TECHNICKÁ UNIVERZITA KOŠICE
Fakulta elektrotechniky a informatiky
Katedra elektroniky a multimediálnych telekomunikácií

APLIKOVANÁ KRYPTOGRAFIA

Dátum : 15.5.2001
Ročník : 4.

Vypracovali : R. Machaj
D. Tomečko
A. Varga

Úloha.

Vytvorte inverznú S tabuľku a túto preveďte do hexadecimálneho tvaru.

Teoretický rozbor.

Operácia ByteSub

Operácia **Bytesub** je nelineárna bajtová substitúcia, realizovaná nezávisle na všetkých bajtoch matice (1.0).

$$A = \begin{bmatrix} A_{00} & A_{01} & A_{02} & & A_{N_b-1} \\ A_{10} & A_{11} & A_{12} & & A_{1N_b-1} \\ A_{20} & A_{22} & A_{23} & & A_{2N_b-1} \\ A_{30} & A_{32} & A_{33} & & A_{3N_b-1} \end{bmatrix} \tag{1.0}$$

Substitučná tabuľka (tzv S-box) je invertiblná transformácia skladajúca sa z dvoch transformácií:

1. pre hodnotu $A_{ij} \in GF(2^8), A_{ij} \neq 0$ určíme multiplikatívne inverzné číslo $A_{ij} = 0$ je mapovaná na hodnotu 0.
2. Hodnota $X \leftrightarrow (x_7, x_6, ..., x_0)$ je transformovaná affinou transformáciou (nad telesom GF(2)) podľa vzťahu

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \overline{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{1.1}$$

Použitie S-boxu na všetky bajty premennej *stav* je označované ako *ByteSub(State)*.

Použité tabuľky:

word8 Logtable[256]={
0, 0, 25, 1, **50**, 2, 26, 198, 75, 199, 27, 104, 51, 238, 223, 3,
100, 4, 224, 14, 52, 141, 129, 239, 76, 113, 8, 200, 248, 105, 28, 193,
125, 194, 29, 181, 249, 185, 39, 106, 77, 228, 166, 114, 154, 201, 9, 120,
101, 47, 138, 5, 33, 15, 225, 36, 18, 240, 130, 69, 53, 147, 218, 142,
150, 143, 219, 189, 54, 208, 206, 148, 19, 92, 210, 241, 64, 70, 131, 56,
102, 221, 253, 48, 191, 6, 139, 98, 179, 37, 226, 152, 34, 136, 145, 16,
126, 110, 72, 195, 163, 182, 30, 66, 58, 107, 40, 84, 250, 133, 61, 186,
43, 121, 10, 21, 155, 159, 94, 202, 78, 212, 172, 229, 243, 115, 167, 87,
175, 88, 168, 80, 244, 234, 214, 116, 79, 174, 233, 213, 231, 230, 173, 232,
44, 215, 117, 122, 235, 22, 11, 245, 89, 203, 95, 176, 156, 169, 81, 160,
127, 12, 246, 111, 23, 196, 73, 236, 216, 67, 31, 45, 164, 118, 123, 183,
204, 187, 62, 90, 251, 96, 177, 134, 59, 82, 161, 108, 170, 85, 41, 157,
151, 178, 135, 144, 97, 190, 220, 252, 188, 149, 207, 205, 55, 63, 91, 209,
83, 57, 132, 60, 65, 162, 109, 71, 20, 42, 158, 93, 86, 242, 211, 171,
68, 17, 146, 217, 35, 32, 46, 137, 180, 124, 184, 38, 119, 153, 227, 165,
103, 74, 237, 222, 197, 49, 254, 24, 13, 99, 140, 128, 192, 247, 112, 7
};

