Katedra elektroniky a multimediálnych telekomunikácií

Zadanie z predmetu Aplikovaná kryptografia

2000/2001

Peter Leško
Imrich Mikita

Zadanie z predmetu Aplikovaná kryptografia

Úloha:

1. Vysvetlenie spôsobu použitia logaritmickej a antilogaritmickej tabuľky, pri softvérovej realizácii algoritmu Rijandel.

2. Pretransformovanie logaritmickej tabuľky do hexadecimálneho kódu.

Teoretický rozbor:

Šifra Rijandel je interačná bloková šifra (t.j. používa N_r opakujúcich sa rúnd).Jednotlivé bloky šifry pracujú s údajmi (medzivýsledkami), nazývanými ***Stav***. Stav je možné reprezentovať, ako obdĺžnikovú maticu, ktorá má 4 riadky a N_b stĺpcov, kde N_b je dĺžka bloku(násobok 32 bitov). Po počiatočných operáciách (výpočet rundových kľúčov a „naxorovanie“), sa získané informácie uložia do premennej *Stav*, ktorá je tvorená maticou **A** s rozmermi 4xN_b .Potom sa vykoná N_r rúnd podľa nasledujúceho pseudo kódu v jazyku C:

```
Round(State,RoundKey)
{
ByteSub(State);
ShiftRow(State);
MixColumn(State);          //nevykonáva sa v poslednej runde
AddRoundKey(State,RoundKey);
}
```

pričom ***Stav*** je reprezentovaný maticou

$$\mathbf{A} = \begin{bmatrix} A_{00} & A_{01} & A_{02} & \dots & \dots & A_{0N_b-1} \\ A_{10} & A_{11} & A_{12} & \dots & \dots & A_{1N_b-1} \\ A_{21} & A_{22} & A_{23} & \dots & \dots & A_{2N_b-1} \\ A_{31} & A_{32} & A_{33} & \dots & \dots & A_{3N_b-1} \end{bmatrix} \tag{1}$$

Operácia Mixcolumn:

Operácia **Mixcolumn** spracováva stĺpce matice ***Stav***(interpretované ako koeficienty polynómu nad telesom GF(2^8)) pomocou súčinu $\otimes$, s polynómom

$$C(X) = 0x03X^3 + 0x01X^2 + 0x01X + 0x02 \tag{2}$$

čo je možné reprezentovať maticovým zápisom

$$\begin{bmatrix} B_{0j} \\ B_{1j} \\ B_{2j} \\ B_{3j} \end{bmatrix} = \begin{bmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{bmatrix} \begin{bmatrix} A_{0j} \\ A_{1j} \\ A_{2j} \\ A_{3j} \end{bmatrix} \tag{3}$$

Prvky $A \in GF(2^8)$ je možné reprezentovať viacerými spôsobmi. Jednou z možností je reprezentácia pomocou polynómov. 256 prvkov $GF(2^8)$ je možné reprezentovať v jednom bajte. Nech prvky $A, B \in GF(2^8)$ sú reprezentované v tvare

$$\mathbf{a} = (a_7, a_6, ..., a_0) \qquad A \leftrightarrow a(X) = \sum_{i=0}^{7} a_i X^i \qquad (4)$$

$$\mathbf{b} = (b_7, b_6, ..., b_0), \qquad B \leftrightarrow b(X) = \sum_{i=0}^{7} b_i X^i \qquad (5)$$

Násobenie v $GF(2^8)$ je definované zložitejším predpisom. Pre polynomiálnu reprezentáciu (4),(5) je násobenie realizované, ako násobenie polynómov *a(X)* a *b(X)* modulo ireducibilný polynóm stupňa 8. Ireducibilný polynóm stupňa 8 nad telesom GF(2)(t.j. má len koeficienty 0 a 1) označený, ako *m(X)* a je definovaný v tvare

$$\mathbf{m}=(1, 0, 0, 0, 1, 1, 0, 1, 1), \quad m(X)=X^8+X^4+X^3+X+1 \qquad (6)$$

