 0x07)
5. w[8] = w[4] XOR temp, w[9] = w[5] XOR w[8], w[10] = w[6] XOR w[9], w[11] = w[7] XOR w[10]

A kulcs táblázat [4,11] oszlopai:

w[4]	w[5]	w[6]	w[7]	w[8]	w[9]	w[10]	w[11]
0xDC	0x9B	0x97	0x38	0xD2	0x49	0xDE	0xE6
0x90	0x49	0xFE	0x81	0xC9	0x80	0x7E	0xFF
0x37	0xDF	0x72	0x15	0x6B	0xB4	0xC6	0xD3
0xB0	0xE9	0x3F	0xA7	0xB7	0x5E	0x61	0xC6

Példa: kulcs kiterjesztés

1. temp = w[11] = (0xE6 0xFF 0xD3 0xC6)
2. temp forgatása: temp = (0xFF 0xD3 0xC6 0xE6)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0x16 0x66 0xB4 0x8E)
4. temp[0]-hoz hozzáadunk 0x04-t: temp = (0x12 0x66 0xB4 0x8E)
5. w[12] = w[8] XOR temp, w[13] = w[9] XOR w[12], w[14] = w[10] XOR w[13], w[15] = w[11] XOR w[14]

A kulcs táblázat [8,15] oszlopai:

w[8]	w[9]	w[10]	w[11]	w[12]	w[13]	w[14]	w[15]
0xD2	0x49	0xDE	0xE6	0xC0	0x89	0x57	0xB1
0xC9	0x80	0x7E	0xFF	0xAF	0x2F	0x51	0xAE
0x6B	0xB4	0xC6	0xD3	0xDF	0x6B	0xAD	0x7E
0xB7	0x5E	0x61	0xC6	0x39	0x67	0x06	0xC0

Példa: kulcs kiterjesztés

1. temp = w[15] = (0xB1 0xAE 0x7E 0xC0)
2. temp forgatása: temp = (0xAE 0x7E 0xC0 0xB1)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0xE4 0xF3 0xBA 0xC8)
4. temp[0]-hoz hozzáadunk 0x08-t: temp = (0xEC 0xF3 0xBA 0xC8)
5. w[16] = w[12] XOR temp, w[17] = w[13] XOR w[16], w[18] = w[14] XOR w[17], w[19] = w[15] XOR w[18]

A kulcs táblázat [12,19] oszlopai:

w[12]	w[13]	w[14]	w[15]	w[16]	w[17]	w[18]	w[19]
0xC0	0x89	0x57	0xB1	0x2C	0xA5	0xF2	0x43
0xAF	0x2F	0x51	0xAE	0x5C	0x73	0x22	0x8C
0xDF	0x6B	0xAD	0x7E	0x65	0x0E	0xA3	0xDD
0x39	0x67	0x06	0xC0	0xF1	0x96	0x90	0x50

Példa: kulcs kiterjesztés

1. temp = w[19] = (0x43 0x8C 0xDD 0x50)
2. temp forgatása: temp = (0x8C 0xDD 0x50 0x43)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0x64 0xC1 0x53 0x1A)
4. temp[0]-hoz hozzáadunk 0x10-t: temp = (0x74 0xC1 0x53 0x1A)
5. w[20] = w[16] XOR temp, w[21] = w[17] XOR w[20], w[22] = w[18] XOR w[21], w[23] = w[19] XOR w[22]

A kulcs táblázat [16,23] oszlopai:

w[16]	w[17]	w[18]	w[19]	w[20]	w[21]	w[22]	w[23]
0x2C	0xA5	0xF2	0x43	0x58	0xFD	0x0F	0x4C
0x5C	0x73	0x22	0x8C	0x9D	0xEE	0xCC	0x40
0x65	0x0E	0xA3	0xDD	0x36	0x38	0x9B	0x46
0xF1	0x96	0x90	0x50	0xEB	0x7D	0xED	0xBD

