Jika diketahui polynomial dalam GF(2^8) sbb:

$x^8 + x^5 + x^3 + x^2 + 1$

$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$

1. Selidiki, apakah polynomial di atas termasuk dalam irreducible polynomial atau bukan ! Jelaskan!
2. Jika termasuk irreducible polynomial tentukan:
   a. Matriks multiplicative inverse
   b. Konstruksi S-box dengan menggunakan 8 bit konstanta tambahan berdasarkan 2 digit terakhir NIM Anda.
3. Implementasikan S-box yang dihasilkan untuk mengenkripsi nama Anda menggunakan kunci NIM Anda.

Nama Hamid Baehaqi
NIM 4611418057

1 Kedua polinomial diatas merupakan irreducible polynomial karena sudah tidak bisa dibagi dengan polinomial lain dengan derajat dibawahnya selain 1 dan polinom itu sendiri.

2a 1 Byte multiplication dari polinom

x^8+x^5+x^3+x^2+1 * x^8+x^5+x^4+x^3+x^2+x+1 = x^16+2x^13+x^12+2x^11+3x^10+2x^9+4x^8+3x^7+3x^6+4x^5+3x^4+3x^3+2x^2+x+1
x^5-x^4+x^2-x x^5+x^2

modulo dengan x^8+x^4+x^3+x+1 = x^16+2x^13+x^12+2x^11+3x^10+2x^9+4x^8+3x^7+3x^6+4x^5+3x^4+3x^3+2x^2+x+1
x^16+x^12+x^11+x^9+x^8
= x^11+3x^10+x^9+3x^8+3x^7+3x^6+3x^4+3x^3+x+1
x^11+x^7+x^6+x^4+x^3
= 3x^10+x^9+3x^8+x+1
x^10+x^6+x^5+x^3+x^2
= x^9+3x^8-x^6-x^5-x^3-x^2+x+1
x^9+x^5+x^4+x^2+x
= 3x^8-x^6-2x^5-x^4-x^3-2x^2+1
x^8+x^4+x^3+x+1

x^5-x^4+x^2-x * x^5+x^2 = x^6-x
1000010 110110 100100
42 36 24

2a 2 Byte inversion

x^8+x^5+x^3+x^2+1 * x^8+x^5+x^4+x^3+x^2+x+1 = x^16+2x^13+x^12+2x^11+3x^10+2x^9+4x^8+3x^7+3x^6+4x^5+3x^4+3x^3+2x^2+x+1

modulo dengan x^8+x^4+x^3+x+1

x^8+x^3+x^2+x+1
x^8+x^4+x^3+x+1 | x^16+2x^13+x^12+2x^11+3x^10+2x^9+4x^8+3x^7+3x^6+4x^5+3x^4+3x^3+2x^2+x+1
x^16+x^12+x^11+x^9+x^8
x^11+3x^10+x^9+3x^8+3x^7+3x^6+4x^5+3x^4+3x^3+x+1
x^11+x^7+x^6+x^4+x^3
3x^10+x^9+3x^8+x+1
x^10+x^6+x^5+x^3+x^2
x^9+3x^8-x^6-x^5-x^3-x^2+x+1
x^9+x^5+x^4+x^2+x
3x^8-x^6-x^4-x^3+1
x^8+x^4+x^3+x+1
x^6x

x^8+x^5+x^3+x^2+1	*	x^8+x^5+x^4+x^3+x^2+x+1	= x^16+2x^13+x^12+2x^11+3x^10+2x^9+4x^8+3x^7+3x^6+4x^5+3x^4+3x^3+2x^2+x+1
x^5-x^4+x^2-x	*	x^5+x^2	= x^6x mod x^8+x^4+x^3+x+1
1000010		110110	
42		36	

3	Plaintex	hamid baehaqi	68616d69642062616568617169
	Key	4611418057	3436313134313830

Sbox

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f	
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76	
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0	
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15	
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75	
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84	
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf	
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8	
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2	
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73	
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db	
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79	
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8	
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a	
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e	
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df	
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16	

Cipherkey `b5 f8 b1 cc 45 b5 82 37 03 a9 57 3b aa c9 c4 c7`

Proses Saya menggunakan program AES Enkriptor yang saya buat, berikut prosesnya.

plaintext 00; 00; 00; 68; 61; 6d; 69; 64; 20; 62; 61; 65; 68; 61; 71; 69
key 00; 00; 00; 00; 00; 00; 00; 00; 34; 36; 31; 31; 34; 31; 38; 30
Initial key 00; 00; 00; 68; 61; 6d; 69; 64; 14; 54; 50; 54; 5c; 50; 49; 59

Round 1

after subbytes 63; 63; 63; 45; ef; 3c; f9; 43; fa; 20; 53; 20; 4a; 53; 3b; cb
after shiftrows 63; 63; 63; 45; 3c; f9; 43; ef; 53; 20; fa; 20; cb; 4a; 53; 3b
2 63
['00000010'] ['01100011']
x^7+x^6+x^2+x
3 3c
['00000011'] ['00111100']

x^7+2x^6+2x^5+2x^4+2x^3+2x^2+x
1 53
['00000001'] ['01010011']
x^7+3x^6+2x^5+3x^4+2x^3+2x^2+2x+1
1 cb
['00000001'] ['11001011']
2x^7+4x^6+2x^5+3x^4+3x^3+2x^2+3x+2
polinom setelah mod 8x ...x^4+x^3+x
2 63
['00000010'] ['01100011']
x^7+x^6+x^2+x
3 f9
['00000011'] ['11111001']
x^8+3x^7+3x^6+2x^5+2x^4+x^3+x^2+2x+1
1 20
['00000001'] ['00100000']
x^8+3x^7+3x^6+3x^5+2x^4+x^3+x^2+2x+1
1 4a
['00000001'] ['01001010']
x^8+3x^7+4x^6+3x^5+2x^4+2x^3+x^2+3x+1
polinom setelah mod 8x ...x^7+x^5-x^4-x^3+x^2
2 63
['00000010'] ['01100011']
x^7+x^6+x^2+x
3 43
['00000011'] ['01000011']
2x^7+2x^6+2x^2+3x+1
1 fa
['00000001'] ['11111010']
3x^7+3x^6+x^5+x^4+x^3+2x^2+4x+1
1 53
['00000001'] ['01010011']
3x^7+4x^6+x^5+2x^4+x^3+2x^2+5x+2
polinom setelah mod 8x ...x^7+x^5+x^3+x
2 45
['00000010'] ['01000101']
x^7+x^3+x
3 ef
['00000011'] ['11101111']
x^8+3x^7+2x^6+x^5+x^4+3x^3+2x^2+3x+1
1 20
['00000001'] ['00100000']
x^8+3x^7+2x^6+2x^5+x^4+3x^3+2x^2+3x+1
1 3b
['00000001'] ['00111011']
x^8+3x^7+2x^6+3x^5+2x^4+4x^3+2x^2+4x+2
polinom setelah mod 8x ...x^7+x^5-x^4-x^3-x-1

1 63
['00000001'] ['01100011']
x^6+x^5+x+1
2 3c
['00000010'] ['00111100']
2x^6+2x^5+x^4+x^3+x+1
3 53
['00000011'] ['01010011']
x^7+3x^6+3x^5+2x^4+x^3+x^2+3x+2
1 cb
['00000001'] ['11001011']
2x^7+4x^6+3x^5+2x^4+2x^3+x^2+4x+3
polinom setelah mod 8x ...x^5+x^2+1
1 63
['00000001'] ['01100011']
x^6+x^5+x+1
2 f9
['00000010'] ['11111001']
x^8+x^7+2x^6+2x^5+x^4+2x+1
3 20
['00000011'] ['00100000']
x^8+x^7+3x^6+3x^5+x^4+2x+1
1 4a
['00000001'] ['01001010']
x^8+x^7+4x^6+3x^5+x^4+x^3+3x+1
polinom setelah mod 8x ...x^7+x^5
1 63
['00000001'] ['01100011']
x^6+x^5+x+1
2 43
['00000010'] ['01000011']
x^7+x^6+x^5+x^2+2x+1
3 fa
['00000011'] ['11111010']
x^8+3x^7+3x^6+3x^5+2x^4+x^3+2x^2+3x+1
1 53
['00000001'] ['01010011']
x^8+3x^7+4x^6+3x^5+3x^4+x^3+2x^2+4x+2
polinom setelah mod 8x ...x^7+x^5-x-1
1 45
['00000001'] ['01000101']
x^6+x^2+1
2 ef
['00000010'] ['11101111']
x^8+x^7+2x^6+x^4+x^3+2x^2+x+1
3 20
['00000011'] ['00100000']

x^8+x^7+3x^6+x^5+x^4+x^3+2x^2+x+1
1 3b
['00000001'] ['00111011']
x^8+x^7+3x^6+2x^5+2x^4+2x^3+2x^2+2x+2
polinom setelah mod 8x ...x^7+x^6-x^4-x^3-x-1
1 63
['00000001'] ['01100011']
x^6+x^5+x+1
1 3c
['00000001'] ['00111100']
x^6+2x^5+x^4+x^3+x^2+x+1
2 53
['00000010'] ['01010011']
x^7+x^6+3x^5+x^4+x^3+2x^2+2x+1
3 cb
['00000011'] ['11001011']
x^8+3x^7+2x^6+3x^5+2x^4+2x^3+3x^2+4x+2
polinom setelah mod 8x ...x^7+x^5-x^4-x^3+x^2-x-1
1 63
['00000001'] ['01100011']
x^6+x^5+x+1
1 f9
['00000001'] ['11111001']
x^7+2x^6+2x^5+x^4+x^3+x+2
2 20
['00000010'] ['00100000']
x^7+3x^6+2x^5+x^4+x^3+x+2
3 4a
['00000011'] ['01001010']
2x^7+4x^6+2x^5+2x^4+2x^3+x^2+2x+2
polinom setelah mod 8x ...x^2
1 63
['00000001'] ['01100011']
x^6+x^5+x+1
1 43
['00000001'] ['01000011']
2x^6+x^5+2x+2
2 fa
['00000010'] ['11111010']
x^8+x^7+3x^6+2x^5+x^4+x^2+2x+2
3 53
['00000011'] ['01010011']
x^8+2x^7+4x^6+3x^5+2x^4+2x^2+4x+3
polinom setelah mod 8x ...x^5-x^4-x^3-x
1 45
['00000001'] ['01000101']
x^6+x^2+1

1 ef
['00000001'] ['11101111']
x^7+2x^6+x^5+x^3+2x^2+x+2
2 20
['00000010'] ['00100000']
x^7+3x^6+x^5+x^3+2x^2+x+2
3 3b
['00000011'] ['00111011']
x^7+4x^6+3x^5+2x^4+2x^3+3x^2+3x+3
polinom setelah mod 8x ...x^7+x^5+x^2+x+1
3 63
['00000011'] ['01100011']
x^7+2x^6+x^5+x^2+2x+1
1 3c
['00000001'] ['00111100']
x^7+2x^6+2x^5+x^4+x^3+2x^2+2x+1
1 53
['00000001'] ['01010011']
x^7+3x^6+2x^5+2x^4+x^3+2x^2+3x+2
2 cb
['00000010'] ['11001011']
x^8+2x^7+3x^6+2x^5+3x^4+x^3+3x^2+4x+2
polinom setelah mod 8x ...x^6+x^2-x-1
3 63
['00000011'] ['01100011']
x^7+2x^6+x^5+x^2+2x+1
1 f9
['00000001'] ['11111001']
2x^7+3x^6+2x^5+x^4+x^3+x^2+2x+2
1 20
['00000001'] ['00100000']
2x^7+3x^6+3x^5+x^4+x^3+x^2+2x+2
2 4a
['00000010'] ['01001010']
3x^7+3x^6+3x^5+2x^4+x^3+2x^2+2x+2
polinom setelah mod 8x ...x^7+x^6+x^5+x^3
3 63
['00000011'] ['01100011']
x^7+2x^6+x^5+x^2+2x+1
1 43
['00000001'] ['01000011']
x^7+3x^6+x^5+x^2+3x+2
1 fa
['00000001'] ['11111010']
2x^7+4x^6+2x^5+x^4+x^3+x^2+4x+2
2 53
['00000010'] ['01010011']