Násobenie dvoch prvkov $A, B \in GF(2^8)$ je definované takto:

$$A. \bullet B \leftrightarrow (\mathbf{a} \bullet \mathbf{b})_{GF(2^8)} = a(X)b(X) mod m(X) \qquad (7)$$

Riešenie(1a):

Ukážeme príklad výpočtu násobenia dvoch prvkov v $GF(2^8)$ $0x57 \bullet 0x83 = ?$, pomocou vzťahov (4) až (7). Pričom zápis 0x... znamená hexadecimálny zápis bajtu.

$$(57)_{16} = (87)_{10} = (1010111)_2 \qquad (83)_{16} = (131)_{10} = (10000011)$$

$$\mathbf{a} = (1,0,1,0,1,1,1) \qquad A \leftrightarrow a(X) = \sum_{i=0}^{7} a_i X^i = X^6 + X^4 + X^2 + X + 1$$

$$\mathbf{b} = (1,0,0,0,0,0,1,1) \qquad B \leftrightarrow b(X) = \sum_{i=0}^{7} b_i X^i = X^7 + X + 1$$

$$a(X)b(X) = (X^6 + X^4 + X^2 + X + 1)(X^7 + X + 1) = X^{13} + X^7 + X^6 + X^{11} + X^5 + X^4 + X^9 + X^3 +$$
$$X^2 + X^8 + X^2 + X + X^7 + X + 1 = X^{13} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^4 + X^3 + 1$$

$$(X^{13} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^4 + X^3 + 1) \div (X^8 + X^4 + X^3 + X + 1) = X^5 + X^3 + \frac{X^7 + X^6 + 1}{X^8 + X^4 + X^3 + X + 1}$$

$$\underline{\oplus (X^{13} + X^9 + X^8 + X^6 + X^5)}$$

$$X^{11} + X^4 + X^3 + 1$$

$$\underline{\oplus (X^{11} + X^7 + X^6 + X^4 + X^3)}$$

$$X^7 + X^6 + 1$$

$$A. \bullet B \leftrightarrow (\mathbf{a} \bullet \mathbf{b})_{GF(2^8)} = a(X)b(X) mod m(X) =$$
$$= (X^{13} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^4 + X^3 + 1) modulo (X^8 + X^4 + X^3 + X + 1) =$$
$$= X^7 + X^6 + 1$$

Výslednému polynómu prislúcha $(11000001)_2 = (193)_{10} = (C1)_{16}$. Výsledkom násobenia dvoch prvkov z $GF(2^8)$ je teda $0x57 \bullet 0x83 = 0xC1$.

Je zrejmé, že počítanie súčinu $GF(2^8)$ pomocou vzťahu (7) je relatívne komplikované a napr. pre softvérovú realizáciu neefektívne. Pre tento prípad sa využíva postup, ktorý umožňuje pomocou dvoch tabuliek realizovať násobenie v $GF(2^8)$ veľmi jednoduchým spôsobom. Využívajú sa dve tabuľky: logaritmická tabuľka Logtable[256]
antilogaritmická tabuľka Alogtable[256]

```
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
};
```

Pre násobenie v GF(2^8) sa využíva nasledujúci kód v jazyku C:

```
word mul(word8 a, word8 b)
{
      if(a && b)
            return Alogtable[(Logtable[a]+Logtable[b])%255];
      else
            return 0;
}
```