Példa: kulcs kiterjesztés

1. temp = w[23] = (0x4C 0x40 0x46 0xBD)
2. temp forgatása: temp = (0x40 0x46 0xBD 0x4C)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0x09 0x5A 0x7A 0x29)
4. temp[0]-hoz hozzáadunk 0x20-t: temp = (0x29 0x5A 0x7A 0x29)
5. w[24] = w[20] XOR temp, w[25] = w[21] XOR w[24], w[26] = w[22] XOR w[25], w[27] = w[23] XOR w[26]

A kulcs táblázat [20,27] oszlopai:

w[20]	w[21]	w[22]	w[23]	w[24]	w[25]	w[26]	w[27]
0x58	0xFD	0x0F	0x4C	0x71	0x8C	0x83	0xCF
0x9D	0xEE	0xCC	0x40	0xC7	0x29	0xE5	0xA5
0x36	0x38	0x9B	0x46	0x4C	0x74	0xEF	0xA9
0xEB	0x7D	0xED	0xBD	0xC2	0xBF	0x52	0xEF

Példa: kulcs kiterjesztés

1. temp = w[27] = (0xCF 0xA5 0xA9 0xEF)
2. temp forgatása: temp = (0xA5 0xA9 0xEF 0xCF)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0x06 0xD3 0xDF 0x8A)
4. temp[0]-hoz hozzáadunk 0x40-t: temp = (0x46 0xD3 0xDF 0x8A)
5. w[28] = w[24] XOR temp, w[29] = w[25] XOR w[27], w[30] = w[26] XOR w[29], w[31] = w[27] XOR w[30]

A kulcs táblázat [24, 31] oszlopai:

w[24]	w[25]	w[26]	w[27]	w[28]	w[29]	w[30]	w[31]
0x71	0x8C	0x83	0xCF	0x37	0xBB	0x38	0xF7
0xC7	0x29	0xE5	0xA5	0x14	0x3D	0xD8	0x7D
0x4C	0x74	0xEF	0xA9	0x93	0xE7	0x08	0xA1
0xC2	0xBF	0x52	0xEF	0x48	0xF7	0xA5	0x4A

Példa: kulcs kiterjesztés

1. temp = w[31] = (0xF7 0x7D 0xA1 0x4A)
2. temp forgatása: temp = (0x7D 0xA1 0x4A 0xF7)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0xFF 0x32 0xD6 0x68)
4. temp[0]-hoz hozzáadunk 0x80-t: temp = (0x7F 0x32 0xD6 0x68)
5. w[32] = w[28] XOR temp, w[33] = w[29] XOR w[32], w[34] = w[30] XOR w[33], w[35] = w[31] XOR w[34]

A kulcs táblázat [28, 35] oszlopai:

w[28]	w[29]	w[30]	w[31]	w[32]	w[33]	w[34]	w[35]
0x37	0xBB	0x38	0xF7	0x48	0xF3	0xCB	0x3C
0x14	0x3D	0xD8	0x7D	0x26	0x1B	0xC3	0xBE
0x93	0xE7	0x08	0xA1	0x45	0xA2	0xAA	0x0B
0x48	0xF7	0xA5	0x4A	0x20	0xD7	0x72	0x38

Példa: kulcs kiterjesztés

1. temp = w[35] = (0x3C 0xBE 0x0B 0x38)
2. temp forgatása: temp = (0xBE 0x0B 0x38 0x3C)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0xAE 0x2B 0x07 0xEB)
4. temp[0]-hoz hozzáadunk 0x1B-t: temp = (0xB5 0x2B 0x07 0xEB)
5. w[36] = w[32] XOR temp, w[37] = w[33] XOR w[36], w[38] = w[34] XOR w[37], w[39] = w[35] XOR w[38]

A kulcs táblázat [32, 39] oszlopai:

w[32]	w[33]	w[34]	w[35]	w[36]	w[37]	w[38]	w[39]
0x48	0xF3	0xCB	0x3C	0xFD	0x0E	0xC5	0xF9
0x26	0x1B	0xC3	0xBE	0x0D	0x16	0xD5	0x6B
0x45	0xA2	0xAA	0x0B	0x42	0xE0	0x4A	0x41
0x20	0xD7	0x72	0x38	0xCB	0x1C	0x6E	0x56