3x^7+4x^6+3x^5+x^4+x^3+2x^2+5x+2
polinom setelah mod 8x ...x^7+x^5+x^4+x^3+x
3 45
['00000011'] ['01000101']
x^7+x^6+x^3+x^2+x+1
1 ef
['00000001'] ['11101111']
2x^7+2x^6+x^5+2x^3+2x^2+2x+2
1 20
['00000001'] ['00100000']
2x^7+2x^6+2x^5+2x^3+2x^2+2x+2
2 3b
['00000010'] ['00111011']
2x^7+3x^6+3x^5+x^4+2x^3+3x^2+3x+2
polinom setelah mod 8x ...x^6+x^5+x^4+x^2+x
after mixcolls 1a; bc; aa; bb; 25; a0; a3; db; bf; 4; 3a; a7; 47; e8; ba; 76
roundkey 62; 62; 62; 62; c7; c7; c7; c7; 30; 06; 37; 06; 57; 66; 5e; 6e
after addroundkeys 78; de; c8; d9; e2; 67; 64; 1c; 8f; 02; 0d; a1; 10; 8e; e4; 18

Round 2

after subbytes bc; 1d; e8; 35; 98; 85; 43; 9c; 73; 77; d7; 32; ca; 19; 69; ad
after shiftrows bc; 1d; e8; 35; 85; 43; 9c; 98; d7; 32; 73; 77; ad; ca; 19; 69
2 bc
['00000010'] ['10111100']
x^8+x^6+x^5+x^4+x^3
3 85
['00000011'] ['10000101']
2x^8+x^7+x^6+x^5+x^4+2x^3+x^2+x+1
1 d7
['00000001'] ['11010111']
2x^8+2x^7+2x^6+x^5+2x^4+2x^3+2x^2+2x+2
1 ad
['00000001'] ['10101101']
2x^8+3x^7+2x^6+2x^5+2x^4+3x^3+3x^2+2x+3
polinom setelah mod 8x ...x^7+x^3+x^2+1
2 1d
['00000010'] ['00011101']
x^5+x^4+x^3+x
3 43
['00000011'] ['01000011']
x^7+x^6+x^5+x^4+x^3+x^2+3x+1
1 32
['00000001'] ['00110010']
x^7+x^6+2x^5+2x^4+x^3+x^2+4x+1

1 ca
['00000001'] ['11001010']
2x^7+2x^6+2x^5+2x^4+2x^3+x^2+5x+1
polinom setelah mod 8x ...x^2+x+1
2 e8
['00000010'] ['11101000']
x^8+x^7+x^6+x^4
3 9c
['00000011'] ['10011100']
2x^8+2x^7+x^6+x^5+3x^4+2x^3+x^2
1 73
['00000001'] ['01110011']
2x^8+2x^7+2x^6+2x^5+4x^4+2x^3+x^2+x+1
1 19
['00000001'] ['00011001']
2x^8+2x^7+2x^6+2x^5+5x^4+3x^3+x^2+x+2
polinom setelah mod 8x ...x^4+x^3+x^2+x
2 35
['00000010'] ['00110101']
x^6+x^5+x^3+x
3 98
['00000011'] ['10011000']
x^8+x^7+x^6+2x^5+2x^4+2x^3+x
1 77
['00000001'] ['01110111']
x^8+x^7+2x^6+3x^5+3x^4+2x^3+x^2+2x+1
1 69
['00000001'] ['01101001']
x^8+x^7+3x^6+4x^5+3x^4+3x^3+x^2+2x+2
polinom setelah mod 8x ...x^7+x^6+x^2-x-1
1 bc
['00000001'] ['10111100']
x^7+x^5+x^4+x^3+x^2
2 85
['00000010'] ['10000101']
x^8+x^7+x^5+x^4+2x^3+x^2+x
3 d7
['00000011'] ['11010111']
2x^8+3x^7+x^6+2x^5+2x^4+3x^3+3x^2+3x+1
1 ad
['00000001'] ['10101101']
2x^8+4x^7+x^6+3x^5+2x^4+4x^3+4x^2+3x+2
polinom setelah mod 8x ...x^6+x^5+x
1 1d
['00000001'] ['00011101']
x^4+x^3+x^2+1
2 43

['00000010'] ['01000011']
x^7+x^4+x^3+2x^2+x+1
3 32
['00000011'] ['00110010']
x^7+x^6+2x^5+2x^4+x^3+3x^2+2x+1
1 ca
['00000001'] ['11001010']
2x^7+2x^6+2x^5+2x^4+2x^3+3x^2+3x+1
polinom setelah mod 8x ...x^2+x+1
1 e8
['00000001'] ['11101000']
x^7+x^6+x^5+x^3
2 9c
['00000010'] ['10011100']
x^8+x^7+x^6+2x^5+x^4+2x^3
3 73
['00000011'] ['01110011']
x^8+2x^7+3x^6+4x^5+2x^4+2x^3+x^2+2x+1
1 19
['00000001'] ['00011001']
x^8+2x^7+3x^6+4x^5+3x^4+3x^3+x^2+2x+2
polinom setelah mod 8x ...x^6+x^2-x-1
1 35
['00000001'] ['00110101']
x^5+x^4+x^2+1
2 98
['00000010'] ['10011000']
x^8+2x^5+2x^4+x^2+1
3 77
['00000011'] ['01110111']
x^8+x^7+2x^6+4x^5+3x^4+x^3+3x^2+2x+2
1 69
['00000001'] ['01101001']
x^8+x^7+3x^6+5x^5+3x^4+2x^3+3x^2+2x+3
polinom setelah mod 8x ...x^7+x^6+x^5-x^3+x^2-x
1 bc
['00000001'] ['10111100']
x^7+x^5+x^4+x^3+x^2
1 85
['00000001'] ['10000101']
2x^7+x^5+x^4+x^3+2x^2+1
2 d7
['00000010'] ['11010111']
x^8+3x^7+2x^5+x^4+2x^3+3x^2+x+1
3 ad
['00000011'] ['10101101']
2x^8+4x^7+x^6+3x^5+2x^4+4x^3+4x^2+2x+2

polinom setelah mod 8x ...x^6+x^5
1 1d
['00000001'] ['00011101']
x^4+x^3+x^2+1
1 43
['00000001'] ['01000011']
x^6+x^4+x^3+x^2+x+2
2 32
['00000010'] ['00110010']
2x^6+x^5+x^4+x^3+2x^2+x+2
3 ca
['00000011'] ['11001010']
x^8+2x^7+3x^6+x^5+2x^4+2x^3+3x^2+2x+2
polinom setelah mod 8x ...x^6+x^5-x^4-x^3+x^2-x-1
1 e8
['00000001'] ['11101000']
x^7+x^6+x^5+x^3
1 9c
['00000001'] ['10011100']
2x^7+x^6+x^5+x^4+2x^3+x^2
2 73
['00000010'] ['01110011']
3x^7+2x^6+2x^5+x^4+2x^3+2x^2+x
3 19
['00000011'] ['00011001']
3x^7+2x^6+3x^5+3x^4+3x^3+2x^2+2x+1
polinom setelah mod 8x ...x^7+x^5+x^4+x^3+1
1 35
['00000001'] ['00110101']
x^5+x^4+x^2+1
1 98
['00000001'] ['10011000']
x^7+x^5+2x^4+x^3+x^2+1
2 77
['00000010'] ['01110111']
2x^7+x^6+2x^5+2x^4+2x^3+2x^2+x+1
3 69
['00000011'] ['01101001']
3x^7+3x^6+3x^5+3x^4+3x^3+2x^2+2x+2
polinom setelah mod 8x ...x^7+x^6+x^5+x^4+x^3
3 bc
['00000011'] ['10111100']
x^8+x^7+x^6+2x^5+2x^4+2x^3+x^2
1 85
['00000001'] ['10000101']
x^8+2x^7+x^6+2x^5+2x^4+2x^3+2x^2+1
1 d7

['00000001'] ['11010111']
x^8+3x^7+2x^6+2x^5+3x^4+2x^3+3x^2+x+2
2 ad
['00000010'] ['10101101']
2x^8+3x^7+3x^6+2x^5+4x^4+3x^3+3x^2+2x+2
polinom setelah mod 8x ...x^7+x^6+x^3+x^2
3 1d
['00000011'] ['00011101']
x^5+2x^4+2x^3+x^2+x+1
1 43
['00000001'] ['01000011']
x^6+x^5+2x^4+2x^3+x^2+2x+2
1 32
['00000001'] ['00110010']
x^6+2x^5+3x^4+2x^3+x^2+3x+2
2 ca
['00000010'] ['11001010']
x^8+x^7+x^6+2x^5+4x^4+2x^3+2x^2+3x+2
polinom setelah mod 8x ...x^7+x^6-x^4-x^3-1
3 e8
['00000011'] ['11101000']
x^8+2x^7+2x^6+x^5+x^4+x^3
1 9c
['00000001'] ['10011100']
x^8+3x^7+2x^6+x^5+2x^4+2x^3+x^2
1 73
['00000001'] ['01110011']
x^8+3x^7+3x^6+2x^5+3x^4+2x^3+x^2+x+1
2 19
['00000010'] ['00011001']
x^8+3x^7+3x^6+3x^5+4x^4+2x^3+x^2+2x+1
polinom setelah mod 8x ...x^7+x^6+x^5-x^4-x^3+x^2-x
3 35
['00000011'] ['00110101']
x^6+2x^5+x^4+x^3+x^2+x+1
1 98
['00000001'] ['10011000']
x^7+x^6+2x^5+2x^4+2x^3+x^2+x+1
1 77
['00000001'] ['01110111']
x^7+2x^6+3x^5+3x^4+2x^3+2x^2+2x+2
2 69
['00000010'] ['01101001']
2x^7+3x^6+3x^5+4x^4+2x^3+2x^2+3x+2
polinom setelah mod 8x ...x^6+x^5+x
after mixcolls 8d; 7; 1e; c7; 62; 7; 47; ee; 60; 7f; b9; f8; cc; d9; fe; 62
roundkey a6; c4; a6; c4; a8; 6f; a8; 6f; af; a9; 9e; 98; fd; 9b; c5; ab

after addroundkeys 2b; c3; b8; 03; ca; 68; ef; 81; cf; d6; 27; 60; 31; 42; 3b; c9

Round 3

after subbytes f1; 2e; 6c; 7b; 74; 45; df; 0c; 8a; f6; cc; d0; c7; 2c; e2; dd
after shiftrows f1; 2e; 6c; 7b; 45; df; 0c; 74; cc; d0; 8a; f6; dd; c7; 2c; e2
2 f1
['00000010'] ['11110001']
x^8+x^7+x^6+x^5+x
3 45
['00000011'] ['01000101']
x^8+2x^7+2x^6+x^5+x^3+x^2+2x+1
1 cc
['00000001'] ['11001100']
x^8+3x^7+3x^6+x^5+2x^3+2x^2+2x+1
1 dd
['00000001'] ['11011101']
x^8+4x^7+4x^6+x^5+x^4+3x^3+3x^2+2x+2
polinom setelah mod 8x ...x^5+x^2-x-1
2 2e
['00000010'] ['00101110']
x^6+x^4+x^3+x^2
3 df
['00000011'] ['11011111']
x^8+2x^7+2x^6+x^5+3x^4+3x^3+3x^2+2x+1
1 d0
['00000001'] ['11010000']
x^8+3x^7+3x^6+x^5+4x^4+3x^3+3x^2+2x+1
1 c7
['00000001'] ['11000111']
x^8+4x^7+4x^6+x^5+4x^4+3x^3+4x^2+3x+2
polinom setelah mod 8x ...x^5-x^4-1
2 6c
['00000010'] ['01101100']
x^7+x^6+x^4+x^3
3 0c
['00000011'] ['00001100']
x^7+x^6+2x^4+3x^3+x^2
1 8a
['00000001'] ['10001010']
2x^7+x^6+2x^4+4x^3+x^2+x
1 2c
['00000001'] ['00101100']
2x^7+x^6+x^5+2x^4+5x^3+2x^2+x
polinom setelah mod 8x ...x^6+x^5+x^3+x