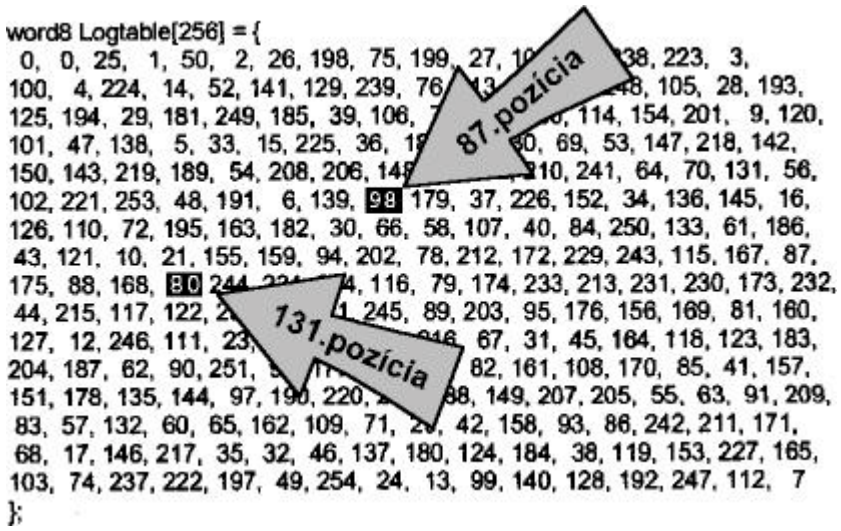
Ako vidieť zo zápisu, využíva sa tu fakt, že $\log(a \bullet b) = \log a + \log b$. Postup pri výpočte násobenia dvoch prvkov v GF(2^8), pomocou týchto tabuliek je veľmi jednoduchý.

V prvej tabuľke(Logtable) nájdeme na rovnakej pozícii, ako je hodnota nášho prvku hodnotu. Rovnakým spôsobom nájdeme aj hodnotu pre druhý prvok, ktorý násobíme. Nesmieme zabudnúť na to, že v jazyku C sa prvky v tabuľke rátajú od 0 (teda 0 až 255)keďže ide o 256 prvkovú tabuľku, zľava doprava po riadkoch. Tieto dve hodnoty spočítame a aplikujeme operáciu modulo255. Výsledná hodnota potom predstavuje pozíciu v druhej tabuľke(Alogtable), na ktorej sa nachádza už výsledná hodnota násobenia.

Tento postup teraz overíme na predošlom príklade $0x57 \bullet 0x83 = 0xC1$.

$(57)_{16} = (87)_{10} = (1010111)_2$ $(83)_{16} = (131)_{10} = (10000011)$

Nájdeme teda v prvej tabuľke(Logtable) hodnoty, ktoré sú na pozíciách 87 a 131.



Na týchto pozíciách sa nachádzajú hodnoty 98 a 80. Teda súčet je 178. Na 178.pozícii budeme v druhej tabuľke (Alogtable) hľadať, výsledok nášho počítania(násobenia).

```
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, 61,171, 76,212,192, 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
};
```

178.pozícia

Ako vidieť v druhej tabuľke(Alogtable) na 178 pozícii sa nachádza prvok 193, čo súhlasí s výsledkom pomocou numerického rátania $0x57 \bullet 0x83 = 0xC1 = (193)_{10}$.

Riešenie(1b):

Ukážeme príklad výpočtu násobenia dvoch prvkov v $GF(2^8)$ $55 \bullet 78 = ?$, pomocou vzťahov (4) až (7). Budeme postupovať rovnakým spôsobom, ako v predošlom riešení.

$$(55)_{10} = (110111)_2 \qquad (78)_{10} = (1001110)$$

$$\mathbf{a} = (1,1,0,1,1,1) \qquad A \leftrightarrow a(X) = \sum_{i=0}^{7} a_i X^i = X^5 + X^4 + X^2 + X + 1$$

$$\mathbf{b} = (1,0,0,1,1,1,0) \qquad B \leftrightarrow b(X) = \sum_{i=0}^{7} b_i X^i = X^6 + X^3 + X^2 + X$$

