



Hillovská šifra.

Stanislav Palúch

Fakula riadenia a informatiky, Žilinská univerzita

11. októbra 2010

Majme priamy text v q -znakovej abecede $A = \{a_0, a_1, \dots, a_{q-1}\}$.

Prvky abecedy A stotožníme s prvkami okruhu \mathbb{Z}_q .

Na abecede A tak máme operácie \oplus a \otimes .

Ak je q prvočíslo, je \mathbb{Z}_q poľom a ku každému $a \in A$ $a \neq 0$ existuje $a^{-1} \in A$ také, že $a \otimes a^{-1} = 1$.


Ak q nie je prvočíslo, potom inverzné prvky existujú len k tým znakom, ktoré nie sú súdeliteľné s q .

Preferujeme teda q prvočíslo.

Existujú konečné telesá s $q = p^n$ prvkami, kde p je prvočíslo.

Sú to tzv. Galoisove polia, značia sa $GF(p^n)$.

Na abecedách, ktoré nemajú prvočíselný počet prvkov alebo počet prvkov rovnajúci sa prirodzenej mocnine prvočísla, nemožno zaviesť operácie \oplus a \otimes tak, aby štruktúra (A, \oplus, \otimes) bola poľom.



Hillovská šifra je polyalfabetická šifra šifrujúca naraz celý blok priameho textu dĺžky n .

$$\underbrace{x_{11}x_{12} \dots x_{1n}}_{x_1} \underbrace{x_{21}x_{22} \dots x_{2n}}_{x_2} \dots \dots \dots \underbrace{x_{m1}x_{m2} \dots x_{mn}}_{x_m} \quad (1)$$

Kľúčom je štvorcová matica typu $n \times n$ taká že k nej existuje inverzná matica \mathbf{K}^{-1} .

$$\mathbf{K} = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{pmatrix} \quad (2)$$

$$\mathbf{y} = \mathbf{Kx} \quad \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} \quad (3)$$

$$y_1 = k_{11}x_1 + k_{12}x_2 + \dots + k_{1n}x_n$$

$$y_2 = k_{21}x_1 + k_{22}x_2 + \dots + k_{2n}x_n$$

...

$$y_n = k_{n1}x_1 + k_{n2}x_2 + \dots + k_{nn}x_n$$




Dešifrovanie

$$\mathbf{x} = \mathbf{K}^{-1}\mathbf{y}$$

Dešifrovanie je korektné, lebo

$$\mathbf{K}^{-1}\mathbf{y} = \mathbf{K}^{-1} \cdot (\mathbf{K} \cdot \mathbf{x}) = (\mathbf{K}^{-1} \cdot \mathbf{K}) \cdot \mathbf{x} = \mathbf{I} \cdot \mathbf{x} = \mathbf{x} \quad (4)$$



Príklad: Abeceda


A, B, C, D, E, F, G, H, I, J, K, L, M, N,

O, P, Q, R, S, T, U, V, W, X, Y, Z} $\equiv \mathbb{Z}_{26}$.

VSTUPNA MATICA

$$\mathbf{K} = \begin{pmatrix} 17 & 4 & 3 & 9 \\ 1 & 13 & 21 & 16 \\ 10 & 12 & 5 & 9 \\ 13 & 6 & 3 & 12 \end{pmatrix}$$

Či je regulárna, zistíme tak, že v niektorom tabuľkovom procesore vypočítame jej determinant. Tu je $\det \mathbf{K} = -11305$ a $\text{mod } (-11305, 26) = 5$ je číslo, ku ktorému existuje v \mathbb{Z}_{26} inverzný prvok – totiž 21.

- 
- Výpočet inverznej matice. Ekvivalentnými úpravami matíc upravíme maticu $(\mathbf{K}|\mathbf{I})$, kde \mathbf{I} je jednotková štvorcová matica, na tvar $(\mathbf{I}|\mathbf{K}^{-1})$.

$$\left(\begin{array}{cccc|cccc} 17 & 4 & 3 & 9 & 1 & 0 & 0 & 0 \\ 1 & 13 & 21 & 16 & 0 & 1 & 0 & 0 \\ 10 & 12 & 5 & 9 & 0 & 0 & 1 & 0 \\ 13 & 6 & 3 & 12 & 0 & 0 & 0 & 0 \end{array} \right)$$


$$\left(\begin{array}{cccc|cccc} 17 & 4 & 3 & 9 & 1 & 0 & 0 & 0 \\ 0 & 25 & 4 & 17 & 3 & 1 & 0 & 0 \\ 0 & 2 & 17 & 19 & 4 & 0 & 1 & 0 \\ 0 & 6 & 16 & 25 & 13 & 0 & 0 & 1 \end{array} \right)$$



$$\left(\begin{array}{cccc|cccc} 17 & 4 & 3 & 9 & 1 & 0 & 0 & 0 \\ 0 & 25 & 4 & 17 & 3 & 1 & 0 & 0 \\ 0 & 0 & 25 & 1 & 10 & 2 & 1 & 0 \\ 0 & 0 & 14 & 23 & 5 & 6 & 0 & 1 \end{array} \right)$$

$$\left(\begin{array}{cccc|cccc} 17 & 4 & 3 & 9 & 1 & 0 & 0 & 0 \\ 0 & 25 & 4 & 17 & 3 & 1 & 0 & 0 \\ 0 & 0 & 25 & 1 & 10 & 2 & 1 & 0 \\ 0 & 0 & 0 & 11 & 15 & 8 & 14 & 1 \end{array} \right)$$

