Review of literature

REVIEW OF LITERATURE

Cryptography deals with the transformation of ordinary text (plain text) into coded from (cipher text) by encryption, and transformation of cipher text into plain text by decryption. One of the most popular current trends in cryptography is the research for new approaches for designing cryptographic primitives. One such approach is to use the algebraic system called "Quasigroup".

The theory of quasigroups ("non associative groups") is one of the oldest branches of algebra and combinatorics. In the guise of Latin squares, it dates back at least to Euler [24]. In 1779 and 1782 Euler published two papers [22] and [23] on pairs of mutually orthogonal Latin squares. Euler's quasigroup operation was considered on a discrete set. The notion of quasigroup was introduced by Suschkewitsch [60]. The term "quasigroup" was first used by Moufang [49], who considered certain quasigroups with a unit. (Later on such quasigroups were named loops.) The first publication on differentiable (and even analytic) quasigroups is the Malcev paper [43].

Belousov, V.D., a Russian Mathematician worked on quasigroups and a large number of papers were published by him. These papers include the following topics [14]:

Transitive and distributive quasigroups, On the structure of distributive quasigroups, Associative systems of quasigroups, On the structure of D-quasigroups, Medial systems of quasigroups, Globally transitive quasigroups, On one class of left-distributive quasigroups, Reciprocally-inverse quasigroups and loops, Some problems on ternary quasigroups, Balanced identities in quasigroups, On Stein's quasigroups, n-ary quasigroups and loops, Quasigroups with the inverse property, Some remarks on TS-quasigroups, Algebraic nets

and quasigroups, Partial identities and nuclei of quasigroups, On infinitary quasigroups, Parastrophic-orthogonal quasigroups, Autotopies and antiautotopies in quasigroups, Crossed isotopies of quasigroups, On the homotopy of inverse n-quasigroups.

In a similar manner, several important contributions to the theory of quasigroups were made by Adrian Petrescu. , Belyavskaya, G.B., Gligoroski, D., Hosszu, M., Kolar-Begović, Z., Kościelny, C., Markovski, S., Shcherbacov, V.A., Smith, D.H., Stojcevska, B., Svein Johan Knapskog., Vedran Krcadinac., Vesna Dimitrova., Volenec, V., Tabarov Abdullo and many others.

The applications of quasigroups in cryptography are increasing rapidly. A few interesting developments in the study of applications of quasigroups in cryptography is detailed below:

1. Quasigroups, Isotopisms and Authentification Schemes, Dawson, E., Donowan, D., (1996) [15].
2. A quasigroup-based public-key cryptosystem, Koscielny, C., Mullen, G.L., (1999) [39].
3. Secure two-way online communication by using quasigroup enciphering with almost public key, Markovski, S., Gligoroski, D. and Stojcevska, B., (2000) [46].
4. Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack, Denes, J., Denes, T., (2001) [17].
5. Using quasigroups for secure encoding of file system, Ochadkova, E., Snasel,V., (2001) [50].
6. Some applications of non-associative algebraic systems in cryptology , Denes, J., Keedwell, A. D., (2002) [19].

7. Secure SMS messaging using Quasigroup encryption and Java SMS API., Hassinen, M., Markovski, S., (2003) [28].
8. Quasigroup string processing and applications in cryptography, Markovski, S., (2003) [44].
9. All-or-nothing transforms using quasigroups, Marnas, S.I., Angelis, L. and Bleris, G.L., (2003) [47].
10. Differential cryptanalysis of the quasigroup cipher, Hassinen, M., Markovski , S., (2004) [29].
11. Quasigroup Transformations and Their Applications, Dimitrova, V., (2005) [20].
12. On application of quasigroups in cryptology, Glukhov, M.M., (2008) [26].
13. On linear and inverse quasigroups and their applications in code theory, Shcherbacov, V.A., (2008) [58].
14. Classification of ternary quasigroups of order 4 applicable in cryptography, Dimitrova, V., Mihajloska, H., (2010) [21].
15. Securing Retinal Template Using Quasigroups, Radha, N., Rubya, T., Karthikeyan, S., (2011) [53].

There is much literature in the study of quasigroups and their applications in cryptography.

In this review of literature a brief survey of some of the articles published on quasigroups, generation of quasigroups, different types of quasigroups and some of their applications in cryptography are given.

1. On Definitions of Groupoids Closely Connected With Quasigroups. Shcherbacov, V.A., (2007) [57]

In this article, both "existential" and "equational" definitions of

binary quasigroups and groupoids closely connected with quasigroups are given. It is proved that a groupoid $(Q, \cdot)$ is a quasigroup if and only if all middle translations of $(Q, \cdot)$ are bijective maps of the set Q.

2. Loops and Quasigroups: Aspects of Current Work and Prospects for the Future.

Jonathan D.H. Smith., (2000) [32]

In this article, a brief survey of certain recently developing aspects of the study of loops and quasigroups are given. It is focused on some of the areas that appear to exhibit the best prospects for subsequent research and for applications both inside and outside mathematics are given.