Példa: kulcs kiterjesztés

1. temp = w[39] = (0xF9 0x6B 0x41 0x56)
2. temp forgatása: temp = (0x6B 0x41 0x56 0xF9)
3. temp bájtjainak helyettesítése S-dobozzal: temp = (0x7F 0x83 0xB1 0x99)
4. temp[0]-hoz hozzáadunk 0x36-t: temp = (0x49 0x83 0xB1 0x99)
5. w[40] = w[36] XOR temp, w[41] = w[37] XOR w[40], w[42] = w[38] XOR w[41], w[43] = w[39] XOR w[42]

A kulcs táblázat [36, 43] oszlopai:

w[36]	w[37]	w[38]	w[39]	w[40]	w[41]	w[42]	w[43]
0xFD	0x0E	0xC5	0xF9	0xB4	0xBA	0x7F	0x86
0x0D	0x16	0xD5	0x6B	0x8E	0x98	0x4D	0x26
0x42	0xE0	0x4A	0x41	0xF3	0x13	0x59	0x18
0xCB	0x1C	0x6E	0x56	0x52	0x4E	0x20	0x76

Példa: Kulcs hozzáadása az iterációk előtt

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [0,3] oszlopait:

0x61	0x65	0x69	0x6D
0x62	0x66	0x6A	0x6E
0x63	0x67	0x6B	0x6F
0x64	0x68	0x6C	0x70

$\oplus$

0x0F	0x47	0x0C	0xAF
0x15	0xD9	0xB7	0x7F
0x71	0xE8	0xAD	0x67
0xC9	0x59	0xD6	0x98

$=$

0x6E	0x22	0x65	0xC2
0x77	0xBF	0xDD	0x11
0x12	0x8F	0xC6	0x08
0xAD	0x31	0xBA	0xE8

Példa: 1. iteráció

0x6E	0x22	0x65	0xC2
0x77	0xBF	0xDD	0x11
0x12	0x8F	0xC6	0x08
0xAD	0x31	0xBA	0xE8

S-doboz →

0x9F	0x93	0x4D	0x25
0xF5	0x08	0xC1	0x82
0xC9	0x73	0xB4	0x30
0x95	0xC7	0xF4	0x9B

Sor forgatás →

0x9F	0x93	0x4D	0x25
0x08	0xC1	0x82	0xF5
0xB4	0x30	0xC9	0x73
0x9B	0x95	0xC7	0xF4

Oszlop keverés →

0x12	0xC0	0x09	0xC9
0xD3	0xCF	0xD5	0xB5
0x52	0x96	0x14	0x31
0x2B	0x6E	0x09	0x1A

Példa: Kulcs hozzáadása az 1. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [4,7] oszlopait:

0x12	0xC0	0x09	0xC9
0xD3	0xCF	0xD5	0xB5
0x52	0x96	0x14	0x31
0x2B	0x6E	0x09	0x1A

$\oplus$

0xDC	0x9B	0x97	0x38
0x90	0x49	0xFE	0x81
0x37	0xDF	0x72	0x15
0xB0	0xE9	0x3F	0xA7

$=$

0xCE	0x5B	0x9E	0xF1
0x43	0x86	0x2B	0x34
0x65	0x49	0x66	0x24
0x9B	0x87	0x36	0xBD

Példa: 2. iteráció

0xCE	0x5B	0x9E	0xF1
0x43	0x86	0x2B	0x34
0x65	0x49	0x66	0x24
0x9B	0x87	0x36	0xBD

S-doboz →

0x8B	0x39	0x0B	0xA1
0x1A	0x44	0xF1	0x18
0x4D	0x3B	0x33	0x36
0x14	0x17	0x05	0x7A

Sor forgatás →

0x8B	0x39	0x0B	0xA1
0x44	0xF1	0x18	0x1A
0x33	0x36	0x4D	0x3B
0x7A	0x14	0x17	0x05

Oszlop keverés →

0x88	0x58	0x64	0x49
0x2C	0x8E	0xFB	0xDD
0x27	0x98	0xB0	0xC2
0x05	0xA4	0x66	0xD3

Példa: Kulcs hozzáadása a 2. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [8,11] oszlopait:

