An attack on Dömösi's cryptosystem

January 10, 2010

Pál Dömösi
College of Nyíregyháza, Institute of Mathematics and Informatics
H-4400 Nyíregyháza, Sóstói út 31/B, Hungary
e-mail: domosi@nyf.hu
and
Zita Kovács
Debrecen University, Faculty of Informatics
Debrecen, Egyetem tér 1, H-4032, Hungary
e-mail : zita.sapine@nyf.hu
and
Andor Pénzes
Debrecen University, Faculty of Informatics
Debrecen, Egyetem tér 1, H-4032, Hungary
e-mail : andor.penzes@gmail.com

1 Abstract

In this paper we introduce an 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 without its restrictions and we introduce the attack, which is based on probability theorem and create equivalent classes. The result of the attack an automaton which is state-equivalent to the key-automaton of the cryptosystem. Then we show how the restrictions help us against the attack.