Introduction

INTRODUCTION

"Security, like correctness, is not an add-on feature."

- Andrew S. Tanenbaum

The above quote is trying to say that security is not something extra, but it is something essential. That is where cryptography comes along. Cryptography is the practice and study of hiding information. Modern Cryptography intersects the disciplines of Mathematics, Computer Science, and Electrical Engineering. Applications of Cryptography include ATM cards, Computer passwords and Electronic commerce. One of the current trends in Cryptography is to search for new approaches to the Cryptography algorithms design. One such approach is to use the other algebraic structures, such as a quasigroup, rather than the traditional. Quasigroups are algebraic objects which are non-commutative, non-associative, non-idempotent, non- involutory and do not have neutral elements. These properties of quasigroups have been recently found to be useful in many information security applications. In particular quasigroups have been used for ensuring confidentiality and integrity of the data transmitted over insecure public channels. Researchers have focused on quasigroups usage, in the Cryptography more seriously from the beginning of this century.

The main aim of this thesis is to study Quasigroups and Their Applications in Cryptography.

The plan of study is as follows:

- ❖ Definitions and basic properties of quasigroups.
- ❖ Generation of quasigroups.
- ❖ Different types of quasigroups.
- ❖ Applications of quasigroups in cryptography.

It is worth mentioning that the author of this thesis published three articles related to this topic as detailed below:

1. "Generation of Quasigroups - A Review ", Proceedings of Second National Conference on "Recent Advancements in Science and Humanities", United Institute of Technology, Coimbatore, 18th and 19th March 2010. [33]

   *** This article was awarded as the "Best Research Paper".**

2. "Ternary Quasigroups and their Applications in Cryptography - A Review ", Proceedings of National Conference on " Scientific Computing and Applied Mathematics", V.L.B. Janakiammal College of Engineering and Technology, Coimbatore, 29th and 30th June 2010. [34]

3. "Some Interesting Geometric Concepts in GS - Quasigroups - A Review", Proceedings of National Seminar on " Recent Advances in Fuzzy Mathematics and its Applications", Nirmala College for Women, Coimbatore, 5th and 6th July 2010. [35]

The first Chapter deals with Definitions and Basic properties of Quasigroups.

" A quasigroup $(Q, *)$ is a set Q of elements along with a binary operation '$*$' having the following properties:

(a) For all $a, b \in Q$, $a * b \in Q$. (Q is closed under $*$)

(b) For all $a, b \in Q$, there exist unique $x, y \in Q$ so that $a * x = b$ and $y * a = b$ i.e. ($(Q, *)$ has unique solubility of equations) ."

Interesting examples and properties of quasigroups are given in this chapter.

Chapter II deals with Generation of Quasigroups. Important cryptographical problem is a generation of large sized quasigroups which is possible to keep easily in a compact form in computer memory. This implies the need for finding a more efficient method for representing quasigroups of large order and performing multiplication within these quasigroups.

In this Chapter , eight different schemes for generating quasigroups of large order are given. They are,

- ❖ Generation Using Isotopies. (Section – 2.1)
- ❖ Generation Using Affine Isotopies. (Section – 2.2)
- ❖ Generation Using Non– Affine Isotopies. (Section – 2.3)
- ❖ Generation Using Linear Mapping. (Section – 2.4)
- ❖ Generation Using Keyed Permutation. (Section – 2.5)
- ❖ Generation Using Complete Mapping. (Section – 2.6)
- ❖ Generation Using Affine Complete Mapping. (Section – 2.7)
- ❖ Generation Using Non- Affine Complete Mapping. (Section – 2.8)

Here, each scheme is illustrated with examples.

Chapter III is devoted to the study of Different types of quasigroups. Different types of quasigroups with interesting properties and applications are available in the literature. Some of them are

1. Linear Quasigroups, Albert, A.A., (1942), [4].
2. Medial Quasigroups, Hosszu, M., (1954), [30].
3. D - Quasigroups, Belousov, V. D., (1958), [5].
4. F - Quasigroups, Belousov, V. D., (1960), [6].
5. Ternary Quasigroups, Belousov, V. D., Hosszu, M., (1964), [10].
6. IP - Quasigroups, Belousov, V. D., Florja, I. A., (1966), [9].
7. Stein's Quasigroups, Belousov, V.D., Gvaramija, A.A., (1966), [12].

8. TS - Quasigroups, Belousov, V. D., (1967), [7]
9. CI - Quasigroups, Belousov, V. D., Curkan, B.V., (1969), [8].
10. Trimedial Quasigroups, Kepka, T., (1976), [37].
11. Infinitary - Quasigroups, Belousov, V. D., Stojakovic, Z., (1976), [11].
12. GS - Quasigroups, Volenec, V., (1990), [63].
13. Hexagonal Quasigroups, Volenec, V., (1991), [65].
14. Idempotent Medial- Quasigroups, Volenec, V., (1991), [64].
15. Quadratical Quasigroups, Volenec, V., (1993), [66].
16. B^* - Quasigroups, Afzal Beg., (1998), [3].
17. G_2- Quasigroups, Krcadinac, V., Volenec, V., (2005), [40].
18. Plastic Quasigroups, Krcadinac, V., Volenec, V., (2007), [41].
19. G - N Quasigroups, Adrian Petrescu., (2008), [2].
20. Napolean's Quasigroups, Krcadinac, V., (2010), [42].