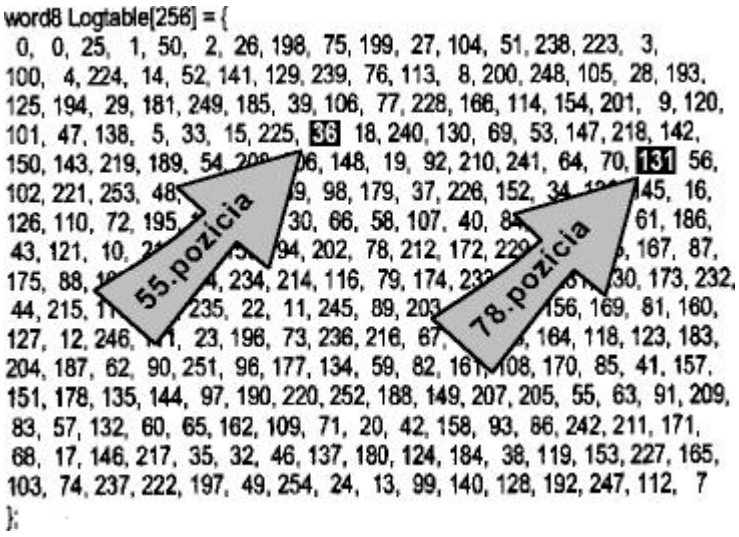
$$A. \bullet B \leftrightarrow (\mathbf{a} \bullet \mathbf{b})_{GF(2^8)} = a(X)b(X) mod m(X) =$$

$$= (X^{11} + X^{10} + X^7 + X^6 + X^3 + X) modulo (X^8 + X^4 + X^3 + X + 1) =$$

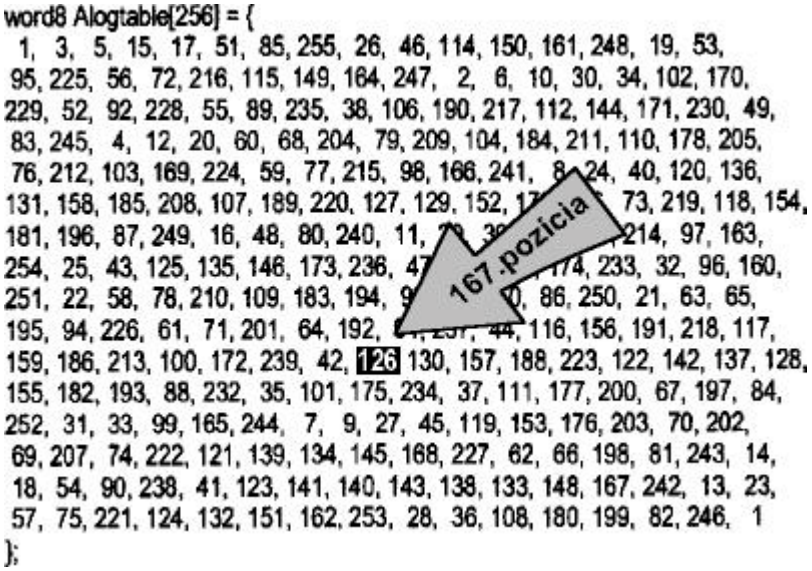
$$= X^6 + X^5 + X^4 + X^3 + X^2 + X$$

Výslednému polynómu prislúcha $(1111110)_2 = (126)_{10}$. Výsledkom násobenia dvoch prvkov z $GF(2^8)$ je teda $55 \bullet 78 = 126$.

Overíme správnosť riešenia pomocou tabuliek. Nájdeme v prvej tabuľke hodnoty na pozíciách 55 a 78.



Na týchto pozíciách sa nachádzajú hodnoty 36 a 131. Teda súčet je 167. Na 167. pozícii budeme v druhej tabuľke (Alogtable) hľadať, výsledok nášho počítania(násobenia).



Ako vidieť v druhej tabuľke(Alogtable) na 167 pozícii sa nachádza prvok 126, čo súhlasí s výsledkom pomocou numerického rátania $55 \bullet 78 = 126$.

Riešenie(1c):

Ukážeme príklad výpočtu násobenia dvoch prvkov v GF(2^8) $232 \bullet 111 = ?$, pomocou vzťahov (4) až (7). Budeme postupovať rovnakým spôsobom, ako v predošlom riešení.

$$(232)_{10} = (11101000)_2 \qquad (111)_{10} = (1101111)$$

$$\mathbf{a} = (1,1,1,0,1,0,0,0) \qquad A \leftrightarrow a(X) = \sum_{i=0}^{7} a_i X^i = X^7 + X^6 + X^5 + X^3$$

$$\mathbf{b} = (1,1,0,1,1,1,1)$$

$$B \leftrightarrow b(X) = \sum_{i=0}^{7} b_i X^i = X^6 + A \leftrightarrow a(X) = \sum_{i=0}^{7} a_i X^i = X^6 + X^5 + X^3 + +X^2 + X + 1$$