2 7b
['00000010'] ['01111011']
x^7+x^6+x^5+x^4+x^2+x
3 74
['00000011'] ['01110100']
2x^7+3x^6+3x^5+2x^4+x^3+2x^2+x
1 f6
['00000001'] ['11110110']
3x^7+4x^6+4x^5+3x^4+x^3+3x^2+2x
1 e2
['00000001'] ['11100010']
4x^7+5x^6+5x^5+3x^4+x^3+3x^2+3x
polinom setelah mod 8x ...x^6+x^5+x^4+x^3+x^2+x
1 f1
['00000001'] ['11110001']
x^7+x^6+x^5+x^4+1
2 45
['00000010'] ['01000101']
2x^7+x^6+x^5+x^4+x^3+x+1
3 cc
['00000011'] ['11001100']
x^8+4x^7+2x^6+x^5+2x^4+3x^3+x^2+x+1
1 dd
['00000001'] ['11011101']
x^8+5x^7+3x^6+x^5+3x^4+4x^3+2x^2+x+2
polinom setelah mod 8x ...x^7+x^6+x^5-x^3-1
1 2e
['00000001'] ['00101110']
x^5+x^3+x^2+x
2 df
['00000010'] ['11011111']
x^8+x^7+2x^5+x^4+2x^3+2x^2+2x
3 d0
['00000011'] ['11010000']
2x^8+3x^7+x^6+3x^5+2x^4+2x^3+2x^2+2x
1 c7
['00000001'] ['11000111']
2x^8+4x^7+2x^6+3x^5+2x^4+2x^3+3x^2+3x+1
polinom setelah mod 8x ...x^5+x^2+x+1
1 6c
['00000001'] ['01101100']
x^6+x^5+x^3+x^2
2 0c
['00000010'] ['00001100']
x^6+x^5+x^4+2x^3+x^2
3 8a
['00000011'] ['10001010']

x^8+x^7+x^6+x^5+2x^4+3x^3+2x^2+x
1 2c
['00000001'] ['00101100']
x^8+x^7+x^6+2x^5+2x^4+4x^3+3x^2+x
polinom setelah mod 8x ...x^7+x^6-x^4-x^3+x^2-1
1 7b
['00000001'] ['01111011']
x^6+x^5+x^4+x^3+x+1
2 74
['00000010'] ['01110100']
x^7+2x^6+2x^5+x^4+2x^3+x+1
3 f6
['00000011'] ['11110110']
x^8+3x^7+4x^6+4x^5+2x^4+3x^3+2x^2+2x+1
1 e2
['00000001'] ['11100010']
x^8+4x^7+5x^6+5x^5+2x^4+3x^3+2x^2+3x+1
polinom setelah mod 8x ...x^6+x^5-x^4
1 f1
['00000001'] ['11110001']
x^7+x^6+x^5+x^4+1
1 45
['00000001'] ['01000101']
x^7+2x^6+x^5+x^4+x^2+2
2 cc
['00000010'] ['11001100']
x^8+2x^7+2x^6+x^5+2x^4+x^3+x^2+2
3 dd
['00000011'] ['11011101']
2x^8+4x^7+3x^6+2x^5+4x^4+3x^3+2x^2+x+3
polinom setelah mod 8x ...x^6+x^3+x+1
1 2e
['00000001'] ['00101110']
x^5+x^3+x^2+x
1 df
['00000001'] ['11011111']
x^7+x^6+x^5+x^4+2x^3+2x^2+2x+1
2 d0
['00000010'] ['11010000']
x^8+2x^7+x^6+2x^5+x^4+2x^3+2x^2+2x+1
3 c7
['00000011'] ['11000111']
2x^8+4x^7+2x^6+2x^5+x^4+3x^3+4x^2+4x+2
polinom setelah mod 8x ...x^4+x^3
1 6c
['00000001'] ['01101100']
x^6+x^5+x^3+x^2

1 0c
['00000001'] ['00001100']
x^6+x^5+2x^3+2x^2
2 8a
['00000010'] ['10001010']
x^8+x^6+x^5+x^4+2x^3+3x^2
3 2c
['00000011'] ['00101100']
x^8+2x^6+2x^5+2x^4+4x^3+4x^2
polinom setelah mod 8x ...-x^4-x^3-x-1
1 7b
['00000001'] ['01111011']
x^6+x^5+x^4+x^3+x+1
1 74
['00000001'] ['01110100']
2x^6+2x^5+2x^4+x^3+x^2+x+1
2 f6
['00000010'] ['11110110']
x^8+x^7+3x^6+3x^5+2x^4+2x^3+2x^2+x+1
3 e2
['00000011'] ['11100010']
2x^8+3x^7+5x^6+4x^5+2x^4+2x^3+3x^2+2x+1
polinom setelah mod 8x ...x^7+x^6+x^2+1
3 f1
['00000011'] ['11110001']
x^8+2x^7+2x^6+2x^5+x^4+x+1
1 45
['00000001'] ['01000101']
x^8+2x^7+3x^6+2x^5+x^4+x^2+x+2
1 cc
['00000001'] ['11001100']
x^8+3x^7+4x^6+2x^5+x^4+x^3+2x^2+x+2
2 dd
['00000010'] ['11011101']
2x^8+4x^7+4x^6+3x^5+2x^4+2x^3+2x^2+2x+2
polinom setelah mod 8x ...x^5
3 2e
['00000011'] ['00101110']
x^6+x^5+x^4+2x^3+2x^2+x
1 df
['00000001'] ['11011111']
x^7+2x^6+x^5+2x^4+3x^3+3x^2+2x+1
1 d0
['00000001'] ['11010000']
2x^7+3x^6+x^5+3x^4+3x^3+3x^2+2x+1
2 c7
['00000010'] ['11000111']

x^8+3x^7+3x^6+x^5+3x^4+4x^3+4x^2+3x+1
polinom setelah mod 8x ...x^7+x^6+x^5-x^3
3 6c
['00000011'] ['01101100']
x^7+2x^6+x^5+x^4+2x^3+x^2
1 0c
['00000001'] ['00001100']
x^7+2x^6+x^5+x^4+3x^3+2x^2
1 8a
['00000001'] ['10001010']
2x^7+2x^6+x^5+x^4+4x^3+2x^2+x
2 2c
['00000010'] ['00101100']
2x^7+3x^6+x^5+2x^4+5x^3+2x^2+x
polinom setelah mod 8x ...x^6+x^5+x^3+x
3 7b
['00000011'] ['01111011']
x^7+2x^6+2x^5+2x^4+x^3+x^2+2x+1
1 74
['00000001'] ['01110100']
x^7+3x^6+3x^5+3x^4+x^3+2x^2+2x+1
1 f6
['00000001'] ['11110110']
2x^7+4x^6+4x^5+4x^4+x^3+3x^2+3x+1
2 e2
['00000010'] ['11100010']
x^8+3x^7+5x^6+4x^5+4x^4+x^3+4x^2+3x+1
polinom setelah mod 8x ...x^7+x^6-x^4
after mixcolls 27; 31; 6a; 7e; e9; 27; dd; 70; 4b; 18; 1b; c5; 20; e8; 6a; d0
roundkey 0a; ce; 68; ac; ee; 81; 29; 46; cd; 64; fa; 62; e1; 7a; bf; 14
after addroundkeys 2d; ff; 02; d2; 07; a6; f4; 36; 86; 7c; e1; a7; c1; 92; d5; c4

Round 4

after subbytes d8; 16; 77; b5; c5; 24; bf; 05; 44; 10; f8; 5c; 78; 4f; 03; 1c
after shiftrows d8; 16; 77; b5; 24; bf; 05; c5; f8; 5c; 44; 10; 1c; 78; 4f; 03
2 d8
['00000010'] ['11011000']
x^8+x^7+x^5+x^4
3 24
['00000011'] ['00100100']
x^8+x^7+x^6+2x^5+x^4+x^3+x^2
1 f8
['00000001'] ['11111000']
x^8+2x^7+2x^6+3x^5+2x^4+2x^3+x^2

1 1c
['00000001'] ['00011100']
x^8+2x^7+2x^6+3x^5+3x^4+3x^3+2x^2
polinom setelah mod 8x ...x^5-x-1
2 16
['00000010'] ['00010110']
x^5+x^3+x^2
3 bf
['00000011'] ['10111111']
x^8+x^7+x^6+3x^5+2x^4+3x^3+3x^2+2x+1
1 5c
['00000001'] ['01011100']
x^8+x^7+2x^6+3x^5+3x^4+4x^3+4x^2+2x+1
1 78
['00000001'] ['01111000']
x^8+x^7+3x^6+4x^5+4x^4+5x^3+4x^2+2x+1
polinom setelah mod 8x ...x^7+x^6-x^4-x
2 77
['00000010'] ['01110111']
x^7+x^6+x^5+x^3+x^2+x
3 05
['00000011'] ['00000101']
x^7+x^6+x^5+2x^3+2x^2+2x+1
1 44
['00000001'] ['01000100']
x^7+2x^6+x^5+2x^3+3x^2+2x+1
1 4f
['00000001'] ['01001111']
x^7+3x^6+x^5+3x^3+4x^2+3x+2
polinom setelah mod 8x ...x^7+x^6+x^5+x^3+x
2 b5
['00000010'] ['10110101']
x^8+x^6+x^5+x^3+x
3 c5
['00000011'] ['11000101']
2x^8+2x^7+2x^6+x^5+2x^3+x^2+2x+1
1 10
['00000001'] ['00010000']
2x^8+2x^7+2x^6+x^5+x^4+2x^3+x^2+2x+1
1 03
['00000001'] ['00000011']
2x^8+2x^7+2x^6+x^5+x^4+2x^3+x^2+3x+2
polinom setelah mod 8x ...x^5+x^4+x^2+x
1 d8
['00000001'] ['11011000']
x^7+x^6+x^4+x^3
2 24