0x88	0x58	0x64	0x49
0x2C	0x8E	0xFB	0xDD
0x27	0x98	0xB0	0xC2
0x05	0xA4	0x66	0xD3

$\oplus$

0xD2	0x49	0xDE	0xE6
0xC9	0x80	0x7E	0xFF
0x6B	0xB4	0xC6	0xD3
0xB7	0x5E	0x61	0xC6

$=$

0x5A	0x11	0xBA	0xAF
0xE5	0x0E	0x85	0x22
0x4C	0x2C	0x76	0x11
0xB2	0xFA	0x07	0x15

Példa: 3. iteráció

0x5A	0x11	0xBA	0xAF
0xE5	0x0E	0x85	0x22
0x4C	0x2C	0x76	0x11
0xB2	0xFA	0x07	0x15

S-doboz →

0xBE	0x82	0xF4	0x79
0xD9	0xAB	0x97	0x93
0x29	0x71	0x38	0x82
0x37	0x2D	0xC5	0x59

Sor forgatás →

0xBE	0x82	0xF4	0x79
0xAB	0x97	0x93	0xD9
0x38	0x82	0x29	0x71
0x59	0x37	0x2D	0xC5

Oszlop keverés →

0xE0	0x08	0x59	0x36
0xE2	0x1D	0x9F	0x86
0x8E	0x53	0x42	0x16
0xF8	0xE6	0xE7	0xB2

Példa: Kulcs hozzáadása a 3. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [12,15] oszlopait:

0xE0	0x08	0x59	0x36
0xE2	0x1D	0x9F	0x86
0x8E	0x53	0x42	0x16
0xF8	0xE6	0xE7	0xB2

$\oplus$

0xC0	0x89	0x57	0xB1
0xAF	0x2F	0x51	0xAE
0xDF	0x6B	0xAD	0x7E
0x39	0x67	0x06	0xC0

$=$

0x20	0x81	0x0E	0x87
0x4D	0x32	0xCE	0x28
0x51	0x38	0xEF	0x68
0xC1	0x81	0xE1	0x72

Példa: 4. iteráció

0x20	0x81	0x0E	0x87
0x4D	0x32	0xCE	0x28
0x51	0x38	0xEF	0x68
0xC1	0x81	0xE1	0x72

S-doboz →

0xB7	0x0C	0xAB	0x17
0xE3	0x23	0x8B	0x34
0xD1	0x07	0xDF	0x45
0x78	0x0C	0xF8	0x40

Sor forgatás →

0xB7	0x0C	0xAB	0x17
0x23	0x8B	0x34	0xE3
0xDF	0x45	0xD1	0x07
0x40	0x78	0x0C	0xF8

Oszlop keverés →

0x8F	0xA3	0xCC	0xEF
0xCB	0xB6	0xA7	0x3B
0xF1	0x85	0x32	0xE9
0xBE	0x2A	0x1B	0x36

Példa: Kulcs hozzáadása a 4. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [16,19] oszlopait:

0x8F	0xA3	0xCC	0xEF
0xCB	0xB6	0xA7	0x3B
0xF1	0x85	0x32	0xE9
0xBE	0x2A	0x1B	0x36

$\oplus$

0x2C	0xA5	0xF2	0x43
0x5C	0x73	0x22	0x8C
0x65	0x0E	0xA3	0xDD
0xF1	0x96	0x90	0x50

$=$

0xA3	0x06	0x3E	0xAC
0x97	0xC5	0x85	0xB7
0x94	0x8B	0x91	0x34
0x4F	0xBC	0x8B	0x66

Példa: 5. iteráció

0xA3	0x06	0x3E	0xAC
0x97	0xC5	0x85	0xB7
0x94	0x8B	0x91	0x34
0x4F	0xBC	0x8B	0x66

S-doboz →

0x0A	0x6F	0xB2	0x91
0x88	0xA6	0x97	0xA9
0x22	0x3D	0x81	0x18
0x84	0x65	0x3D	0x33

Sor forgatás →

0x0A	0x6F	0xB2	0x91
0xA6	0x97	0xA9	0x88
0x81	0x18	0x22	0x3D
0x33	0x84	0x65	0x3D

Oszlop keverés →

0x57	0xE0	0xD8	0xBA
0xF6	0xF6	0xF8	0xE0
0xE0	0x5F	0xF0	0x24
0x5F	0x2D	0x8C	0x67

Példa: Kulcs hozzáadása az 5. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [20,23] oszlopait:

