Семінар на тему

«Алгебро-автоматний метод і система обміну інформацією»

Автори: Кривий С.Л., Рябов К.С.

Факультет комп'ютерних наук та кібернетики КНУ імені Тараса Шевченка

Анотація. Розглядається метод і симетрична криптографічна система обміну інформацією на основі ізоморфізмів кілець та метод обміну інформацією на основі скінченних автоматів Мілі та операції коректної послідовної композиції таких автоматів. Описуються способи побудови автоматів, їхні властивості та можливість побудови оберненої композиції автоматів. Розглядається взаємозв'язок обох методів і систем та спосіб побудови нової симетричної криптосистеми на основі такого взаємозв'язку. Додатково розглядається задача канонічного кодування довільних текстових і бінарних повідомлень у послідовності лишків відповідного кільця з однозначним відновленням початкових даних для узгодження звичайного подання даних з алгебраїчною областю, у якій виконуються перетворення криптосистеми.

Algebraic-automaton method and information exchange system

Authors: Kryvyi S.L., Ryabov K.S.

Faculty of Computer Science and Cybernetics of Taras Shevchenko National University in Kyiv

Abstract. The method and symmetric cryptographic information exchange system based on ring isomorphisms and the method of information exchange based on finite Mealy automata and the operations of correct sequential composition of such automata are considered. Methods of constructing automata, their properties and the possibility of constructing an inverse composition of automata are described. The relationship of both methods and systems and the method of constructing a new symmetric cryptosystem based on such a relationship are considered. In addition, the problem of canonical encoding of arbitrary text and binary messages as residue sequences in the corresponding ring, with unambiguous recovery of the original data is covered to align the ordinary representation of data with the algebraic domain in which the cryptosystem transformations are performed.