['00000010'] ['00100100']
x^7+2x^6+x^4+2x^3
3 f8
['00000011'] ['11111000']
x^8+3x^7+4x^6+2x^5+3x^4+3x^3
1 1c
['00000001'] ['00011100']
x^8+3x^7+4x^6+2x^5+4x^4+4x^3+x^2
polinom setelah mod 8x ...x^7-x^4-x^3+x^2-x-1
1 16
['00000001'] ['00010110']
x^4+x^2+x
2 bf
['00000010'] ['10111111']
x^8+x^6+x^5+2x^4+x^3+2x^2+2x
3 5c
['00000011'] ['01011100']
x^8+x^7+2x^6+2x^5+4x^4+3x^3+3x^2+2x
1 78
['00000001'] ['01111000']
x^8+x^7+3x^6+3x^5+5x^4+4x^3+3x^2+2x
polinom setelah mod 8x ...x^7+x^6+x^5-x^3+x^2-x-1
1 77
['00000001'] ['01110111']
x^6+x^5+x^4+x^2+x+1
2 05
['00000010'] ['00000101']
x^6+x^5+x^4+x^3+x^2+2x+1
3 44
['00000011'] ['01000100']
x^7+2x^6+x^5+x^4+2x^3+2x^2+2x+1
1 4f
['00000001'] ['01001111']
x^7+3x^6+x^5+x^4+3x^3+3x^2+3x+2
polinom setelah mod 8x ...x^7+x^6+x^5+x^4+x^3+x^2+x
1 b5
['00000001'] ['10110101']
x^7+x^5+x^4+x^2+1
2 c5
['00000010'] ['11000101']
x^8+2x^7+x^5+x^4+x^3+x^2+x+1
3 10
['00000011'] ['00010000']
x^8+2x^7+2x^5+2x^4+x^3+x^2+x+1
1 03
['00000001'] ['00000011']
x^8+2x^7+2x^5+2x^4+x^3+x^2+2x+2

polinom setelah mod 8x ...-x^4+x^2-x-1
1 d8
['00000001'] ['11011000']
x^7+x^6+x^4+x^3
1 24
['00000001'] ['00100100']
x^7+x^6+x^5+x^4+x^3+x^2
2 f8
['00000010'] ['11111000']
x^8+2x^7+2x^6+2x^5+2x^4+x^3+x^2
3 1c
['00000011'] ['00011100']
x^8+2x^7+2x^6+3x^5+4x^4+3x^3+2x^2
polinom setelah mod 8x ...x^5-x^4-x-1
1 16
['00000001'] ['00010110']
x^4+x^2+x
1 bf
['00000001'] ['10111111']
x^7+x^5+2x^4+x^3+2x^2+2x+1
2 5c
['00000010'] ['01011100']
2x^7+2x^5+3x^4+2x^3+2x^2+2x+1
3 78
['00000011'] ['01111000']
3x^7+2x^6+4x^5+5x^4+3x^3+2x^2+2x+1
polinom setelah mod 8x ...x^7+x^4+x^3+1
1 77
['00000001'] ['01110111']
x^6+x^5+x^4+x^2+x+1
1 05
['00000001'] ['00000101']
x^6+x^5+x^4+2x^2+x+2
2 44
['00000010'] ['01000100']
x^7+x^6+x^5+x^4+x^3+2x^2+x+2
3 4f
['00000011'] ['01001111']
2x^7+2x^6+x^5+2x^4+3x^3+4x^2+3x+3
polinom setelah mod 8x ...x^5+x^3+x+1
1 b5
['00000001'] ['10110101']
x^7+x^5+x^4+x^2+1
1 c5
['00000001'] ['11000101']
2x^7+x^6+x^5+x^4+2x^2+2
2 10

['00000010'] ['00010000']
2x^7+x^6+2x^5+x^4+2x^2+2
3 03
['00000011'] ['00000011']
2x^7+x^6+2x^5+x^4+3x^2+2x+3
polinom setelah mod 8x ...x^6+x^4+x^2+1
3 d8
['00000011'] ['11011000']
x^8+2x^7+x^6+x^5+2x^4+x^3
1 24
['00000001'] ['00100100']
x^8+2x^7+x^6+2x^5+2x^4+x^3+x^2
1 f8
['00000001'] ['11111000']
x^8+3x^7+2x^6+3x^5+3x^4+2x^3+x^2
2 1c
['00000010'] ['00011100']
x^8+3x^7+2x^6+4x^5+4x^4+3x^3+x^2
polinom setelah mod 8x ...x^7-x^4+x^2-x-1
3 16
['00000011'] ['00010110']
x^5+x^4+x^3+2x^2+x
1 bf
['00000001'] ['10111111']
x^7+2x^5+2x^4+2x^3+3x^2+2x+1
1 5c
['00000001'] ['01011100']
x^7+x^6+2x^5+3x^4+3x^3+4x^2+2x+1
2 78
['00000010'] ['01111000']
2x^7+2x^6+3x^5+4x^4+3x^3+4x^2+2x+1
polinom setelah mod 8x ...x^5+x^3+1
3 77
['00000011'] ['01110111']
x^7+2x^6+2x^5+x^4+x^3+2x^2+2x+1
1 05
['00000001'] ['00000101']
x^7+2x^6+2x^5+x^4+x^3+3x^2+2x+2
1 44
['00000001'] ['01000100']
x^7+3x^6+2x^5+x^4+x^3+4x^2+2x+2
2 4f
['00000010'] ['01001111']
2x^7+3x^6+2x^5+2x^4+2x^3+5x^2+3x+2
polinom setelah mod 8x ...x^6+x^2+x
3 b5
['00000011'] ['10110101']

x^8+x^7+x^6+2x^5+x^4+x^3+x^2+x+1
1 c5
['00000001'] ['11000101']
x^8+2x^7+2x^6+2x^5+x^4+x^3+2x^2+x+2
1 10
['00000001'] ['00010000']
x^8+2x^7+2x^6+2x^5+2x^4+x^3+2x^2+x+2
2 03
['00000010'] ['00000011']
x^8+2x^7+2x^6+2x^5+2x^4+x^3+3x^2+2x+2
polinom setelah mod 8x ...-x^4+x^2-x-1
after mixcolls 23; d2; ea; 36; 9f; ef; fe; 17; 33; 99; 2b; 55; 97; 29; 46; 17
roundkey 58; 96; fe; 52; 44; c5; ec; aa; 37; 53; a9; cb; 70; 0a; b5; a1
after addroundkeys 7b; 44; 14; 64; db; 2a; 12; bd; 04; ca; 82; 9e; e7; 23; f3; b6

Round 5

after subbytes 21; 1b; fa; 43; b9; e5; c9; 7a; f2; 74; 13; 0b; 94; 26; 0d; 4e
after shiftrows 21; 1b; fa; 43; e5; c9; 7a; b9; 13; 0b; f2; 74; 4e; 94; 26; 0d
2 21
['00000010'] ['00100001']
x^6+x
3 e5
['00000011'] ['11100101']
x^8+2x^7+3x^6+x^5+x^3+x^2+2x+1
1 13
['00000001'] ['00010011']
x^8+2x^7+3x^6+x^5+x^4+x^3+x^2+3x+2
1 4e
['00000001'] ['01001110']
x^8+2x^7+4x^6+x^5+x^4+2x^3+2x^2+4x+2
polinom setelah mod 8x ...x^5-x^3-x-1
2 1b
['00000010'] ['00011011']
x^5+x^4+x^2+x
3 c9
['00000011'] ['11001001']
x^8+2x^7+x^6+x^5+2x^4+x^3+x^2+2x+1
1 0b
['00000001'] ['00001011']
x^8+2x^7+x^6+x^5+2x^4+2x^3+x^2+3x+2
1 94
['00000001'] ['10010100']
x^8+3x^7+x^6+x^5+3x^4+2x^3+2x^2+3x+2
polinom setelah mod 8x ...x^7+x^6+x^5-x^3-1

2 fa
['00000010'] ['11111010']
x^8+x^7+x^6+x^5+x^4+x^2
3 7a
['00000011'] ['01111010']
x^8+2x^7+3x^6+3x^5+3x^4+x^3+2x^2+x
1 f2
['00000001'] ['11110010']
x^8+3x^7+4x^6+4x^5+4x^4+x^3+2x^2+2x
1 26
['00000001'] ['00100110']
x^8+3x^7+4x^6+5x^5+4x^4+x^3+3x^2+3x
polinom setelah mod 8x ...x^7+x^5-x^4+x^2-1
2 43
['00000010'] ['01000011']
x^7+x^2+x
3 b9
['00000011'] ['10111001']
x^8+2x^7+x^6+2x^5+2x^4+x^3+x^2+2x+1
1 74
['00000001'] ['01110100']
x^8+2x^7+2x^6+3x^5+3x^4+x^3+2x^2+2x+1
1 0d
['00000001'] ['00001101']
x^8+2x^7+2x^6+3x^5+3x^4+2x^3+3x^2+2x+2
polinom setelah mod 8x ...x^5-x^3+x^2-x-1
1 21
['00000001'] ['00100001']
x^5+1
2 e5
['00000010'] ['11100101']
x^8+x^7+x^6+x^5+x^3+x+1
3 13
['00000011'] ['00010011']
x^8+x^7+x^6+2x^5+x^4+x^3+x^2+3x+2
1 4e
['00000001'] ['01001110']
x^8+x^7+2x^6+2x^5+x^4+2x^3+2x^2+4x+2
polinom setelah mod 8x ...x^7-x^3-x-1
1 1b
['00000001'] ['00011011']
x^4+x^3+x+1
2 c9
['00000010'] ['11001001']
x^8+x^7+2x^4+x^3+2x+1
3 0b
['00000011'] ['00001011']

x^8+x^7+3x^4+2x^3+x^2+4x+2
1 94
['00000001'] ['10010100']
x^8+2x^7+4x^4+2x^3+2x^2+4x+2
polinom setelah mod 8x ...-x^4-x^3-x-1
1 fa
['00000001'] ['11111010']
x^7+x^6+x^5+x^4+x^3+x
2 7a
['00000010'] ['01111010']
2x^7+2x^6+2x^5+2x^4+x^3+x^2+x
3 f2
['00000011'] ['11110010']
x^8+4x^7+4x^6+4x^5+3x^4+x^3+2x^2+2x
1 26
['00000001'] ['00100110']
x^8+4x^7+4x^6+5x^5+3x^4+x^3+3x^2+3x
polinom setelah mod 8x ...x^5+x^2-1
1 43
['00000001'] ['01000011']
x^6+x+1
2 b9
['00000010'] ['10111001']
x^8+2x^6+x^5+x^4+2x+1
3 74
['00000011'] ['01110100']
x^8+x^7+4x^6+3x^5+2x^4+x^3+x^2+2x+1
1 0d
['00000001'] ['00001101']
x^8+x^7+4x^6+3x^5+2x^4+2x^3+2x^2+2x+2
polinom setelah mod 8x ...x^7+x^5-x^4-x^3-x-1
1 21
['00000001'] ['00100001']
x^5+1
1 e5
['00000001'] ['11100101']
x^7+x^6+2x^5+x^2+2
2 13
['00000010'] ['00010011']
x^7+x^6+3x^5+2x^2+x+2
3 4e
['00000011'] ['01001110']
2x^7+2x^6+3x^5+x^4+2x^3+4x^2+2x+2
polinom setelah mod 8x ...x^5+x^4
1 1b
['00000001'] ['00011011']
x^4+x^3+x+1

1 c9
['00000001'] ['11001001']
x^7+x^6+x^4+2x^3+x+2
2 0b
['00000010'] ['00001011']
x^7+x^6+2x^4+2x^3+x^2+2x+2
3 94
['00000011'] ['10010100']
x^8+2x^7+x^6+x^5+3x^4+3x^3+2x^2+2x+2
polinom setelah mod 8x ...x^6+x^5-x-1
1 fa
['00000001'] ['11111010']
x^7+x^6+x^5+x^4+x^3+x
1 7a
['00000001'] ['01111010']
x^7+2x^6+2x^5+2x^4+2x^3+2x
2 f2
['00000010'] ['11110010']
x^8+2x^7+3x^6+3x^5+2x^4+2x^3+x^2+2x
3 26
['00000011'] ['00100110']
x^8+2x^7+4x^6+4x^5+2x^4+3x^3+3x^2+3x
polinom setelah mod 8x ...-x^4+x^2-1
1 43
['00000001'] ['01000011']
x^6+x+1
1 b9
['00000001'] ['10111001']
x^7+x^6+x^5+x^4+x^3+x+2
2 74
['00000010'] ['01110100']
2x^7+2x^6+2x^5+x^4+2x^3+x+2
3 0d
['00000011'] ['00001101']
2x^7+2x^6+2x^5+2x^4+4x^3+x^2+2x+3
polinom setelah mod 8x ...x^2+1
3 21
['00000011'] ['00100001']
x^6+x^5+x+1
1 e5
['00000001'] ['11100101']
x^7+2x^6+2x^5+x^2+x+2
1 13
['00000001'] ['00010011']
x^7+2x^6+2x^5+x^4+x^2+2x+3
2 4e
['00000010'] ['01001110']