In this Chapter the following types of quasigroups are dealt with.

- ❖ Medial Quasigroups and Idempotent Medial Quasigroups
- ❖ Hexagonal Quasigroups
- ❖ GS - Quasigroups
- ❖ CI - Quasigroups
- ❖ Ternary Quasigroups

In section 3.1, Medial Quasigroups and Idempotent Medial Quasigroups (IM Quasigroups) are defined with examples and some interesting properties are proved. The geometric concept "Par" in medial quasigroup is introduced (Definition 3.1.7). Based on this geometric concept, an interesting characterization in Idempotent Medial quasigroup is proved (Theorem 3.1.13).

In section 3.2, Hexagonal Quasigroups are defined using semi symmetric quasigroup, idempotent quasigroup and medial quasigroup. Some

important properties of hexagonal quasigroups are studied. In hexagonal quasigroups the geometric concept "Par" is introduced and studied.

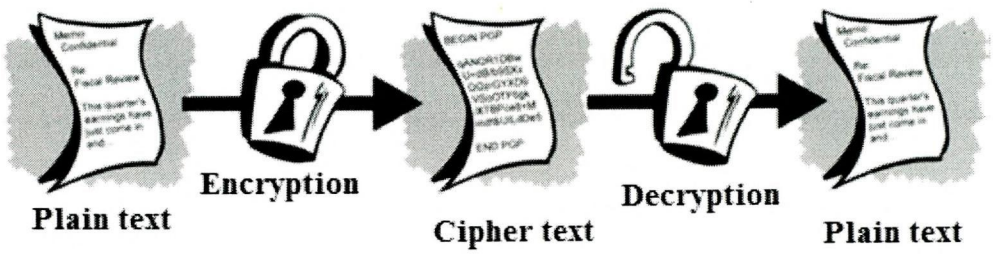
In section 3.3, the definition of Golden Section Quasigroup (GS – Quasigroup) is given with an example. The geometric concepts Parallelogram (Par), GS – Trapezoid (GST), Double GS – Trapezoid (DGST), Affine regular pentagon (ARP) and GS – Deltoid (GSD) are introduced in GS – Quasigroups and some interesting results regarding these concepts are obtained.

In section 3.4, Crossed – Inverse Quasigroups (CI – Quasigroups) are defined and some of their properties are studied. The interesting theorem proved here is

"Let $(G, \cdot)$ be an abelian group of order n such that n+1 is composite. Define a binary operation $(\bullet)$ on the elements of G by the relation $a \bullet b = a^r b^s$, where $rs = n+1$. Then $(G, \bullet)$ is a CI-quasigroup and the right crossed inverse of the element a is a^u, where $u = (-r)^3$."

Section 3.5 is focused on Ternary Quasigroups. Some interesting properties for ternary quasigroups are given with example.

Chapter IV deals with Applications of quasigroups in Cryptography. Cryptography deals with the transformation of ordinary text (plain text) into coded form (cipher text) by encryption and transformation of cipher text into plain text by decryption.



In section 4.1 of this chapter, Basic encryption and decryption schemes using quasigroups are explained with simple examples.

In section 4.2, some ideas for constructing hash functions using quasigroups are proposed. Hash functions are a special kind of (public) functions which are used in cryptography for different cryptographic purposes, like signature schemes, message authentication codes. Two quasigroup transformations $QM1: A^{2m} \to A^{2m}$ and $QM2: A^{m} \to A^{2m}$, (A is a quasigroup) are used for construction of hash functions. Based on these transformations it is shown that different kinds of hash functions can be designed with suitable security. In this section, the quasigroup transformation QM2 is considered for designing hash functions.

Section 4.3 deals with Authentication Schemes using Quasigroups. Message Authentication Codes (MACs), are a widely studied and used cryptographic tool. As the name suggests, MACs are most often used to authenticate a message. A MAC can be used both to ensure that a message has not been changed in transit and to verify the sender of a message. The key part of a message authentication code is the "secret" input to the MAC. By definition, the output of a MAC (called a check digit or an authentication tag) must be easy to compute with knowledge of the secret key, but difficult to compute without knowledge of this key. In addition, in order for a MAC to be practical, the key must require a reasonable amount of storage space, and the number of potential keys must be large enough to prevent attacks on the MAC.

MACs can be created in a variety of ways. Many MACs are based on some other cryptographic function, such as a hash function or a block cipher. The security of these MACs is then derived from the security of the hash function or the block cipher. However, MACs can also be developed which are not derived from any other cryptographic process, but instead are based on

some other algebraic structure. In this case, the security of the MAC comes from properties of the underlying algebraic structure. Denes and keedwell [18] and Kristen Ann Meyer [48] developed MACs based on quasigroups. In this section these two schemes are described with examples.

CI – quasigroups have certain properties which make them particularly appropriate for use in cryptography. Section 4.4 deals with Applications of CI – quasigroups in Cryptography. Here, the use of CI – quasigroups in encryption and decryption process is explained with examples.

In section 4.5, Ternary quasigroup transformations are defined for encryption and decryption and it is shown that these transformations are applicable in cryptography for cryptosystems based on quasigroups.