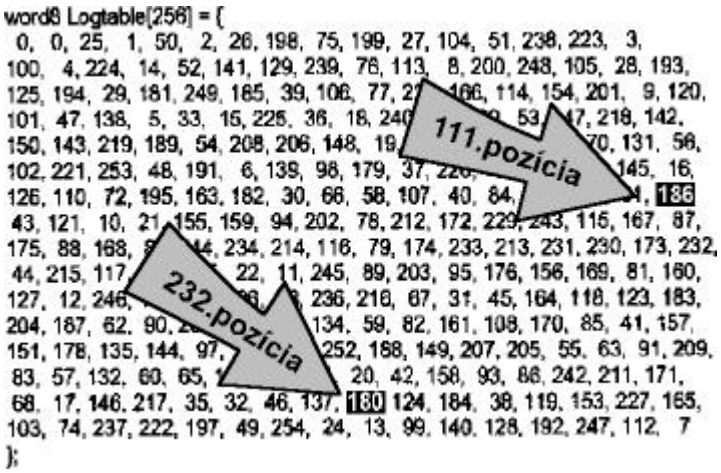
$$A. \bullet B \leftrightarrow (\mathbf{a} \bullet \mathbf{b})_{GF(2^8)} = a(X)b(X) mod m(X) =$$

$$= (X^{13} + X^9 + X^7 + X^6 + X^4 + X^3) modulo (X^8 + X^4 + X^3 + X + 1) =$$

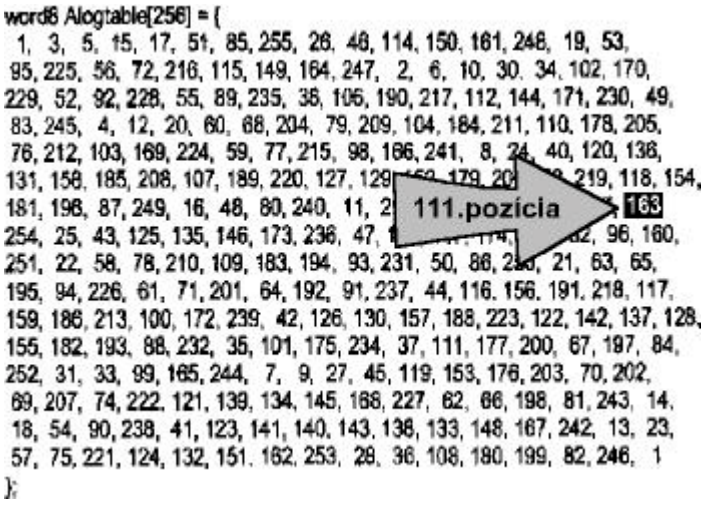
$$= X^7 + X^5 + X + 1$$

Výslednému polynómu prislúcha $(10100011)_2 = (163)_{10}$. Výsledkom násobenia dvoch prvkov z GF(2^8) je teda $232 \bullet 111 = 163$.

Overíme správnosť riešenia pomocou tabuliek. Nájdeme v prvej tabuľke hodnoty na pozíciách 232 a 111.



Na týchto pozíciách sa nachádzajú hodnoty 186 a 180. Teda súčet je 366. Súčet je väčší ako 255, teda aplikujeme modulo operáciu a získame hodnotu 366mod255=111.Na 111. pozícii budeme v druhej tabuľke (Alogtable) hľadať, výsledok nášho počítania(násobenia).



Ako vidieť v druhej tabuľke(Alogtable) na 111 pozícii sa nachádza prvok 163, čo súhlasí s výsledkom pomocou numerického rátania $232 \bullet 111 = 163$.

Riešenie(2):

Našou úlohou bolo, pretransformovanie logaritmickej tabuľky do hexadecimálneho kódu. Po pretransformovaní vyzerá tabuľka nasledovne:

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