0x57	0xE0	0xD8	0xBA
0xF6	0xF6	0xF8	0xE0
0xE0	0x5F	0xF0	0x24
0x5F	0x2D	0x8C	0x67

$\oplus$

0x58	0xFD	0x0F	0x4C
0x9D	0xEE	0xCC	0x40
0x36	0x38	0x9B	0x46
0xEB	0x7D	0xED	0xBD

$=$

0x0F	0x1D	0xD7	0xF6
0x6B	0x18	0x34	0xA0
0xD6	0x67	0x6B	0x62
0xB4	0x50	0x61	0xDA

Példa: 6. iteráció

0x0F	0x1D	0xD7	0xF6
0x6B	0x18	0x34	0xA0
0xD6	0x67	0x6B	0x62
0xB4	0x50	0x61	0xDA

S-doboz →

0x76	0xA4	0x0E	0x42
0x7F	0xAD	0x18	0xE0
0xF6	0x85	0x7F	0xAA
0x8D	0x53	0xEF	0x57

Sor forgatás →

0x76	0xA4	0x0E	0x42
0xAD	0x18	0xE0	0x7F
0x7F	0xAA	0xF6	0x85
0x57	0x8D	0x53	0xEF

Oszlop keverés →

0x28	0x5C	0x82	0x6F
0xE1	0xFC	0x87	0xC7
0xDC	0x7F	0xEC	0x06
0xE6	0x44	0xA2	0xF9

Példa: Kulcs hozzáadása a 6. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [24,27] oszlopait:

0x28	0x5C	0x82	0x6F
0xE1	0xFC	0x87	0xC7
0xDC	0x7F	0xEC	0x06
0xE6	0x44	0xA2	0xF9

$\oplus$

0x71	0x8C	0x83	0xCF
0xC7	0x29	0xE5	0xA5
0x4C	0x74	0xEF	0xA9
0xC2	0xBF	0x52	0xEF

=

0x59	0xD0	0x01	0xA0
0x26	0xD5	0x62	0x62
0x90	0x0B	0x03	0xAF
0x24	0xFB	0xF0	0x16

Példa: 7. iteráció

0x59	0xD0	0x01	0xA0
0x26	0xD5	0x62	0x62
0x90	0x0B	0x03	0xAF
0x24	0xFB	0xF0	0x16

S-doboz →

0xCB	0x70	0x7C	0xE0
0xF7	0x03	0xAA	0xAA
0x60	0x2B	0x7B	0x79
0x36	0x0F	0x8C	0x47

Sor forgatás →

0xCB	0x70	0x7C	0xE0
0x03	0xAA	0xAA	0xF7
0x7B	0x79	0x60	0x2B
0x47	0x36	0x0F	0x8C

Oszlop keverés →

0xB4	0x4A	0x72	0x7E
0x07	0x82	0x9C	0xE4
0xF7	0x72	0x07	0xCE
0xB0	0x2F	0x50	0xE4

Példa: Kulcs hozzáadása a 7. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [28,31] oszlopait:

0xB4	0x4A	0x72	0x7E
0x07	0x82	0x9C	0xE4
0xF7	0x72	0x07	0xCE
0xB0	0x2F	0x50	0xE4

$\oplus$

0x37	0xBB	0x38	0xF7
0x14	0x3D	0xD8	0x7D
0x93	0xE7	0x08	0xA1
0x48	0xF7	0xA5	0x4A

$=$

0x83	0xF1	0x4A	0x89
0x13	0xBF	0x44	0x99
0x64	0x95	0x0F	0x6F
0xF8	0xD8	0xF5	0xAE

Példa: 8. iteráció

0x83	0xF1	0x4A	0x89
0x13	0xBF	0x44	0x99
0x64	0x95	0x0F	0x6F
0xF8	0xD8	0xF5	0xAE

S-doboz →

0xEC	0xA1	0xD6	0xA7
0x7D	0x08	0x1B	0xEE
0x43	0x2A	0x76	0xA8
0x41	0x61	0xE6	0xE4

Sor forgatás →

0xEC	0xA1	0xD6	0xA7
0x08	0x1B	0xEE	0x7D
0x76	0xA8	0x43	0x2A
0xE4	0x41	0x61	0xE6

Oszlop keverés →

0x49	0x9D	0xBC	0x1E
0x82	0x35	0xB5	0xC5
0x3F	0x32	0x1D	0xBF
0x82	0xC9	0x0E	0x72

Példa: Kulcs hozzáadása a 8. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [32,35] oszlopait:

