An implementation of an attack on Dömösi's cryptosystem

Zita Kovács and Andor Pénzes

University of Debrecen, Faculty of Informatics

kovacs.zitu@gmail.com and andor.penzes@gmail.com

In this paper we introduce an implementation of attack on a practical stream cipher based on a finite automata without outputs. For encryption and decryption the apparatus uses the same secret keys, which have the transition matrix of a key-automaton without outputs and with an initial state and final states. This cryptosystem called Dömösi cryptosystem from its maker. First, we introduce the system and its restrictions and we introduce the attack, which is based on probability theory and create equivalent classes. The attack's result an automaton which has equivalent functions to the cryptosystem's key-automaton. To verify our results we developed a computer program which is implementing the attack. This article is about this implementation.

References

[1] Pál Dömösi, A novel stream cipher based on finite automata, *IntelliSec - The 1st International Workshop on Intelligent Security Systems,* 11-14th November 2009, Bucharest, Romania.

[2] Géza Horváth, The φ factoring algorithm (in Hungarian), *Alkalmazott Mat. Lapok*, Vol. 21 (2004), 355-364.

[3] Zoltán Mecsei, Andor Pénzes, A comparison of the DES and 3DES with Dömösi cryptosystems, *Proc. Pali'65, International Conference on Automata, Languages, and Related Topics, Debrecen, submitted for publication.*

[4] J.E. Hopcroft, R. Motwani, J.D.Ullman, Introduction to Automata Theory, Languages, and Computation, *Pearson Education, Addison Wesley*, Second Edition (2001).

[5] Renji Tao, Finite Automata and Application to Cryptography, *Tsinghua University Press*, (2008).

[6] A. J. Menezes, P. C. Oorschot, S. A. Vanstone (1996, 2001, 2008) Handbook of Applied Cryptography, *CRC Press.*

[7] Zita Kovács, Andor Pénzes, Analysis of the security of the Domosi's cryptosystem (in Hungarian), *II. Nyíregyházi Doktorandusz (PHD/DLA) Konferencia*, (2009), 261–265.