2x^7+2x^6+2x^5+2x^4+x^3+2x^2+2x+3
polinom setelah mod 8x ...x^3+1
3 1b
['00000011'] ['00011011']
x^5+2x^4+x^3+x^2+2x+1
1 c9
['00000001'] ['11001001']
x^7+x^6+x^5+2x^4+2x^3+x^2+2x+2
1 0b
['00000001'] ['00001011']
x^7+x^6+x^5+2x^4+3x^3+x^2+3x+3
2 94
['00000010'] ['10010100']
x^8+x^7+x^6+2x^5+2x^4+4x^3+x^2+3x+3
polinom setelah mod 8x ...x^7+x^6-x^4-x^3+x^2
3 fa
['00000011'] ['11111010']
x^8+2x^7+2x^6+2x^5+2x^4+x^3+x^2+x
1 7a
['00000001'] ['01111010']
x^8+2x^7+3x^6+3x^5+3x^4+2x^3+x^2+2x
1 f2
['00000001'] ['11110010']
x^8+3x^7+4x^6+4x^5+4x^4+2x^3+x^2+3x
2 26
['00000010'] ['00100110']
x^8+3x^7+5x^6+4x^5+4x^4+3x^3+2x^2+3x
polinom setelah mod 8x ...x^7+x^6-x^4-1
3 43
['00000011'] ['01000011']
x^7+x^6+x^2+2x+1
1 b9
['00000001'] ['10111001']
2x^7+x^6+x^5+x^4+x^3+x^2+2x+2
1 74
['00000001'] ['01110100']
2x^7+2x^6+2x^5+2x^4+x^3+2x^2+2x+2
2 0d
['00000010'] ['00001101']
2x^7+2x^6+2x^5+3x^4+2x^3+2x^2+3x+2
polinom setelah mod 8x ...x^4+x
after mixcolls 2b; e9; b5; 2f; 8b; 1b; 25; bb; 30; 63; 15; 5; 9; dc; d1; 12
roundkey e4; 72; 8c; de; 5b; 9e; 72; d8; 05; 56; ff; 34; 70; 7a; cf; 6e
after addroundkeys cf; 9b; 39; f1; d0; 85; 57; 63; 35; 35; ea; 31; 79; a6; 1e; 7c

---

Round 6

after subbytes 8a; 14; 12; a1; 70; 97; 5b; fb; 96; 96; 87; c7; b6; 24; 72; 10
after shiftrows 8a; 14; 12; a1; 97; 5b; fb; 70; 87; c7; 96; 96; 10; b6; 24; 72
2 8a
['00000010'] ['10001010']
x^8+x^4+x^2
3 97
['00000011'] ['10010111']
2x^8+x^7+x^5+2x^4+x^3+3x^2+2x+1
1 87
['00000001'] ['10000111']
2x^8+2x^7+x^5+2x^4+x^3+4x^2+3x+2
1 10
['00000001'] ['00010000']
2x^8+2x^7+x^5+3x^4+x^3+4x^2+3x+2
polinom setelah mod 8x ...x^5+x^4+x^3+x
2 14
['00000010'] ['00010100']
x^5+x^3
3 5b
['00000011'] ['01011011']
x^7+x^6+2x^5+2x^4+2x^3+x^2+2x+1
1 c7
['00000001'] ['11000111']
2x^7+2x^6+2x^5+2x^4+2x^3+2x^2+3x+2
1 b6
['00000001'] ['10110110']
3x^7+2x^6+3x^5+3x^4+2x^3+3x^2+4x+2
polinom setelah mod 8x ...x^7+x^5+x^4+x^2
2 12
['00000010'] ['00010010']
x^5+x^2
3 fb
['00000011'] ['11111011']
x^8+2x^7+2x^6+3x^5+2x^4+x^3+2x^2+2x+1
1 96
['00000001'] ['10010110']
x^8+3x^7+2x^6+3x^5+3x^4+x^3+3x^2+3x+1
1 24
['00000001'] ['00100100']
x^8+3x^7+2x^6+4x^5+3x^4+x^3+4x^2+3x+1
polinom setelah mod 8x ...x^7
2 a1
['00000010'] ['10100001']
x^8+x^6+x
3 70

['00000011'] ['01110000']
x^8+x^7+3x^6+2x^5+x^4+x
1 96
['00000001'] ['10010110']
x^8+2x^7+3x^6+2x^5+2x^4+x^2+2x
1 72
['00000001'] ['01110010']
x^8+2x^7+4x^6+3x^5+3x^4+x^2+3x
polinom setelah mod 8x ...x^5-x^3+x^2-1
1 8a
['00000001'] ['10001010']
x^7+x^3+x
2 97
['00000010'] ['10010111']
x^8+x^7+x^5+2x^3+x^2+2x
3 87
['00000011'] ['10000111']
2x^8+2x^7+x^5+3x^3+3x^2+4x+1
1 10
['00000001'] ['00010000']
2x^8+2x^7+x^5+x^4+3x^3+3x^2+4x+1
polinom setelah mod 8x ...x^5+x^4+x^3+x^2+1
1 14
['00000001'] ['00010100']
x^4+x^2
2 5b
['00000010'] ['01011011']
x^7+x^5+2x^4+2x^2+x
3 c7
['00000011'] ['11000111']
x^8+3x^7+x^6+x^5+2x^4+x^3+4x^2+3x+1
1 b6
['00000001'] ['10110110']
x^8+4x^7+x^6+2x^5+3x^4+x^3+5x^2+4x+1
polinom setelah mod 8x ...x^6+x^2-x
1 12
['00000001'] ['00010010']
x^4+x
2 fb
['00000010'] ['11111011']
x^8+x^7+x^6+x^5+2x^4+x^2+2x
3 96
['00000011'] ['10010110']
2x^8+2x^7+x^6+2x^5+3x^4+x^3+3x^2+3x
1 24
['00000001'] ['00100100']
2x^8+2x^7+x^6+3x^5+3x^4+x^3+4x^2+3x

polinom setelah mod 8x ...x^6+x^5+x^4+x^3+x
1 a1
['00000001'] ['10100001']
x^7+x^5+1
2 70
['00000010'] ['01110000']
2x^7+x^6+2x^5+1
3 96
['00000011'] ['10010110']
x^8+3x^7+x^6+3x^5+x^4+x^3+2x^2+x+1
1 72
['00000001'] ['01110010']
x^8+3x^7+2x^6+4x^5+2x^4+x^3+2x^2+2x+1
polinom setelah mod 8x ...x^7-x^4-x
1 8a
['00000001'] ['10001010']
x^7+x^3+x
1 97
['00000001'] ['10010111']
2x^7+x^4+x^3+x^2+2x+1
2 87
['00000010'] ['10000111']
x^8+2x^7+x^4+2x^3+2x^2+3x+1
3 10
['00000011'] ['00010000']
x^8+2x^7+x^5+2x^4+2x^3+2x^2+3x+1
polinom setelah mod 8x ...x^5-x^4-x^3
1 14
['00000001'] ['00010100']
x^4+x^2
1 5b
['00000001'] ['01011011']
x^6+2x^4+x^3+x^2+x+1
2 c7
['00000010'] ['11000111']
x^8+x^7+x^6+2x^4+2x^3+2x^2+2x+1
3 b6
['00000011'] ['10110110']
2x^8+2x^7+2x^6+2x^5+3x^4+3x^3+4x^2+3x+1
polinom setelah mod 8x ...x^4+x^3+x+1
1 12
['00000001'] ['00010010']
x^4+x
1 fb
['00000001'] ['11111011']
x^7+x^6+x^5+2x^4+x^3+2x+1
2 96

['00000010'] ['10010110']
x^8+x^7+x^6+2x^5+2x^4+2x^3+x^2+2x+1
3 24
['00000011'] ['00100100']
x^8+x^7+2x^6+3x^5+2x^4+3x^3+2x^2+2x+1
polinom setelah mod 8x ...x^7+x^5-x^4-x
1 a1
['00000001'] ['10100001']
x^7+x^5+1
1 70
['00000001'] ['01110000']
x^7+x^6+2x^5+x^4+1
2 96
['00000010'] ['10010110']
x^8+x^7+x^6+3x^5+x^4+x^3+x^2+1
3 72
['00000011'] ['01110010']
x^8+2x^7+3x^6+5x^5+2x^4+x^3+2x^2+x+1
polinom setelah mod 8x ...x^6+x^5-x^4
3 8a
['00000011'] ['10001010']
x^8+x^7+x^4+x^3+x^2+x
1 97
['00000001'] ['10010111']
x^8+2x^7+2x^4+x^3+2x^2+2x+1
1 87
['00000001'] ['10000111']
x^8+3x^7+2x^4+x^3+3x^2+3x+2
2 10
['00000010'] ['00010000']
x^8+3x^7+x^5+2x^4+x^3+3x^2+3x+2
polinom setelah mod 8x ...x^7+x^5-x^4+x^2-1
3 14
['00000011'] ['00010100']
x^5+x^4+x^3+x^2
1 5b
['00000001'] ['01011011']
x^6+x^5+2x^4+2x^3+x^2+x+1
1 c7
['00000001'] ['11000111']
x^7+2x^6+x^5+2x^4+2x^3+2x^2+2x+2
2 b6
['00000010'] ['10110110']
x^8+x^7+3x^6+2x^5+2x^4+3x^3+3x^2+2x+2
polinom setelah mod 8x ...x^7+x^6-x^4+x^2-x-1
3 12
['00000011'] ['00010010']

x^5+x^4+x^2+x
1 fb
['00000001'] ['11111011']
x^7+x^6+2x^5+2x^4+x^3+x^2+2x+1
1 96
['00000001'] ['10010110']
2x^7+x^6+2x^5+3x^4+x^3+2x^2+3x+1
2 24
['00000010'] ['00100100']
2x^7+2x^6+2x^5+3x^4+2x^3+2x^2+3x+1
polinom setelah mod 8x ...x^4+x+1
3 a1
['00000011'] ['10100001']
x^8+x^7+x^6+x^5+x+1
1 70
['00000001'] ['01110000']
x^8+x^7+2x^6+2x^5+x^4+x+1
1 96
['00000001'] ['10010110']
x^8+2x^7+2x^6+2x^5+2x^4+x^2+2x+1
2 72
['00000010'] ['01110010']
x^8+3x^7+3x^6+3x^5+2x^4+2x^2+2x+1
polinom setelah mod 8x ...x^7+x^6+x^5-x^4-x^3-x
after mixcolls 3a; b4; 80; 2d; 3d; 46; 7a; 92; 38; 1b; b2; 70; b5; d7; 13; fa
roundkey a5; d7; 5b; 85; 43; dd; af; 77; 9a; cc; 33; 07; 6d; 17; d8; b6
after addroundkeys 9f; 63; db; a8; 7e; 9b; d5; e5; a2; d7; 81; 77; d8; c0; cb; 4c

---

Round 7

after subbytes db; fb; b9; c2; f3; 14; 03; d9; 3a; 0e; 0c; f5; 61; ba; 1f; 29
after shiftrows db; fb; b9; c2; 14; 03; d9; f3; 0c; f5; 3a; 0e; 29; 61; ba; 1f
2 db
['00000010'] ['11011011']
x^8+x^7+x^5+x^4+x^2+x
3 14
['00000011'] ['00010100']
x^8+x^7+2x^5+2x^4+x^3+2x^2+x
1 0c
['00000001'] ['00001100']
x^8+x^7+2x^5+2x^4+2x^3+3x^2+x
1 29
['00000001'] ['00101001']
x^8+x^7+3x^5+2x^4+3x^3+3x^2+x+1
polinom setelah mod 8x ...x^7+x^5-x^4+x^2