word8 Alogtable[256]={
1, 3, 5, 15, 17, 51, 85, 255, 26, 46, 114, 150,161, 248, 19, 53,
95, 225, 56,72, 216, 115, 149, 164, 247, 2, 6, 10, 30, 34, 102, 170,
229, 52, 92, 228, 55, 89, 235, 38, 106, 190, 217, 112, 144, 171, 230, 49,
83, 245, 4, 12, 20, 60, 68, 204, 79, 209, 104, 184, 211, 110, 178, 205,
76, 212, 103, 169, 224, 59, 77, 215, 98, 166, 241, 8, 24, 40, 120, 136,
131, 158, 185, 208, 107, 189, 220, 127, 129, 152, 179, 206, 73, 219, 118, 154,
181, 196, 87, 249, 16, 48, 80, 240, 11, 29, 39, 105, 187, 214, 97, 163
254, 25, 43, 125, 135, 146, 173, 236, 47, 113, 147, 174, 233, 32, 96, 160,
251, 22, 58, 78, 210, 109, 183, 194, 93, 231, 50, 86, 250, 21, 63, 65,
195, 94, 226, 61, 71, 201, 64, 192, 91, 237, 44, 116, 156, 191, 218, 117,
159, 186, 213, 100, 172, 239, 42, 126, 130, 157, 188, 223, 122, 142, 137, 128,
155, 182, 193, 88, 232, 35, 101, 175, 234, 37, 111, 177, 200, 67, 197, 84,
252, 31, 33, 99, 165, 244, 7, 9, 27, 45, 119, 153, 176, **203**, 70, 202,
69, 207, 74, 222, 121, 139, 134, 145, 168, 227, 62, 66, 198, 81, 243, 14,
18, 54, 90, 238, 41, 123, 141, 140, 143, 138, 133, 148, 167, 242, 13, 23,
57, 75, 221, 124, 132, 151, 162, 253, 28, 36, 108, 180, 199, 82, 246, 1
};

S-Tabuľky:

Word8 S[256]={
99, 124, 119, 123, 24, 107, 111, 197, 48, 1, 103, 43, 254, 215, 171, 118,
202, 130, 201, 125, 250, 89, 71, 240, 173, 212, 162, 175, 156, 164, 114, 192,
183, 253, 143, 38, 54, 63, 247, 204, 52, 165, 229, 241, 113, 216, 49, 21,
4, 199, 35, 195, 24, 150, 5, 154, 7, 18, 128, 226, 235, 39, 178, 117,
9, 131, 44, 26, 27, 110, 90, 160, 82, 59, 214, 179, 41, 227, 47, 132,
83, 209, 0, 237, 32, 252, 177, 91, 106, 203, 190, 57, 74, 76, 88, 207,
208, 239, 170, 251, 67, 77, 51, 133, 69, 249, 2, 127, 80, 60, 159, 168,
81, 163, 64, 143, 146, 157, 56, 245, 188, 182, 218, 33, 16, 255, 243, 210,
205, 12, 19, 236, 95, 151, 68, 23, 196, 167, 126, 61, 100, 93, 25, 115,
96, 129, 79, 220, 34, 42, 144, 136, 70, 238, 184, 20, 222, 94, 11, 219,
224, 50, 58, 10, 73, 6, 36, 92, 194, 211, 172, 98, 145, 149, 228, 121,
231, 200, 55, 109, 141, 213, 78, 169, 108, 86, 244, 234, 101, 122, 174, 8,
186, 120, 37, 46, 28, 166, 180, 198, 232, 221, 116, 31, 75, 189, 139, 138,
112, 62, 181, 102, 72, 3, 246, 14, 97, 53, 87, 185, 134, 193, 29, 158,
225, 248, 152, 17, 105, 217, 142, 148, 155, 30, 135, 233, 206, 85, 40, **223**,
140, 161, 137, 13, 191, 230, 66, 104, 65, 153, 45, 15, 176, 84, 187, 22
};

Word8 Si[256]={
82, 9, 106, 213, 48, 54, 165, 56, 191, 64, 163, 158, 129, 243, 215, 251,
124, 227, 57, 130, 155, 47, 255, 135, 52, 142, 67, 68, 196, 222, 233, 203,
84, 123, 148, 50, 166, 194, 35, 61, 238, 76, 149, 11, 66, 250, 195, 78,
8, 46, 161, 102, 40, 217, 36, 178, 118, 91, 162, 73, 109, 139, 209, 37,
114, 248, 246, 10, 134, 104, 152, 22, 212, 164, 92, 204, 93, 101, 182, 146,
108, 112, 72, 80, 253, 237, 185, 218, 94, 21, 70, 87, 167, 141, 157, 132,
144, 216, 171, 0, 140, 188, 211, 10, 247, 228, 88, 5, 184, 179, 69, 6,
208, 44, 30, 143, 202, 63, 15, 2, 193, 175, 189, 3, 1, 19, 138, 107
58, 145, 17, 65, 79, 103, 220, 234, 151, 242, 207, 206, 240, 180, 230, 115,
150, 172, 116, 34, 231, 173, 53, 133, 226, 249, 55, 232, 28, 117, 223, 110,
71, 241, 26, 113, 29, 41, 197, 137, 111, 183, 98, 14, 170, 24, 190, 27,
252, 86, 62, 75, 198, 210, 121, 32, 154, 219, 192, 254, 120, 205, 90, 244,
31, 221, 168, 51, 136, 7, 199, 49, 177, 18, 16, 89, 39, 128, 236, 95,
96, 81, 127, 169, 25, 181, 74, 13, 45, 229, 122, 159, 147, 201, 156, **239**,
160, 224, 59, 77, 174, 42, 245, 176, 200, 235, 187, 60, 131, 83, 153, 97,
23, 43, 4, 126, 186, 119, 214, 38, 225, 105, 20, 99, 85, 33, 12, 125
};