Teraz máme maticu upravenú na hornú diagonálnu.
Teraz treba ešte dosiahnuť nuly nad diagonálou.



$$\left(\begin{array}{cccc|cccc} 17 & 4 & 3 & 0 & 10 & 10 & 24 & 11 \\ 0 & 25 & 4 & 0 & 20 & 17 & 2 & 15 \\ 0 & 0 & 25 & 0 & 11 & 6 & 21 & 7 \\ 0 & 0 & 0 & 11 & 15 & 8 & 14 & 1 \end{array} \right)$$

$$\left(\begin{array}{cccc|cccc} 17 & 4 & 0 & 0 & 17 & 2 & 9 & 6 \\ 0 & 25 & 0 & 0 & 12 & 15 & 8 & 17 \\ 0 & 0 & 25 & 0 & 11 & 6 & 21 & 7 \\ 0 & 0 & 0 & 11 & 15 & 8 & 14 & 1 \end{array} \right)$$

$$\left(\begin{array}{cccc|cccc} 17 & 0 & 0 & 0 & 13 & 10 & 15 & 22 \\ 0 & 25 & 0 & 0 & 12 & 15 & 8 & 17 \\ 0 & 0 & 25 & 0 & 11 & 6 & 21 & 7 \\ 0 & 0 & 0 & 11 & 15 & 8 & 14 & 1 \end{array} \right)$$




Pretože $17^{-1} = 23 \pmod{26}$, $25^{-1} = 25 \pmod{26}$, $11^{-1} = 19 \pmod{26}$, vynásobením prvého riadku matice číslom 23 druhého a tretieho číslom 25 a posledného číslom 19 (všetko modulo 26) dosiahneme:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 13 & 22 & 7 & 12 \\ 0 & 1 & 0 & 0 & 14 & 11 & 18 & 9 \\ 0 & 0 & 1 & 0 & 15 & 20 & 5 & 19 \\ 0 & 0 & 0 & 1 & 25 & 22 & 6 & 19 \end{array} \right)$$

Máme teda:

$$\mathbf{K}^{-1} = \begin{pmatrix} 13 & 22 & 7 & 12 \\ 14 & 11 & 18 & 9 \\ 15 & 20 & 5 & 19 \\ 25 & 22 & 6 & 19 \end{pmatrix}$$




$$\mathbf{K} \cdot \mathbf{x} = \begin{pmatrix} 17 & 4 & 3 & 9 \\ 1 & 13 & 21 & 16 \\ 10 & 12 & 5 & 9 \\ 13 & 6 & 3 & 12 \end{pmatrix} \begin{pmatrix} A \equiv 0 \\ B \equiv 1 \\ C \equiv 2 \\ D \equiv 3 \end{pmatrix} = \begin{pmatrix} L \equiv 11 \\ Z \equiv 25 \\ X \equiv 23 \\ W \equiv 22 \end{pmatrix}$$

$$\mathbf{K}^{-1} \cdot \mathbf{y} = \begin{pmatrix} 13 & 22 & 7 & 12 \\ 14 & 11 & 18 & 9 \\ 15 & 20 & 5 & 19 \\ 25 & 22 & 6 & 19 \end{pmatrix} \begin{pmatrix} L \equiv 11 \\ Z \equiv 25 \\ X \equiv 23 \\ W \equiv 22 \end{pmatrix} = \begin{pmatrix} A \equiv 0 \\ B \equiv 1 \\ C \equiv 2 \\ D \equiv 3 \end{pmatrix}$$

Ukážka toho, že zmena jedného znaku v bloku priameho textu má za následok (vo väčšine prípadov) zmenu všetkých znakov v zašifrovanom texte.

$$\mathbf{K} \cdot \mathbf{x}' = \begin{pmatrix} 17 & 4 & 3 & 9 \\ 1 & 13 & 21 & 16 \\ 10 & 12 & 5 & 9 \\ 13 & 6 & 3 & 12 \end{pmatrix} \begin{pmatrix} P \equiv 15 \\ B \equiv 1 \\ C \equiv 2 \\ D \equiv 3 \end{pmatrix} = \begin{pmatrix} G \equiv 6 \\ O \equiv 14 \\ R \equiv 17 \\ J \equiv 9 \end{pmatrix}$$



Known plaintext attack proti hillovskej šifre. Predpokladajme, že poznáme n dvojíc priameho textu a príslušného textu.

$$\mathbf{y}_1 = \mathbf{K}\mathbf{x}_1, \mathbf{y}_2 = \mathbf{K}\mathbf{x}_2, \dots, \mathbf{y}_n = \mathbf{K}\mathbf{x}_n \quad (5)$$

Zostrojme štvorcové matice typu $n \times n$ \mathbf{X} , \mathbf{Y} , ktorých stĺpce budú tvorené stĺpcovými vektormi $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$, resp. $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_n$, t.j.:

$$\mathbf{X} = (\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n), \quad \mathbf{Y} = (\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_n).$$

Potom vzťahy (5) možno zapísať v maticovom tvare

$$\mathbf{Y} = \mathbf{K}\mathbf{X} \quad (6)$$

Vynásobením rovnice (6) maticou \mathbf{X}^{-1} z prava (za predpokladu, že \mathbf{X}^{-1} existuje) dostávame:

$$\mathbf{Y}\mathbf{X}^{-1} = (\mathbf{K}\mathbf{X})\mathbf{X}^{-1} = \mathbf{K}(\mathbf{X}\mathbf{X}^{-1}) = \mathbf{K}\mathbf{I} = \mathbf{K}$$