2 fb
['00000010'] ['11111011']
x^8+x^7+x^6+x^5+x^4+x^2+x
3 03
['00000011'] ['00000011']
x^8+x^7+x^6+x^5+x^4+2x^2+3x+1
1 f5
['00000001'] ['11110101']
x^8+2x^7+2x^6+2x^5+2x^4+3x^2+3x+2
1 61
['00000001'] ['01100001']
x^8+2x^7+3x^6+3x^5+2x^4+3x^2+3x+3
polinom setelah mod 8x ...x^6+x^5-x^4-x^3+x^2
2 b9
['00000010'] ['10111001']
x^8+x^6+x^5+x^4+x
3 d9
['00000011'] ['11011001']
2x^8+2x^7+2x^6+2x^5+3x^4+x^3+2x+1
1 3a
['00000001'] ['00111010']
2x^8+2x^7+2x^6+3x^5+4x^4+2x^3+3x+1
1 ba
['00000001'] ['10111010']
2x^8+3x^7+2x^6+4x^5+5x^4+3x^3+4x+1
polinom setelah mod 8x ...x^7+x^4+x^3+1
2 c2
['00000010'] ['11000010']
x^8+x^7+x^2
3 f3
['00000011'] ['11110011']
2x^8+3x^7+2x^6+2x^5+x^4+2x^2+2x+1
1 0e
['00000001'] ['00001110']
2x^8+3x^7+2x^6+2x^5+x^4+x^3+3x^2+3x+1
1 1f
['00000001'] ['00011111']
2x^8+3x^7+2x^6+2x^5+2x^4+2x^3+4x^2+4x+2
polinom setelah mod 8x ...x^7
1 db
['00000001'] ['11011011']
x^7+x^6+x^4+x^3+x+1
2 14
['00000010'] ['00010100']
x^7+x^6+x^5+x^4+2x^3+x+1
3 0c
['00000011'] ['00001100']

x^7+x^6+x^5+2x^4+4x^3+x^2+x+1
1 29
['00000001'] ['00101001']
x^7+x^6+2x^5+2x^4+5x^3+x^2+x+2
polinom setelah mod 8x ...x^7+x^6+x^3+x^2+x
1 fb
['00000001'] ['11111011']
x^7+x^6+x^5+x^4+x^3+x+1
2 03
['00000010'] ['00000011']
x^7+x^6+x^5+x^4+x^3+x^2+2x+1
3 f5
['00000011'] ['11110101']
x^8+3x^7+3x^6+3x^5+2x^4+2x^3+2x^2+3x+2
1 61
['00000001'] ['01100001']
x^8+3x^7+4x^6+4x^5+2x^4+2x^3+2x^2+3x+3
polinom setelah mod 8x ...x^7-x^4-x^3
1 b9
['00000001'] ['10111001']
x^7+x^5+x^4+x^3+1
2 d9
['00000010'] ['11011001']
x^8+2x^7+2x^5+2x^4+x^3+x+1
3 3a
['00000011'] ['00111010']
x^8+2x^7+x^6+4x^5+4x^4+2x^3+x^2+2x+1
1 ba
['00000001'] ['10111010']
x^8+3x^7+x^6+5x^5+5x^4+3x^3+x^2+3x+1
polinom setelah mod 8x ...x^7+x^6+x^5+x^2
1 c2
['00000001'] ['11000010']
x^7+x^6+x
2 f3
['00000010'] ['11110011']
x^8+2x^7+2x^6+x^5+x^2+2x
3 0e
['00000011'] ['00001110']
x^8+2x^7+2x^6+x^5+x^4+2x^3+3x^2+3x
1 1f
['00000001'] ['00011111']
x^8+2x^7+2x^6+x^5+2x^4+3x^3+4x^2+4x+1
polinom setelah mod 8x ...x^5-x^4-x
1 db
['00000001'] ['11011011']
x^7+x^6+x^4+x^3+x+1

1 14
['00000001'] ['00010100']
x^7+x^6+2x^4+x^3+x^2+x+1
2 0c
['00000010'] ['00001100']
x^7+x^6+3x^4+2x^3+x^2+x+1
3 29
['00000011'] ['00101001']
x^7+2x^6+x^5+4x^4+3x^3+x^2+2x+2
polinom setelah mod 8x ...x^7+x^5+x^3+x^2
1 fb
['00000001'] ['11111011']
x^7+x^6+x^5+x^4+x^3+x+1
1 03
['00000001'] ['00000011']
x^7+x^6+x^5+x^4+x^3+2x+2
2 f5
['00000010'] ['11110101']
x^8+2x^7+2x^6+2x^5+x^4+2x^3+3x+2
3 61
['00000011'] ['01100001']
x^8+3x^7+4x^6+3x^5+x^4+2x^3+4x+3
polinom setelah mod 8x ...x^7+x^5-x^3-x
1 b9
['00000001'] ['10111001']
x^7+x^5+x^4+x^3+1
1 d9
['00000001'] ['11011001']
2x^7+x^6+x^5+2x^4+2x^3+2
2 3a
['00000010'] ['00111010']
2x^7+2x^6+2x^5+3x^4+2x^3+x^2+2
3 ba
['00000011'] ['10111010']
x^8+3x^7+3x^6+4x^5+5x^4+3x^3+2x^2+x+2
polinom setelah mod 8x ...x^7+x^6-1
1 c2
['00000001'] ['11000010']
x^7+x^6+x
1 f3
['00000001'] ['11110011']
2x^7+2x^6+x^5+x^4+2x+1
2 0e
['00000010'] ['00001110']
2x^7+2x^6+x^5+2x^4+x^3+x^2+2x+1
3 1f
['00000011'] ['00011111']

2x^7+2x^6+2x^5+4x^4+3x^3+3x^2+4x+2
polinom setelah mod 8x ...x^3+x^2
3 db
['00000011'] ['11011011']
x^8+2x^7+x^6+x^5+2x^4+x^3+x^2+2x+1
1 14
['00000001'] ['00010100']
x^8+2x^7+x^6+x^5+3x^4+x^3+2x^2+2x+1
1 0c
['00000001'] ['00001100']
x^8+2x^7+x^6+x^5+3x^4+2x^3+3x^2+2x+1
2 29
['00000010'] ['00101001']
x^8+2x^7+2x^6+x^5+4x^4+2x^3+3x^2+3x+1
polinom setelah mod 8x ...x^5-x^4-x^3+x^2
3 fb
['00000011'] ['11111011']
x^8+2x^7+2x^6+2x^5+2x^4+x^3+x^2+2x+1
1 03
['00000001'] ['00000011']
x^8+2x^7+2x^6+2x^5+2x^4+x^3+x^2+3x+2
1 f5
['00000001'] ['11110101']
x^8+3x^7+3x^6+3x^5+3x^4+x^3+2x^2+3x+3
2 61
['00000010'] ['01100001']
x^8+4x^7+4x^6+3x^5+3x^4+x^3+2x^2+4x+3
polinom setelah mod 8x ...x^5-x
3 b9
['00000011'] ['10111001']
x^8+x^7+x^6+2x^5+2x^4+x^3+x+1
1 d9
['00000001'] ['11011001']
x^8+2x^7+2x^6+2x^5+3x^4+2x^3+x+2
1 3a
['00000001'] ['00111010']
x^8+2x^7+2x^6+3x^5+4x^4+3x^3+2x+2
2 ba
['00000010'] ['10111010']
2x^8+2x^7+3x^6+4x^5+5x^4+3x^3+x^2+2x+2
polinom setelah mod 8x ...x^6+x^4+x^3+x^2
3 c2
['00000011'] ['11000010']
x^8+2x^7+x^6+x^2+x
1 f3
['00000001'] ['11110011']
x^8+3x^7+2x^6+x^5+x^4+x^2+2x+1

1 0e
['00000001'] ['00001110']
x^8+3x^7+2x^6+x^5+x^4+x^3+2x^2+3x+1
2 1f
['00000010'] ['00011111']
x^8+3x^7+2x^6+2x^5+2x^4+2x^3+3x^2+4x+1
polinom setelah mod 8x ...x^7-x^4-x^3+x^2-x
after mixcolls b4; 7c; 99; 80; ce; 98; e4; 32; ac; aa; c1; c; 3c; 22; 5c; 9e
roundkey 10; c7; 9c; 19; 86; 5b; f4; 83; d4; 18; 2b; 2c; fa; ed; 35; 83
after addroundkeys a4; bb; 05; 99; 48; c3; 10; b1; 78; b2; ea; 20; c6; cf; 69; 1d

---

Round 8

after subbytes 49; ea; 6b; ee; 52; 2e; ca; c8; bc; 37; 87; b7; b4; 8a; f9; a4
after shiftrows 49; ea; 6b; ee; 2e; ca; c8; 52; 87; b7; bc; 37; a4; b4; 8a; f9
2 49
['00000010'] ['01001001']
x^7+x^4+x
3 2e
['00000011'] ['00101110']
x^7+x^6+x^5+2x^4+2x^3+2x^2+2x
1 87
['00000001'] ['10000111']
2x^7+x^6+x^5+2x^4+2x^3+3x^2+3x+1
1 a4
['00000001'] ['10100100']
3x^7+x^6+2x^5+2x^4+2x^3+4x^2+3x+1
polinom setelah mod 8x ...x^7+x^6+x+1
2 ea
['00000010'] ['11101010']
x^8+x^7+x^6+x^4+x^2
3 ca
['00000011'] ['11001010']
2x^8+3x^7+2x^6+2x^4+x^3+2x^2+x
1 b7
['00000001'] ['10110111']
2x^8+4x^7+2x^6+x^5+3x^4+x^3+3x^2+2x+1
1 b4
['00000001'] ['10110100']
2x^8+5x^7+2x^6+2x^5+4x^4+x^3+4x^2+2x+1
polinom setelah mod 8x ...x^7+x^3+1
2 6b
['00000010'] ['01101011']
x^7+x^6+x^4+x^2+x
3 c8

