Zobrazení SBoxu a odstranění reverzace u afinní ransformace:

In[ ]:=
```
m = x^8 + x^4 + x^3 + x + 1;
a = x^7 + x + 1;
inv[polynom_] := PolynomialExtendedGCD[polynom, m, x, Modulus → 2][[2, 1]];
aff[polynom_] := PolynomialRemainder[
   (x^6 + x^5 + x + 1) + polynom (x^4 + x^3 + x^2 + x + 1), x^8 + 1, x, Modulus → 2];
p2hex[polynom_] := polynom /. {x → 2} // IntegerString[#, 16, 2] &;
invItem[polynom_] := inv[polynom] // aff // p2hex;
fourBitRepresentation[number_] := PadLeft[IntegerDigits[number - 1, 2], 4];
polynomFromSBoxPosition[xx_, yy_] :=
  Join[fourBitRepresentation[xx], fourBitRepresentation[yy]] //
    FromDigits[#, x] & // Expand;
SBox = Table[invItem[polynomFromSBoxPosition[i, j]], {i, 16}, {j, 16}];
TableForm[SBox, TableHeadings →
  {{"0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "a", "b", "c", "d", "e", "f"},
   {"0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "a", "b", "c", "d", "e", "f"}}]
```

Out[ ]//TableForm=

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	a
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	7
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	3
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	5
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	1
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	a
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	2
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	b

Úlohy z Moodlu:

Dopočítejte výstup SBOXu, tj. SubBytes pro bajt {73}.:

```
In[ ]:= getSBoxValueHEX[value_] :=
          SBox[[Interpreter["HexInteger"][StringTake[ToString[value], 1]] + 1,
           Interpreter["HexInteger"][StringTake[ToString[value], -1]] + 1]];
        getSBoxValueHEX["73"]
        getSBoxValueHEX[73]
```

Out[ ]= 8f

Out[ ]= 8f

Spočítejte multiplikativní inverzi polynomu a(x)={73} modulo m(x)={11b}, tedy b(x)=a(x)-1 mod m(x). Použijte rozšířený Euklidův algoritmus pro polynomy:

```
In[ ]:= hexToBinary[value_] := IntegerDigits[FromDigits[ToString[value], 16], 2];
        hex2p[value_] := PadLeft[hexToBinary[value], 8] // FromDigits[#, x] & // Expand;
        aPolynom = hex2p["73"]
        mPolynom = hex2p["bb"]
        aPolInv = PolynomialExtendedGCD[aPolynom, mPolynom, x, Modulus → 2][[2, 1]]
        PolynomialRemainder[aPolInv * aPolynom, mPolynom, x, Modulus → 2]
```

Out[ ]= $1 + x + x^4 + x^5 + x^6$

Out[ ]= $1 + x + x^3 + x^4 + x^5 + x^7$

Out[ ]= x^2

Out[ ]= 1