***Fakulta Elektrotechniky a Informatiky***
***technickej univerzity v Košiciach***

# *Aplikovaná Kryptografia*

**Dátum: 9.5.2001**
**Ročník:4.B-ETT**
**Vypracovali: Erik Szopka**
**Miroslav Tančibok**

# Substitúcia bytov matice – Stav

***Úloha:***

**Majme Galoisove pole GF($2^8$). Našou úlohou je vybrať prvok a z tohto poľa, ktorý je súčasne prvkom matice stavu a pomocu S –boxu substituovať tento prvok prvkom y. Prvok b tiež patrí do Galoisovho poľa GF($2^8$).**

***Postup:***

**K prvku a nájdeme inverzný prvok b, čiže má platiť a*b = 1. Využívame operácie násobenia a sčítania definované v Galoisovom poli GF($2^8$).**

1. **Vyberieme si ľubovoľný prvok a patriaci do Galoisovho poľa GF($2^8$).**
2. **Prvok reprezentujeme ako polynóm a(x).**
3. **Z logaritmickej tabuľky určíme exponent e, ktorý prináleží práve prvku a.**
4. **Zo vzťahu d = 255 – e získame exponet, ktorý v inverznej logaritmickej tabuľke určuje inverzný prvok b.**
5. **Prvok b opäť reprezentujeme ako polynóm b(x).**
6. $\bar{y} = P * \bar{b} + R$

**, kde**

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$R = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

## *1. Príklad*

1. **a = 3**
2. **a(x) = x + 1**
3. **e = 1**
4. **d = 255 – 1 = 254 a potom b = 246**
5. **b(x) = $x^7 + x^6 + x^{5+} x^4 + x^2 + x$**

**Skúška: a(x) * b(x) mod m(x) = 1, kde m(x) = $x^8 + x^4 + x^3 + x + 1$ je ireducibilný polynóm.**

**(x + 1) * ($x^7 + x^6 + x^{5+} x^4 + x^2 + x$) mod ($x^8 + x^4 + x^3 + x + 1$) = $x^8 + x^4 + x^3 + x$ mod ($x^8 + x^4 + x^3 + x + 1$) =1**

**6.**

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

**y = 123.**

## *2. Príklad*

1. **a = 15**
2. **$a(x) = x^3 + x^2 + x + 1$**
3. **e = 3**
4. **d = 255 – 3 = 252 a potom b = 199**
5. **$b(x) = x^7 + x^6 + x^2 + x + 1$**

**Skúška: $a(x) * b(x) \bmod m(x) = 1$, kde $m(x) = x^8 + x^4 + x^3 + x + 1$ je ireducibilný polynóm.**

**$(x^3 + x^2 + x + 1) * (x^7 + x^6 + x^2 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = x^{10} + x^6 + x^5 + x^3 + x^2 + 1 \bmod (x^8 + x^4 + x^3 + x + 1) = 1$**

**6.**

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

**y = 119.**

## *3. Príklad*

1. **a = 79**
2. **$a(x) = x^6 + x^3 + x^2 + x + 1$**
3. **e = 56**
4. **d = 255 – 56 = 199 a potom b = 9**
5. **$b(x) = x^3 + 1$**

**Skúška: $a(x) * b(x) \bmod m(x) = 1$, kde $m(x) = x^8 + x^4 + x^3 + x + 1$ je ireducibilný polynóm.**

**$(x^6 + x^3 + x^2 + x + 1) * (x^3 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = x^9 + x^5 + x^4 + x^2 + x + 1 \bmod (x^8 + x^4 + x^3 + x + 1) = 1$**

**6.**

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

**y = 132.**

## *4. Príklad*

1. **a = 255**
2. **$a(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$**
3. **e = 7**
4. **d = 255 – 7 = 248 a potom b = 28**
5. **$b(x) = x^4 + x^3 + x^2$**

**Skúška: $a(x) * b(x) \bmod m(x) = 1$, kde $m(x) = x^8 + x^4 + x^3 + x + 1$ je ireducibilný polynóm.**

**$(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) * (x^4 + x^3 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 \bmod (x^8 + x^4 + x^3 + x + 1) = 1$**

**6.**

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

**y = 22.**