Zoznam publikačnej činnosti
Autor: Antal, Eugen
Zobrazovací formát: Zoznam dokumentov podľa ISO690
Štatistika: Kategória publikačnej činnosti

Skupina B - **Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS**

ANTAL, Eugen [50 %] - ZAJAC, Pavol [50 %]. Key Space and Period of Fialka M-125 Cipher Machine. In *Cryptologia*. Vol. 39, No. 2 (2015), s. 126-144. ISSN 0161-1194. V databáze: WOS: 000353113100003 ; SCOPUS.

ANTAL, Eugen - GROŠEK, Otokar - HORAK, Peter. On a Mnemonic Construction of Permutations. In *Journal of Mathematical Cryptology.* Prijaté 25.01.2017. V databáze: SCOPUS.

Skupina B - Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS

ANTAL, Eugen [50 %] - HROMADA, Viliam [50 %]. A New Stream Cipher Based on Fialka M-125. In *Tatra Mountains Mathematical Publications*. Vol. 57, Iss. 4 (2013), s.101-118. ISSN 1210-3195. V databáze: SCOPUS.

ANTAL, Eugen [50 %] - HROMADA, Viliam [50 %]. A micro-controller implementation of a FIALKA M-125 based stream cipher. In *Tatra Mountains Mathematical Publications*. Vol. 60, (2014), Issue: 1, s. 101-116. ISSN 1210-3195. V databáze: SCOPUS.

Ostatné publikácie

ANTAL, Eugen [50 %] - VARGA, Juraj [50 %]. Zodiac. In *Mikulášská kryptobesídka 2010 : Sborník příspěvků. Praha, 2.-3.12.2010*. Praha : Trusted Network Solutions, 2010, s.89-90. ISBN 978-80-904257-1-2.

ANTAL, Eugen [100 %]. Fialka M-125. In *Mikulášská kryptobesídka 2010 : Sborník příspěvků. Praha, 2.-3.12.2010*. Praha : Trusted Network Solutions, 2010, , s.87-88. ISBN 978-80-904257-1-2.

ANTAL, Eugen [100 %]. Nature-inspired heuristic methods in classical cipher cryptanalysis. In *Norwegian-slovakian workshop in crypto : Bergen, Norway. February 8 - 10, 2016*. 1. ed. Bratislava : Slovak University of Technology, 2016, S. 25-33. ISBN 978-80-227-4541-3.

ANTAL, Eugen - GROŠEK, Otokar. Fialka M-125. In *ŠVOČ 2009 : Študentská vedecká a odborná činnosť. Zborník víťazných prác. Bratislava, Slovak Republic, 29.4.2009*. Bratislava : STU v Bratislave FEI, 2009, s.CD-Rom. ISBN 978-80-227-3094-5.

ANTAL, Eugen [100 %]. Computer Processing of the Rohonczi Codex. In *ELITECH´12 [elektronický zdroj] : 14th Conference of Doctoral Students. Bratislava, Slovak Republic, 22 May 2012*. Bratislava : Nakladatel'stvo STU, 2012, s.CD-ROM, [5] s. ISBN 978-80-227-3705-0.

ANTAL, Eugen [40 %] - SÝS, Marek [20 %] - VARGA, Juraj [40 %]. Evaluation Functions in the Cryptoanalysis of Homophonic Substitution. In *ISCAMI 2012 : Book of abstracts. Malenovice, Czech Republic, 10.-13.5.2012*. Ostrava : University of Ostrava, 2012, s.12.

ANTAL, Eugen [50 %] - JÓKAY, Matúš [50 %]. Rotorový šifrátor Fialka M-125. Diel 1. Popis šifrátora. In *Crypto-World*. Roč. 13, č. 4 (2011), s.18-27. ISSN 1801-2140.

ANTAL, Eugen [50 %] - JÓKAY, Matúš [50 %]. Rotorový šifrátor Fialka M-125. Úvod k seriálu. In *Crypto-World*. Roč. 13, č. 4 (2011), s.17. ISSN 1801-2140.

ANTAL, Eugen [70 %] - JÓKAY, Matúš [30 %]. Rotorový šifrátor Fialka M-125. Diel 2. Porovnanie s viacerými rotorovými šifrátormi. In *Crypto-World*. Roč. 13, č. 5 (2011), s.15-23. ISSN 1801-2140.

ANTAL, Eugen [60 %] - JÓKAY, Matúš [40 %]. Rotorový šifrátor Fialka M-125. Diel 4: Implementácia a možnosti využitia. In *Crypto-World*. Roč. 13, č. 9 (2011), s.9-15. ISSN 1801-2140.

ANTAL, Eugen [50 %] - JÓKAY, Matúš [50 %]. Rotorový šifrátor Fialka M-125. Diel 3. Vybrané vlastnosti šifry. In *Crypto-World*. Roč. 13, č. 6 (2011), s.23-32. ISSN 1801-2140.

