Abstract

Quasigroups Transformations and Their Applications in Cryptography

Vesna Dimitrova

Faculty of the Natural Sciences and Mathematics,
Institute of Informatics, P.O.Box 162
Skopje, Republic of Macedonia

Finite quasigroups theory is used in many applications: cryptography, coding theory, design theory and many more. It was noticed that some quasigroups are suitable for cryptographic purposes. Structures of quasigroups and their properties enable them to be applied in cryptography. Today, quasigroups applications in cryptography rapidly growth.

We define quasigroup transformations using quasigroups. Properties of sequences obtained by quasigroup transformations give possibilities of their applications. In our investigation some of the properties of quasigroups, quasigroup transformations and classification of quasigroups are researched.

We present some applications of quasigroup transformations in cryptography for designing cryptographic primitives, especially for implementation of pseudo random generators.