Povzetek

Sticklov algoritem spada med kriptografske algoritme. Kriptografija je veda, ki tekstovno sporočilo pretvori v kombinacijo števk, ki je za malega človeka nerazumljiva. Kombinacija števk je zaščitena z javnim in zasebnim ključem. Kriptografi želijo svoje skrivnosti obdržati skrite pred dekriptorji. Naloga in cilj dekriptorjev je čimprejšnje razvozlanje tajnega sporočila. Za nosilni steber modernega šifriranja velja algoritem RSA.

Tropska matematika je množica $\mathbb{R} \cup \{\varepsilon\}, \varepsilon = \infty$. Na množici definiramo operaciji seštevanja $\oplus$ in množenja $\otimes$ s predpisoma: $a \oplus b \equiv \min(a, b)$ in $a \otimes b \equiv a + b$. Je algebrska struktura, ki jo imenujemo polkolobar. Polkolobarje odlikujejo različne lastnosti in zakoni seštevanja in množenja. Lastnosti in zakoni so predstavljeni z matematičnimi objekti iz linearne algebre. V diplomski nalogi bomo podrobneje predstavili matrike. Spoznali bomo lastnosti in zakone v običajni linearni algebri in v tropski matematiki.

Math. Subj. Class. (2010): 16Y60, 12K10, 11T71.

Ključne besede: matrike, linearna algebra, tropska matematika, polkolobar, tropski polkolobar, kodiranje, permutacije, algoritem RSA, Sticklov algoritem

Abstract

Stickel's protocol is one of the cryptographic algorithms. Cryptography is the study of techniques which convert text messages into a combinations of digits, which are incomprehensible to the common man. The combination of digits protects private and public keys. Cryptographers want to keep their secrets hidden from the decrypters. The decrypters goal is to reveal the secret messages as fast as they can. The base of modern encryption is the algorithm RSA.

Tropical mathematics is a set of $\mathbb{R} \cup \{\varepsilon\}\, \varepsilon = \infty$. On the set of defined two operations of aggregation of addition $\oplus$ and multiplication $\otimes$ with regulations: a $\oplus b \equiv \min(a, b)$ and $a \otimes b \equiv a + b$. It is the algebraic structure called semiring. Semirings are distinguished by different characteristics and laws of addition and multiplication. Properties and laws are presented by mathematical objects from linear algebra. In this thesis we will present matrices. We will learn about the characteristics and laws in normal linear algebra and tropical mathematics.

Keywords: matrices, linear algebra, tropical algebra, semiring, tropical semiring, cryptography, permutation, algorithm RSA, Stickel's protocol

9 LITERATURA IN SPLETNI VIRI

Literatura

[1] D. Grigoriev, V. Shpilrain, "*Tropical cryptography*", Comm. Algebra 42 (2014), no. 6, 2624 (2014).

[2] S. Singh, "*Knjiga šifer: umetnost šifriranja od starega Egipta do kvantne kriptografije*", (Učila International, Tržič, 2006).

[3] J. Grasselli, "*Elementarna teorija števil*", (DMFA, Ljubljana, 2009), str. 1-43.

[4] K. G. Farlow, "*Max Plus Algebra*", 25. 3. 2016, https://theses.lib.vt.edu/theses/available/etd-05042009-152934/unrestricted/Finalthesis.pdf.

[5] "*Tropical cryptography*", 5. 4. 2016 https://www.yumpu.com/en/document/view/3086918/tropical-mathematics.

[6] "*Introdruction to tropical mathematics*", 30. 3. 2016 https://www.yumpu.com/en/document/view/19029486/introduction-to-tropical-mathematics-fullerton-college-staff-web-.

[7] D. Dolžan, P. Oblak, "*Invertible and nilpotent matrices over antirings, Linear Algebra and its Applications*", (2009), 430, str. 271-278, 20. 5. 2016 http://www.sciencedirect.com/science/article/pii/S002437950800356X.

[8] "*Matrike*", 25. 3. 2016 http://www.fmf.uni-lj.si/ kosir/poucevanje/skripta/matrike.pdf

[9] "*Kriptografija*", 10. 2. 2016 https://sl.wikipedia.org/wiki/Kriptografija.

[10] "*Algoritem RSA* ", 10. 2. 2016
http://fizika.zf42.net/razno/rsa.

[11] "*Permutacija*", 30. 3. 2016
https://sl.wikipedia.org/wiki/Permutacija.

[12] "*Permutacije*", 30. 3. 2016
http://www.presek.si/16/930-Klavzar.pdf.

[13] "*Algebraične strukture*", 4. 4. 2016
http://www.fmf.uni-lj.si/ kosir/poucevanje/skripta/strukture.pdf.

[14] V. Shpilrain, "*Cryptanalisis of Stickel's key exchange scheme*",
Computer Science in Russia 2008, Lecture Notes Comp. Sc. 5010, 283 (2008).

[15] E. Stickel, "*A New Method for Exchanging Secret Keys*",
Proc. of the Third International Conference on Information Technology and Applications (ICITA05) 2, 426 (2005).

[16] C. Mullan, "*Cryptanalysing variants of Stickel's key agreement scheme*", *preprint.*

[17] P. Butkovic, "*Max-linear systems: theory and algorithms*",
Springer-Verlag London, (2010).

[18] "*Bijektivna preslikava*", 20. 6. 2016
https://sl.wikipedia.org/wiki/Bijektivna_preslikava.