ANTAL, Eugen [100 %]. Záhada kódexu Rohonczi. In *Crypto-World*. Roč. 14, č. 9-10 (2012), s.21-28. ISSN 1801-2140.

ANTAL, Eugen [50 %] - ZAJAC, Pavol [50 %]. Analýza Rabenhauptovho zašifrovaného dopisu. In *Crypto-World*. Roč. 15, č. 11-12 (2013), s.9-17. ISSN 1801-2140.

ANTAL, Eugen [100 %]. Modern cryptanalysis of classical ciphers. In *CECC 2016 : The 16th central european conference on cryptology. Piestany, Slovakia. June 22 - 24, 2016*. Bratislava : STU, 2016, S. 29-33.

ANTAL, Eugen [80 %] - SÝS, Marek [20 %]. Solving Homophonic Cipher Using Heuristic Methods. In *ISCAMI 2013 : Book of abstracts. Malenovice, Czech Republic, May 2-5, 2013*. Ostrava : University of Ostrava, 2013, s.9.

ANTAL, Eugen [80 %] - SÝS, Marek [20 %]. Nature-inspired heuristic methods in classical cipher cryptanalysis. In *ISCAMI 2014 : book of abstracts. Malenovice, ČR, 27. - 30. 3. 2014*. 1. vyd. Ostrava : Ostravská univerzita, 2014, s. 9.

ANTAL, Eugen [100 %].. Lightweight Cipher Based on FIALKA M-125 Design. In *Central European Conference on Cryptology 2013 : Telč, Czech Republic, June 26-28, 2013*. Brno : Masaryk University, 2013, s.1.

Rôzne publikácie v spoluatorstve so študentmi

ANTAL, Eugen - BARANEC, František. Techniky získavania citlivých údajov z Apple iOS zariadení. In *43. konference EurOpen.CZ : Vranov, Czech Republik; 29. 9.-2.10.2013*. Plzeň : EurOpen.CZ, 2013, s.21-32. ISBN 978-80-86583-26-6.

SOVIČ, Tomáš - ANTAL, Eugen . Comparison of selected rotor ciphers. In *Mikulášská kryptobesídka 2016 : sborník příspěvků. Praha, ČR, 1. - 2. 12. 2016*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2016, S. 41-42. ISBN 978-80-904257-8-1.

BARANEC, František - ANTAL, Eugen. Forenzná analýza iOS. In *ŠVOČ 2013 [elektronický zdroj] : Zborník vybraných prác, Bratislava, 23. apríl 2013*. 1. vyd. Bratislava : FEI STU, 2013, s.CD ROM, s. 19-21. ISBN 978-80-227-3909-2.

JACKULIAK, Daniel - ANTAL, Eugen. Lúštenie vybraných substitučných šifier pomocou SWARM intelligence. In *ŠVOČ 2014 [elektronický zdroj] : Zborník vybraných prác 2014, Bratislava, 29. apríl 2014*. 1.vyd. Bratislava : FEI STU, 2014, CD-ROM, s. 15-20. ISBN 978-80-227-5154-5.

KANIČÁR, Martin - ANTAL, Eugen. Lúštenie homofónnej substitúcie pomocou genetických algoritmov. In *ŠVOČ 2013 [elektronický zdroj] : Zborník vybraných prác, Bratislava, 23. apríl 2013*. 1. vyd. Bratislava : FEI STU, 2013, s.CD ROM, s. 6-9. ISBN 978-80-227-3909-2.

Ohlasy a citácie (bez autocitácií)

Stephen Budiansky v knihe *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union* cituje článok *Key Space and Period of Fialka M-125 Cipher Machine*.

Pavol Zajac v článku *On insecurity of 4-round Feistel ciphers* cituje článok *A New Stream Cipher Based on Fialka M-125*.

NSA's National Cryptologic Museum Library uvádza článok *Key Space and Period of Fialka M-125 Cipher Machine* v katalógu publikácií: “The Museum Library maintains a collection of unclassified and declassified books and documents relating to every aspect of cryptology. The books and records complement the museum exhibits and artifacts, but also offer unique and in-depth sources of information for researchers."

Štatistika: kategória publikačnej činnosti

ADM	Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS	2
ADN	Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS	2
AFC	Publikované príspevky na zahraničných vedeckých konferenciách	3
AFD	Publikované príspevky na domácich vedeckých konferenciách	5
AFG	Abstrakty príspevkov zo zahraničných konferencií	1
BDE	Odborné práce v ostatných zahraničných časopisoch	7
BFA	Abstrakty odborných prác zo zahraničných podujatí (konferencie...)	2
BEE	Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)	2
BEF	Odborné práce v domácich zborníkoch (konferenčných aj nekonferenčných)	1
GII	Rôzne publikácie a dokumenty, ktoré nemožno zaradiť do žiadnej z predchádzajúcich kategórií	1
Súčet		**26**