['00000011'] ['11001000']
x^8+3x^7+2x^6+2x^4+x^3+x^2+x
1 bc
['00000001'] ['10111100']
x^8+4x^7+2x^6+x^5+3x^4+2x^3+2x^2+x
1 8a
['00000001'] ['10001010']
x^8+5x^7+2x^6+x^5+3x^4+3x^3+2x^2+2x
polinom setelah mod 8x ...x^7+x^5-x-1
2 ee
['00000010'] ['11101110']
x^8+x^7+x^6+x^4+x^3+x^2
3 52
['00000011'] ['01010010']
x^8+2x^7+2x^6+x^5+2x^4+x^3+2x^2+x
1 37
['00000001'] ['00110111']
x^8+2x^7+2x^6+2x^5+3x^4+x^3+3x^2+2x+1
1 f9
['00000001'] ['11111001']
x^8+3x^7+3x^6+3x^5+4x^4+2x^3+3x^2+2x+2
polinom setelah mod 8x ...x^7+x^6+x^5-x^4-x^3+x^2-x-1
1 49
['00000001'] ['01001001']
x^6+x^3+1
2 2e
['00000010'] ['00101110']
2x^6+x^4+2x^3+x^2+1
3 87
['00000011'] ['10000111']
x^8+x^7+2x^6+x^4+3x^3+3x^2+2x+2
1 a4
['00000001'] ['10100100']
x^8+2x^7+2x^6+x^5+x^4+3x^3+4x^2+2x+2
polinom setelah mod 8x ...x^5-x-1
1 ea
['00000001'] ['11101010']
x^7+x^6+x^5+x^3+x
2 ca
['00000010'] ['11001010']
x^8+2x^7+x^6+x^5+x^4+x^3+x^2+x
3 b7
['00000011'] ['10110111']
2x^8+3x^7+2x^6+3x^5+2x^4+2x^3+3x^2+3x+1
1 b4
['00000001'] ['10110100']
2x^8+4x^7+2x^6+4x^5+3x^4+2x^3+4x^2+3x+1

polinom setelah mod 8x ...x^4+x+1
1 6b
['00000001'] ['01101011']
x^6+x^5+x^3+x+1
2 c8
['00000010'] ['11001000']
x^8+x^7+x^6+x^5+x^4+x^3+x+1
3 bc
['00000011'] ['10111100']
2x^8+2x^7+2x^6+3x^5+3x^4+3x^3+x^2+x+1
1 8a
['00000001'] ['10001010']
2x^8+3x^7+2x^6+3x^5+3x^4+4x^3+x^2+2x+1
polinom setelah mod 8x ...x^7+x^5+x^4+x^2+1
1 ee
['00000001'] ['11101110']
x^7+x^6+x^5+x^3+x^2+x
2 52
['00000010'] ['01010010']
2x^7+x^6+2x^5+x^3+2x^2+x
3 37
['00000011'] ['00110111']
2x^7+2x^6+4x^5+x^4+2x^3+4x^2+3x+1
1 f9
['00000001'] ['11111001']
3x^7+3x^6+5x^5+2x^4+3x^3+4x^2+3x+2
polinom setelah mod 8x ...x^7+x^6+x^5+x^3+x
1 49
['00000001'] ['01001001']
x^6+x^3+1
1 2e
['00000001'] ['00101110']
x^6+x^5+2x^3+x^2+x+1
2 87
['00000010'] ['10000111']
x^8+x^6+x^5+3x^3+2x^2+2x+1
3 a4
['00000011'] ['10100100']
2x^8+x^7+2x^6+2x^5+4x^3+3x^2+2x+1
polinom setelah mod 8x ...x^7+x^2+1
1 ea
['00000001'] ['11101010']
x^7+x^6+x^5+x^3+x
1 ca
['00000001'] ['11001010']
2x^7+2x^6+x^5+2x^3+2x
2 b7

['00000010'] ['10110111']
x^8+2x^7+3x^6+2x^5+3x^3+x^2+3x
3 b4
['00000011'] ['10110100']
2x^8+3x^7+4x^6+4x^5+x^4+4x^3+2x^2+3x
polinom setelah mod 8x ...x^7+x^4+x
1 6b
['00000001'] ['01101011']
x^6+x^5+x^3+x+1
1 c8
['00000001'] ['11001000']
x^7+2x^6+x^5+2x^3+x+1
2 bc
['00000010'] ['10111100']
x^8+x^7+3x^6+2x^5+x^4+3x^3+x+1
3 8a
['00000011'] ['10001010']
2x^8+2x^7+3x^6+2x^5+2x^4+4x^3+x^2+2x+1
polinom setelah mod 8x ...x^6+x^2+1
1 ee
['00000001'] ['11101110']
x^7+x^6+x^5+x^3+x^2+x
1 52
['00000001'] ['01010010']
x^7+2x^6+x^5+x^4+x^3+x^2+2x
2 37
['00000010'] ['00110111']
x^7+3x^6+2x^5+x^4+2x^3+2x^2+3x
3 f9
['00000011'] ['11111001']
x^8+3x^7+5x^6+4x^5+3x^4+3x^3+2x^2+4x+1
polinom setelah mod 8x ...x^7+x^6-x
3 49
['00000011'] ['01001001']
x^7+x^6+x^4+x^3+x+1
1 2e
['00000001'] ['00101110']
x^7+x^6+x^5+x^4+2x^3+x^2+2x+1
1 87
['00000001'] ['10000111']
2x^7+x^6+x^5+x^4+2x^3+2x^2+3x+2
2 a4
['00000010'] ['10100100']
x^8+2x^7+2x^6+x^5+x^4+3x^3+2x^2+3x+2
polinom setelah mod 8x ...x^5-1
3 ea
['00000011'] ['11101010']

x^8+2x^7+2x^6+x^5+x^4+x^3+x^2+x
1 ca
['00000001'] ['11001010']
x^8+3x^7+3x^6+x^5+x^4+2x^3+x^2+2x
1 b7
['00000001'] ['10110111']
x^8+4x^7+3x^6+2x^5+2x^4+2x^3+2x^2+3x+1
2 b4
['00000010'] ['10110100']
2x^8+4x^7+4x^6+3x^5+2x^4+3x^3+2x^2+3x+1
polinom setelah mod 8x ...x^5+x^3+x+1
3 6b
['00000011'] ['01101011']
x^7+2x^6+x^5+x^4+x^3+x^2+2x+1
1 c8
['00000001'] ['11001000']
2x^7+3x^6+x^5+x^4+2x^3+x^2+2x+1
1 bc
['00000001'] ['10111100']
3x^7+3x^6+2x^5+2x^4+3x^3+2x^2+2x+1
2 8a
['00000010'] ['10001010']
x^8+3x^7+3x^6+2x^5+3x^4+3x^3+3x^2+2x+1
polinom setelah mod 8x ...x^7+x^6+x^2-x
3 ee
['00000011'] ['11101110']
x^8+2x^7+2x^6+x^5+x^4+2x^3+2x^2+x
1 52
['00000001'] ['01010010']
x^8+2x^7+3x^6+x^5+2x^4+2x^3+2x^2+2x
1 37
['00000001'] ['00110111']
x^8+2x^7+3x^6+2x^5+3x^4+2x^3+3x^2+3x+1
2 f9
['00000010'] ['11111001']
2x^8+3x^7+4x^6+3x^5+4x^4+2x^3+3x^2+4x+1
polinom setelah mod 8x ...x^7+x^5+x^2+1
after mixcolls c3; 89; a3; ff; 23; 13; b5; ea; 85; 92; 45; c2; 21; 2b; c6; a5
roundkey 7c; bb; 27; 3e; f7; ac; 58; db; 38; 20; 0b; 27; 2e; c3; f6; 75
after addroundkeys bf; 32; 84; c1; d4; bf; ed; 31; bd; b2; 4e; e5; 0f; e8; 30; d0

Round 9

after subbytes 08; 23; 5f; 78; 48; 08; 55; c7; 7a; 37; 2f; d9; 76; 9b; 04; 70
after shiftrows 08; 23; 5f; 78; 08; 55; c7; 48; 2f; d9; 7a; 37; 70; 76; 9b; 04

2 08
['00000010'] ['00001000']
x^4
3 08
['00000011'] ['00001000']
2x^4+x^3
1 2f
['00000001'] ['00101111']
x^5+2x^4+2x^3+x^2+x+1
1 70
['00000001'] ['01110000']
x^6+2x^5+3x^4+2x^3+x^2+x+1
polinom setelah mod 8x ...x^6+x^4+x^2+x+1
2 23
['00000010'] ['00100011']
x^6+x^2+x
3 55
['00000011'] ['01010101']
x^7+2x^6+x^5+x^4+x^3+2x^2+2x+1
1 d9
['00000001'] ['11011001']
2x^7+3x^6+x^5+2x^4+2x^3+2x^2+2x+2
1 76
['00000001'] ['01110110']
2x^7+4x^6+2x^5+3x^4+2x^3+3x^2+3x+2
polinom setelah mod 8x ...x^4+x^2+x
2 5f
['00000010'] ['01011111']
x^7+x^5+x^4+x^3+x^2+x
3 c7
['00000011'] ['11000111']
x^8+3x^7+x^6+x^5+x^4+2x^3+3x^2+3x+1
1 7a
['00000001'] ['01111010']
x^8+3x^7+2x^6+2x^5+2x^4+3x^3+3x^2+4x+1
1 9b
['00000001'] ['10011011']
x^8+4x^7+2x^6+2x^5+3x^4+4x^3+3x^2+5x+2
polinom setelah mod 8x ...-x^3+x^2-1
2 78
['00000010'] ['01111000']
x^7+x^6+x^5+x^4
3 48
['00000011'] ['01001000']
2x^7+2x^6+x^5+2x^4+x^3
1 37
['00000001'] ['00110111']

2x^7+2x^6+2x^5+3x^4+x^3+x^2+x+1
1 04
['00000001'] ['00000100']
2x^7+2x^6+2x^5+3x^4+x^3+2x^2+x+1
polinom setelah mod 8x ...x^4+x^3+x+1
1 08
['00000001'] ['00001000']
x^3
2 08
['00000010'] ['00001000']
x^4+x^3
3 2f
['00000011'] ['00101111']
x^6+x^5+2x^4+3x^3+2x^2+2x+1
1 70
['00000001'] ['01110000']
2x^6+2x^5+3x^4+3x^3+2x^2+2x+1
polinom setelah mod 8x ...x^4+x^3+1
1 23
['00000001'] ['00100011']
x^5+x+1
2 55
['00000010'] ['01010101']
x^7+2x^5+x^3+2x+1
3 d9
['00000011'] ['11011001']
x^8+3x^7+x^6+3x^5+2x^4+2x^3+3x+2
1 76
['00000001'] ['01110110']
x^8+3x^7+2x^6+4x^5+3x^4+2x^3+x^2+4x+2
polinom setelah mod 8x ...x^7-x^3+x^2-x-1
1 5f
['00000001'] ['01011111']
x^6+x^4+x^3+x^2+x+1
2 c7
['00000010'] ['11000111']
x^8+x^7+x^6+x^4+2x^3+2x^2+2x+1
3 7a
['00000011'] ['01111010']
x^8+2x^7+3x^6+2x^5+3x^4+3x^3+3x^2+3x+1
1 9b
['00000001'] ['10011011']
x^8+3x^7+3x^6+2x^5+4x^4+4x^3+3x^2+4x+2
polinom setelah mod 8x ...x^7+x^6-x^4-x^3+x^2-x-1
1 78
['00000001'] ['01111000']
x^6+x^5+x^4+x^3

2 48
['00000010'] ['01001000']
x^7+x^6+x^5+2x^4+x^3
3 37
['00000011'] ['00110111']
x^7+2x^6+3x^5+3x^4+2x^3+2x^2+2x+1
1 04
['00000001'] ['00000100']
x^7+2x^6+3x^5+3x^4+2x^3+3x^2+2x+1
polinom setelah mod 8x ...x^7+x^5+x^4+x^2+1
1 08
['00000001'] ['00001000']
x^3
1 08
['00000001'] ['00001000']
2x^3
2 2f
['00000010'] ['00101111']
x^6+x^4+3x^3+x^2+x
3 70
['00000011'] ['01110000']
x^7+3x^6+2x^5+2x^4+3x^3+x^2+x
polinom setelah mod 8x ...x^7+x^6+x^3+x^2+x
1 23
['00000001'] ['00100011']
x^5+x+1
1 55
['00000001'] ['01010101']
x^6+x^5+x^4+x^2+x+2
2 d9
['00000010'] ['11011001']
x^8+x^7+x^6+2x^5+2x^4+x^2+2x+2
3 76
['00000011'] ['01110110']
x^8+2x^7+3x^6+4x^5+3x^4+x^3+3x^2+3x+2
polinom setelah mod 8x ...x^6+x^2-1
1 5f
['00000001'] ['01011111']
x^6+x^4+x^3+x^2+x+1
1 c7
['00000001'] ['11000111']
x^7+2x^6+x^4+x^3+2x^2+2x+2
2 7a
['00000010'] ['01111010']
2x^7+3x^6+x^5+2x^4+x^3+3x^2+2x+2
3 9b
['00000011'] ['10011011']

x^8+3x^7+3x^6+2x^5+4x^4+2x^3+4x^2+4x+3
polinom setelah mod 8x ...x^7+x^6-x^4-x^3-x
1 78
['00000001'] ['01111000']
x^6+x^5+x^4+x^3
1 48
['00000001'] ['01001000']
2x^6+x^5+x^4+2x^3
2 37
['00000010'] ['00110111']
3x^6+2x^5+x^4+3x^3+x^2+x
3 04
['00000011'] ['00000100']
3x^6+2x^5+x^4+4x^3+2x^2+x
polinom setelah mod 8x ...x^6+x^4+x
3 08
['00000011'] ['00001000']
x^4+x^3
1 08
['00000001'] ['00001000']
x^4+2x^3
1 2f
['00000001'] ['00101111']
x^5+x^4+3x^3+x^2+x+1
2 70
['00000010'] ['01110000']
x^7+x^6+2x^5+x^4+3x^3+x^2+x+1
polinom setelah mod 8x ...x^7+x^6+x^4+x^3+x^2+x+1
3 23
['00000011'] ['00100011']
x^6+x^5+x^2+2x+1
1 55
['00000001'] ['01010101']
2x^6+x^5+x^4+2x^2+2x+2
1 d9
['00000001'] ['11011001']
x^7+3x^6+x^5+2x^4+x^3+2x^2+2x+3
2 76
['00000010'] ['01110110']
2x^7+4x^6+2x^5+2x^4+2x^3+3x^2+2x+3
polinom setelah mod 8x ...x^2+1
3 5f
['00000011'] ['01011111']
x^7+x^6+x^5+2x^4+2x^3+2x^2+2x+1
1 c7
['00000001'] ['11000111']
2x^7+2x^6+x^5+2x^4+2x^3+3x^2+3x+2