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

Postup pri vytváraní S tabuľky:

V logaritmickej tabuľke si ako prvé určíme hodnotu exponentu logaritmu v Galoisovom poli. Nech je to napr. $\log_Z 4 = e$, kde e –reprezentuje exponent, ktorého hodnotu si určíme pomocou logaritmickej tabuľky Logtable[256].
S tabuľky je to hodnota 50 pričom si treba všimnúť usporiadanie hodnôt v tabuľke ktoré je nasledovné: prvé číslo predstavuje nultú pozíciu a zvyšné pozície jedna až dvestopäťdesiatpäť. Na 5 pozícii (hodnota 4) je teda $\rightarrow e = 50,\ (4 = z^{50})$. Pre hodnotu 50 určíme inverzný prvok e^- tak, že vychádzame z podmienky $e + e^- = 255(= 0)$. Teda $e^- = 255 - e = 255 - 50 = 205$. Túto hodnotu si nájdeme v tabuľke Logtable (kde je zvýraznená). Teraz máme opačný prípad kedy k exponentu $e^- = 205$ máme určiť hodnotu logaritmu. Pri tomto použijeme antilogaritmickú tabuľku Alogtable[256]. Exponent 205 nám reprezentuje pozíciu prvku v antilogaritmickej tabuľke. Táto tabuľka má tiež usporiadanie počnúc 0 po 255. Tak k exponentu 205 je výsledok na pozícii 206. Táto pozícia má hodnotu 203 a teda platí $z^{205} = 203$. Spätným postupom sa dá overiť hodnota logaritmu 4. Hodnota 203 zodpovedá multiplikatívnemu inverznému číslu X, ktoré nám poslúži k vytvoreniu S (substitučnej) tabuľky. Číslo X vyjadrené v binárnom tvare sa dosadí do vzťahu (1.1), ktorého výsledkom je číslo $(1\ 1\ 0\ 1\ 1\ 1\ 1\ 1)_2 = (223)_{10}$. Tento údaj je v tabuľke S[256] zvýraznený. Tabuľku Si (inverznú ku S) zostavíme tak, že preusporiadame S tabuľku tek, že čísla pozícií budú predstavovať hodnoty a naopak, jej hodnoty budú v inverznej S-Tabuľke príslušné. Platí, že prvok 223 z S[256] , je v tejto tabuľke na 239 pozícii. Táto pozícia je súčasne hodnota prvku v Si tabuľke t.j. 239, ktorá je na 223+1 pozícii v tabuľke Si[256].
Spätné overenie spočíva v určení pozície v tabuľke S[256] kde pre pozíciu (239+1) je hodnota 223.

Uskutočníme tento celý postup ešte pre hodnotu logaritmu 247, ktorej zodpovedá exponent $e = 24$, $247 = z^{24}$. Pre e je $e^{-} = 255 - 24 = 231$. V tabuľke Alogtable [256] je na pozícii (231+1) hodnota 140, $z^{231} = 240$. Dosadením $X = (140)_{10}$ do vzťahu (1.1) v binárnom tvare dostaneme výslednú hodnotu v S tabuľke $(0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0)_2 = (118)_{10}$. Pre túto hodnotu 118, ktorá je v S tabuľke na pozícii 15, v tabuľke Si zodpovedá na pozícii (118+1) hodnota 15. Pri spätnom postupe z 15 sa v S tabuľke dopracujeme k hodnote 118 na pozícii (15+1).