0x49	0x9D	0xBC	0x1E
0x82	0x35	0xB5	0xC5
0x3F	0x32	0x1D	0xBF
0x82	0xC9	0x0E	0x72

$\oplus$

0x48	0xF3	0xCB	0x3C
0x26	0x1B	0xC3	0xBE
0x45	0xA2	0xAA	0x0B
0x20	0xD7	0x72	0x38

$=$

0x01	0x6E	0x77	0x22
0xA4	0x2E	0x76	0x7B
0x7A	0x90	0xB7	0xB4
0xA2	0x1E	0x7C	0x4A

Példa: 9. iteráció

0x01	0x6E	0x77	0x22
0xA4	0x2E	0x76	0x7B
0x7A	0x90	0xB7	0xB4
0xA2	0x1E	0x7C	0x4A

S-doboz →

0x7C	0x9F	0xF5	0x93
0x49	0x31	0x38	0x21
0xDA	0x60	0xA9	0x8D
0x3A	0x72	0x10	0xD6

Sor forgatás →

0x7C	0x9F	0xF5	0x93
0x31	0x38	0x21	0x49
0xA9	0x8D	0xDA	0x60
0xD6	0x3A	0x72	0x10

Oszlop keverés →

0xD4	0xDA	0x3A	0x96
0x28	0x59	0xB0	0xB1
0x65	0xE8	0xED	0x2A
0xAB	0x7B	0x1B	0xA7

Példa: Kulcs hozzáadása a 9. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [36,39] oszlopait:

0xD4	0xDA	0x3A	0x96
0x28	0x59	0xB0	0xB1
0x65	0xE8	0xED	0x2A
0xAB	0x7B	0x1B	0xA7

$\oplus$

0xFD	0x0E	0xC5	0xF9
0x0D	0x16	0xD5	0x6B
0x42	0xE0	0x4A	0x41
0xCB	0x1C	0x6E	0x56

=

0x29	0xD4	0xFF	0x6F
0x25	0x4F	0x65	0xDA
0x27	0x08	0xA7	0x6B
0x60	0x67	0x75	0xF1

Példa: 10. iteráció

0x29	0xD4	0xFF	0x6F
0x25	0x4F	0x65	0xDA
0x27	0x08	0xA7	0x6B
0x60	0x67	0x75	0xF1

S-doboz →

0xA5	0x48	0x16	0xA8
0x3F	0x84	0x4D	0x57
0xCC	0x30	0x5C	0x7F
0xD0	0x85	0x9D	0xA1

Sor forgatás →

0xA5	0x48	0x16	0xA8
0x84	0x4D	0x57	0x3F
0x5C	0x7F	0xCC	0x30
0xA1	0xD0	0x85	0x9D

Példa: Kulcs hozzáadása a 10. iteráció végén

Az állapot táblázathoz hozzáadjuk a kulcs táblázat [40,43] oszlopait:

0xA5	0x48	0x16	0xA8
0x84	0x4D	0x57	0x3F
0x5C	0x7F	0xCC	0x30
0xA1	0xD0	0x85	0x9D

$\oplus$

0xB4	0xBA	0x7F	0x86
0x8E	0x98	0x4D	0x26
0xF3	0x13	0x59	0x18
0x52	0x4E	0x20	0x76

$=$

0x11	0xF2	0x69	0x2E
0x0A	0xD5	0x1A	0x19
0xAF	0x6C	0x95	0x28
0xF3	0x9E	0xA5	0xEB

A kódoló kimenete: (`0x11 0x0A 0xAF 0xF3 0xF2 0xD5 0x6C 0x9E 0x69 0x1A 0x95 0xA5 0x2E 0x19 0x28 0xEB`)