3. Crossed-Inverse-Property Groupoids.

Izbash,V., Labo, N., (2007) [31]

In this article, the right and left crossed-inverse-property in groupoids are investigated. It is shown that the class of all crossed-inverse-property groupoids is a variety of quasigroups. Some properties of the right-crossed-property groupoids are established.

4. The Plastic Quasigroups.

Krcadinac, V., Volenec, V., (2007) [41]

In this article, Plastic quasigroups are defined. One-to-one correspondence between G_2- quasigroups and Plastic quasigroups are studied. A Toyoda-like representation theorem for plastic quasigroups is proved.

5. Affine Regular Decagons in GS–Quasigroup.

Volenec, V., Kolar-Begovic, Z., (2008) [69]

In this article, the "geometric" concept of the affine regular decagon in a general GS–quasigroup is introduced. The relationships between

affine regular decagon and some other geometric concepts in a general GS–quasigroup are explored. The geometrical presentation of all proved statements is given in the GS–quasigroup $C(\frac{1}{2}(1+\sqrt{5}))$.

6. Linear Quasigroups. I.

Tabarov A.K., (2010) [61]

In this article, linear quasigroups and some of their generalizations are given. In the first part main definitions and notions of the theory of quasigroups are given. In the second part some elementary properties of linear quasigroups and their generalizations are presented. Finally in the third part endomorphisms and endotopies of linear quasigroups and their generalizations are investigated.

7. A Quasigroup – Based Public Key Cryptosystem.

Kościelny, C., Mullen, G.L., (1999) [39]

In this article, a public-key cryptosystem, using generalized quasigroup-based stream ciphers is presented. It is shown that such a cryptosystem allows one to transmit securely both a cryptogram and a secret portion of the enciphering key using the same insecure channel.

8. Secure Two-Way Online Communication By Using Quasigroup Enciphering With Almost Public Key.

Markovski, S., Gligoroski, D. and Stojcevska, B., (2000) [46]

In this article, a stream cipher with almost public key, based on quasigroups for defining suitable encryption and decryption. They consider the security of this method. It is shown that the key (quasigroups) can be public and still having sufficient security. A software implementation is also given.

9. Generating Quasigroups for Cryptographic Applications.

Kościelny, C., (2002) [38]

In this article, a method of generating a practically unlimited number of quasigroups of a (theoretically) arbitrary order using the computer algebra system Maple 7 is presented. This problem is crucial to cryptography and its solution permits to implement practical quasigroup-based endomorphic cryptosystems. The order of a quasigroup usually equals the number of characters of the alphabet used for recording both the plaintext and the cipher text. From the practical viewpoint, the most important quasigroups are of order 256, suitable for a fast software encryption of messages written down in the universal ASCII code. This paper provides fast and easy ways of generating quasigroups of order up to 256 and a little more.

10. Quasigroups Transformations and Their Applications in Cryptography.

Dimitrova, V., (2005) [20]

In this article, quasigroup transformations are defined by using quasigroups. Some of the properties of quasigroups, quasigroup transformations and classification of quasigroups are researched. Some applications of quasigroup transformations in cryptography for designing cryptographic primitives, especially for implementation of pseudo random generators are presented.

11. Applications of Quasigroups in Cryptography.

Adrian Petrescu., (2007) [1]

In this article, a class of very efficient and simple stream ciphers based on 3-quasigroups is studied. Ciphers based on non-associative systems show better possibilities than known ciphers based on associative systems.

12. A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups.

Gligoroski, D., Markovski, S. and Knapskog, S.J., (2008) [25]

In this article, a new class of public key algorithms based on quasigroup string transformations using a specific class of quasigroups called Multivariate Quadratic Quasigroups (MQQ) is designed.

13. Development of Efficient Algorithms for Quasigroup Generation and Encryption.

Pal, S.K., Sumitra, (2009) [52]

In this article, a fast and efficient method of generating a practically unlimited number of quasigroups of an arbitrary order is presented. A lightweight quasigroup based encryption scheme is proposed for providing message confidentiality. The scheme first generates a random quasigroup of order 256 out of the extremely large number of available options. A new method using shift and lookup operations on the quasigroup is then used for encryption / decryption of the data.

14. Block Cipher Based on Randomly Generated Quasigroups.

Deepthi Haridas., Venkataraman, S., Geeta Varadan, (2010) [16]

In this article, the security of the existing block ciphers based quasigroups is enhanced, by introducing a method for construction of huge quasigroups randomly. Quasigroup of large order depends mainly on the cryptographic algorithm and its other memory requirements. This paper defines a block cipher that initially generates two quasigroups of order256, such that neither the entire multiplicative table be stored before the encryption or decryption starts nor the first permutation has to be stored in memory for quasigroup constructions.