Postup pri vytváraní Si tabuľky:

V tomto prípade máme k dispozícii y. Zo vzťahu 1.1, v ktorom si prv vyjadríme vektor x, obdržíme x^{-1} nasledovne.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} \overline{1} & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Ak si ju prepíšeme do symbolického tvaru:

$$\bar{y} = \underline{A}.\bar{x} \otimes \bar{v}$$

Vyjadríme si vektor $\bar{x}$:

$$\bar{x} = \underline{A}^{-1}.\left(\bar{y} \oplus \bar{v}\right)$$

$\underline{A}^{-1}$ ... Inverzná matica ku matici $\underline{A}$

$\bar{v}$ ... $[1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0]^T$

Teda:

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} . \left(\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right)$$

Výsledný vektor $\bar{x}$ predstavuje x^{-1}. K tomuto číslu ešte musíme nájsť príslušné inverzné číslo x, ako prvok *Si* tabuľky.

Príklad 1.

Nech $\bar{y} = (223)_{10} = [1 \;\; 1 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 1 \;\; 1]_2 = [y_0 \;\; y_1 \;\; y_2 \;\; y_3 \;\; y_4 \;\; y_5 \;\; y_6 \;\; y_7]$

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} . \left(\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$[1 \;\; 1 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 1 \;\; 1]_2 = (203)_{10} = \bar{x}$$

Inverzné číslo hľadáme podobne, ako pri vytváraní S tabuľky:

- 203 -tia pozícia Logaritmickej tabuľky je číslo 205
- $e^- = 255 - e = 255 - 205 = 50$, teda si nájdeme $50 + 1$. pozíciu Alogaritmickej tabuľky, čo je číslo $\underline{\underline{4}}$.

Tento výsledok je prvok Si tabuľky.

Príklad 2.

Nech $\bar{y} = (224)_{10} = [1 \;\; 1 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0]_2 = [y_0 \;\; y_1 \;\; y_2 \;\; y_3 \;\; y_4 \;\; y_5 \;\; y_6 \;\; y_7]$

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} . \left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$[0 \;\; 1 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 1]_2 = (79)_{10} = \bar{x}$$

Inverzné číslo hľadáme podobne, ako pri vytváraní S tabuľky:

- 79 -ta pozícia Logaritmickej tabuľky je číslo 56
- $e^- = 255 - e = 255 - 56 = 199$, teda si nájdeme $199 + 1$. pozíciu Alogaritmickej tabuľky, čo je číslo $\underline{\underline{9}}$.

Príklad 3.

Nech $\bar{y} = (225)_{10} = [1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1]_2 = [y_0\ \ y_1\ \ y_2\ \ y_3\ \ y_4\ \ y_5\ \ y_6\ \ y_7]$

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \cdot \left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$[1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1]_2 = (235)_{10} = \bar{x}$$

Inverzné číslo hľadáme podobne, ako pri vytváraní S tabuľky:

- 235 -ta pozícia Logaritmickej tabuľky je číslo 85
- $e^- = 255 - e = 255 - 85 = 140$, teda si nájdeme $140 + 1$. pozíciu Alogaritmickej tabuľky, čo je číslo $\underline{\underline{250}}$.

Príklad 4.

Nech $\bar{y} = (15)_{10} = [0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1]_2 = [y_0\ \ y_1\ \ y_2\ \ y_3\ \ y_4\ \ y_5\ \ y_6\ \ y_7]$

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \cdot \left(\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$[1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0]_2 = (140)_{10} = \bar{x}$$

Inverzné číslo hľadáme podobne, ako pri vytváraní S tabuľky:

- 140 -ta pozícia Logaritmickej tabuľky je číslo 231
- $e^- = 255 - e = 255 - 231 = 24$, teda si nájdeme $24 + 1$. pozíciu Alogaritmickej tabuľky, čo je číslo $\underline{\underline{247}}$.

Skúška Správnosti:

Vykonajme skúšku správnosti určenia inverzného čísla aspoň pre jeden prípad.
Násobenie dvoch prvkov $A, B \in GF(2^8)$ je definované takto:

$$A \bullet B \leftrightarrow (a \bullet b)_{GF(2^8)} = a(X)b(X) \bmod m(X)$$

Keďže v tomto prípade sa jedná o inverzné čísla, musí platiť:

$$a(X)a^{-1}(X) \bmod m(X) = 1$$

$a = (203)_{10} = (1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1)_2 \Rightarrow a(X) = x^7 + x^6 + x^3 + x + 1$