1 7a
['00000001'] ['01111010']
2x^7+3x^6+2x^5+3x^4+3x^3+3x^2+4x+2
2 9b
['00000010'] ['10011011']
x^8+2x^7+3x^6+3x^5+4x^4+3x^3+4x^2+5x+2
polinom setelah mod 8x ...x^6+x^5-x^4-1
3 78
['00000011'] ['01111000']
x^7+2x^6+2x^5+2x^4+x^3
1 48
['00000001'] ['01001000']
x^7+3x^6+2x^5+2x^4+2x^3
1 37
['00000001'] ['00110111']
x^7+3x^6+3x^5+3x^4+2x^3+x^2+x+1
2 04
['00000010'] ['00000100']
x^7+3x^6+3x^5+3x^4+3x^3+x^2+x+1
polinom setelah mod 8x ...x^7+x^6+x^5+x^4+x^3+x^2+x+1
after mixcolls 57; 16; d; 1b; 19; 8f; df; b5; ce; 45; da; 52; df; 5; 71; ff
roundkey de; 65; 42; 7c; 3b; 97; cf; 14; a5; 85; 8e; a9; 9c; 5f; a9; dc
after addroundkeys 89; 73; 4f; 67; 22; 18; 10; a1; 6b; c0; 54; fb; 43; 5a; d8; 23

Round 10

after subbytes a7; 8f; 84; 85; 93; ad; ca; 32; 7f; ba; 20; 0f; 1a; be; 61; 26
after shiftrows a7; 8f; 84; 85; ad; ca; 32; 93; 20; 0f; 7f; ba; 26; 1a; be; 61
2 a7
['00000010'] ['10100111']
x^8+x^6+x^3+x^2+x
3 ad
['00000011'] ['10101101']
2x^8+x^7+2x^6+x^5+x^4+3x^3+2x^2+2x+1
1 20
['00000001'] ['00100000']
2x^8+x^7+2x^6+2x^5+x^4+3x^3+2x^2+2x+1
1 26
['00000001'] ['00100110']
2x^8+x^7+2x^6+3x^5+x^4+3x^3+3x^2+3x+1
polinom setelah mod 8x ...x^7+x^5+x^4+x^3+x^2+x+1
2 8f
['00000010'] ['10001111']
x^8+x^4+x^3+x^2+x
3 ca

['00000011'] ['11001010']
2x^8+2x^7+x^6+2x^4+2x^3+2x^2+2x
1 0f
['00000001'] ['00001111']
2x^8+2x^7+x^6+2x^4+3x^3+3x^2+3x+1
1 1a
['00000001'] ['00011010']
2x^8+2x^7+x^6+3x^4+4x^3+3x^2+4x+1
polinom setelah mod 8x ...x^6+x^4+x^2+1
2 84
['00000010'] ['10000100']
x^8+x^3
3 32
['00000011'] ['00110010']
x^8+x^6+2x^5+x^4+x^3+x^2+x
1 7f
['00000001'] ['01111111']
x^8+2x^6+3x^5+2x^4+2x^3+2x^2+2x+1
1 be
['00000001'] ['10111110']
x^8+x^7+2x^6+4x^5+3x^4+3x^3+3x^2+3x+1
polinom setelah mod 8x ...x^7+x^2
2 85
['00000010'] ['10000101']
x^8+x^3+x
3 93
['00000011'] ['10010011']
2x^8+x^7+x^5+x^4+x^3+x^2+3x+1
1 ba
['00000001'] ['10111010']
2x^8+2x^7+2x^5+2x^4+2x^3+x^2+4x+1
1 61
['00000001'] ['01100001']
2x^8+2x^7+x^6+3x^5+2x^4+2x^3+x^2+4x+2
polinom setelah mod 8x ...x^6+x^5+x^2
1 a7
['00000001'] ['10100111']
x^7+x^5+x^2+x+1
2 ad
['00000010'] ['10101101']
x^8+x^7+x^6+x^5+x^4+x^3+x^2+2x+1
3 20
['00000011'] ['00100000']
x^8+x^7+2x^6+2x^5+x^4+x^3+x^2+2x+1
1 26
['00000001'] ['00100110']
x^8+x^7+2x^6+3x^5+x^4+x^3+2x^2+3x+1

polinom setelah mod 8x ...x^7+x^5
1 8f
['00000001'] ['10001111']
x^7+x^3+x^2+x+1
2 ca
['00000010'] ['11001010']
x^8+2x^7+x^4+x^3+2x^2+x+1
3 0f
['00000011'] ['00001111']
x^8+2x^7+2x^4+3x^3+4x^2+3x+2
1 1a
['00000001'] ['00011010']
x^8+2x^7+3x^4+4x^3+4x^2+4x+2
polinom setelah mod 8x ...-x^3-x-1
1 84
['00000001'] ['10000100']
x^7+x^2
2 32
['00000010'] ['00110010']
x^7+x^6+x^5+2x^2
3 7f
['00000011'] ['01111111']
2x^7+3x^6+3x^5+2x^4+2x^3+4x^2+2x+1
1 be
['00000001'] ['10111110']
3x^7+3x^6+4x^5+3x^4+3x^3+5x^2+3x+1
polinom setelah mod 8x ...x^7+x^6+x^4+x^3+x^2+x+1
1 85
['00000001'] ['10000101']
x^7+x^2+1
2 93
['00000010'] ['10010011']
x^8+x^7+x^5+2x^2+x+1
3 ba
['00000011'] ['10111010']
2x^8+2x^7+x^6+3x^5+2x^4+x^3+3x^2+2x+1
1 61
['00000001'] ['01100001']
2x^8+2x^7+2x^6+4x^5+2x^4+x^3+3x^2+2x+2
polinom setelah mod 8x ...x^3+x^2
1 a7
['00000001'] ['10100111']
x^7+x^5+x^2+x+1
1 ad
['00000001'] ['10101101']
2x^7+2x^5+x^3+2x^2+x+2
2 20

['00000010'] ['00100000']
2x^7+x^6+2x^5+x^3+2x^2+x+2
3 26
['00000011'] ['00100110']
2x^7+2x^6+3x^5+2x^3+4x^2+2x+2
polinom setelah mod 8x ...x^5
1 8f
['00000001'] ['10001111']
x^7+x^3+x^2+x+1
1 ca
['00000001'] ['11001010']
2x^7+x^6+2x^3+x^2+2x+1
2 0f
['00000010'] ['00001111']
2x^7+x^6+x^4+3x^3+2x^2+3x+1
3 1a
['00000011'] ['00011010']
2x^7+x^6+x^5+3x^4+4x^3+3x^2+4x+1
polinom setelah mod 8x ...x^6+x^5+x^4+x^2+1
1 84
['00000001'] ['10000100']
x^7+x^2
1 32
['00000001'] ['00110010']
x^7+x^5+x^4+x^2+x
2 7f
['00000010'] ['01111111']
2x^7+x^6+2x^5+2x^4+x^3+2x^2+2x
3 be
['00000011'] ['10111110']
x^8+3x^7+2x^6+4x^5+4x^4+3x^3+4x^2+3x
polinom setelah mod 8x ...x^7-x^4-1
1 85
['00000001'] ['10000101']
x^7+x^2+1
1 93
['00000001'] ['10010011']
2x^7+x^4+x^2+x+2
2 ba
['00000010'] ['10111010']
x^8+2x^7+x^6+x^5+2x^4+2x^2+x+2
3 61
['00000011'] ['01100001']
x^8+3x^7+3x^6+2x^5+2x^4+2x^2+2x+3
polinom setelah mod 8x ...x^7+x^6-x^4-x^3-x
3 a7
['00000011'] ['10100111']

x^8+x^7+x^6+x^5+x^3+2x^2+2x+1
1 ad
['00000001'] ['10101101']
x^8+2x^7+x^6+2x^5+2x^3+3x^2+2x+2
1 20
['00000001'] ['00100000']
x^8+2x^7+x^6+3x^5+2x^3+3x^2+2x+2
2 26
['00000010'] ['00100110']
x^8+2x^7+2x^6+3x^5+3x^3+4x^2+2x+2
polinom setelah mod 8x ...x^5-x^4-x-1
3 8f
['00000011'] ['10001111']
x^8+x^7+x^4+2x^3+2x^2+2x+1
1 ca
['00000001'] ['11001010']
x^8+2x^7+x^6+x^4+3x^3+2x^2+3x+1
1 0f
['00000001'] ['00001111']
x^8+2x^7+x^6+x^4+4x^3+3x^2+4x+2
2 1a
['00000010'] ['00011010']
x^8+2x^7+x^6+x^5+2x^4+4x^3+4x^2+4x+2
polinom setelah mod 8x ...x^6+x^5-x^4-x^3-x-1
3 84
['00000011'] ['10000100']
x^8+x^7+x^3+x^2
1 32
['00000001'] ['00110010']
x^8+x^7+x^5+x^4+x^3+x^2+x
1 7f
['00000001'] ['01111111']
x^8+x^7+x^6+2x^5+2x^4+2x^3+2x^2+2x+1
2 be
['00000010'] ['10111110']
2x^8+x^7+2x^6+3x^5+3x^4+3x^3+3x^2+2x+1
polinom setelah mod 8x ...x^7+x^5+x^4+x^3+x^2+1
3 85
['00000011'] ['10000101']
x^8+x^7+x^3+x^2+x+1
1 93
['00000001'] ['10010011']
x^8+2x^7+x^4+x^3+x^2+2x+2
1 ba
['00000001'] ['10111010']
x^8+3x^7+x^5+2x^4+2x^3+x^2+3x+2
2 61

['00000010'] ['01100001']
x^8+4x^7+x^6+x^5+2x^4+2x^3+x^2+4x+2
polinom setelah mod 8x ...x^6+x^5-x^4-x^3+x^2-x-1
after mixcolls bf; 55; 84; 64; a0; b; df; c; 20; 75; 91; da; 33; 7b; bd; 7f
roundkey 12; 77; 35; 49; e8; 7f; b0; a4; 23; a6; 28; 81; 8c; d3; 7a; a6
after addroundkeys b5; f8; b1; cc; 45; b5; 82; 37; 03; a9; 57; 3b; aa; c9; c4; c7