$a = (4)_{10} = (0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0)_2 \Rightarrow a(X) = x^2$

$m(X) = x^8 + x^4 + x^3 + x + 1$

$(x^7 + x^6 + x^3 + x + 1)(x^2) \bmod m(x) =$

$(x^9 + x^8 + x^5 + x^3 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x + 1$

$x^9 + x^5 + x^4 + x^2 + x$

$x^8 + x^4 + x^3 + x$

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

1

S-Box pre čísla z postupnosti {0,1,2,...,255}

{

55 55, 135, 71, 223, 70, 6, 172, 243, 224,134, 66, 31, 141, 74, 151,
92, 216, 108, 39, 95, 101, 132, 255, 42, 189, 218, 10, 57, 186, 215, 252,
139, 47, 201, 146, 147, 3, 143, 60, 179, 170, 174, 239, 231, 125, 227, 161,
176, 140, 194, 204, 113, 153, 160, 89, 128, 209, 248, 222, 78, 130, 219, 167,
96, 200, 50, 81, 65, 22, 85, 250, 213, 67, 157, 203, 98, 206, 2, 184,
197, 237, 240, 46, 242, 63, 235, 69, 86, 76, 27, 99, 84, 52, 117, 12,
253, 14, 90, 79, 196, 36, 195, 168, 164, 111, 208, 7, 245, 51, 9, 122,
229, 202, 244, 8, 217, 41, 115, 175, 59, 155, 93, 226, 241, 15, 207, 221,
44, 48, 193, 62, 5, 137, 180, 129, 188, 138, 23, 35, 182, 37, 97, 199,
246, 232, 4, 61, 210, 82, 249, 120, 148, 30, 123, 177, 29, 21, 64, 77,
254, 211, 83, 80, 100, 144, 178, 53, 220, 205, 58, 214, 233, 169, 190, 103,
142, 124, 131, 38, 40, 173, 20, 106, 54, 149, 191, 94, 166, 87, 26, 112,
91, 119, 162, 18, 49, 154, 187, 156, 126, 45, 183, 1, 68, 43, 72, 88,
247, 19, 171, 150, 116, 192, 159, 16, 230, 163, 133, 10, 152, 236, 33, 25,
238, 127, 121, 225, 102, 109, 24, 185, 73, 17, 136, 110, 28, 165, 114, 13,
56, 234, 104, 32, 11, 158, 212, 118, 228, 105, 34, 0, 251, 181, 75, 145

}

S-box vytvorená z ALogtable(256)

{

55, 71, 70, 151, 216, 204, 63, 145, 218, 227, 246, 249, 211, 228, 39, 153,
12, 127, 128, 213, 230, 8, 61, 100, 118, 135, 6, 134, 215, 201, 195, 58,
109, 113, 84, 102, 89, 76, 110, 143, 208, 26, 163, 229, 246, 214, 24, 140
46, 158, 223, 31, 95, 78, 65, 68, 184, 19, 164, 54, 150, 9, 131, 43
98, 116, 168, 205, 238, 222, 206, 16, 90, 178, 234, 243, 42, 179, 59, 180
62, 64, 149, 247, 7, 87, 152, 221, 48, 148, 38, 72, 67, 107, 115, 123
173, 49, 69, 105, 92, 176, 197, 56, 66, 186, 60, 111, 94, 159, 14, 80
75, 189, 239, 15, 129, 4, 169, 28, 161, 202, 61, 190, 17, 139, 253, 254
0, 132, 248, 2, 171, 51, 106, 162, 52, 185, 194, 235, 34, 101, 167, 200,
18, 117, 121, 130, 250, 45, 96, 91, 99, 165, 231, 217, 29, 112, 133, 41,
77, 191, 192, 196, 233, 13, 174, 207, 193, 21, 166, 25, 93, 97, 138, 44,
177, 20, 119, 86, 73, 146, 36, 103, 136, 3, 122, 124, 126, 81, 154, 242,
251, 252, 47, 79, 144, 11, 172, 224, 10, 125, 175, 30, 142, 1, 85, 183,
22, 88, 157, 33, 155, 35, 180, 232, 220, 225, 219, 50, 187, 237, 32, 74,
108, 160, 27, 114, 170, 226, 37, 182, 199, 23, 137, 210, 53, 104, 141, 255,
209, 203, 236, 241, 5, 120, 83, 181, 57, 147, 245, 40, 156, 240, 212, 55

}