Summary and Conclusion

SUMMARY AND CONCLUSION

In today's world, the security concept is an important and essential factor, which is associated with almost all fields in peoples modern life. Cryptography is the science of securing data. Cryptography is not only used by spies but also used for phone, fax and e-mail communication, bank transactions, bank account security, PINs, passwords and credit card transactions on the web. It is also used for a variety of other information security issues including electronic signatures, which are used to prove who sent a message. The non-associative property of quasigroups has 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. Quasigroups operations are computationally simple and can be efficiently used for protection of voluminous media like images, audio, video and different forms of multimedia. They are also suitable for securing data transmitted from and to mobile and miniature resource-constrained devices with limited capability. Quasigroups are suitable for designing efficient as well as secure encryption schemes due to simplicity of the basic operation. Moreover, large and unstructured quasigroups can be generated. Use of such quasigroups helps to improve the security of the scheme.

This thesis is devoted to the study of Quasigroups and Their Applications to Cryptography. The discussion is under the following topics:

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

The first Chapter deals with Definitions and Basic properties of Quasigroups. Interesting Examples and properties of quasigroups are given in this chapter.

In Chapter II, eight different schemes for generating quasigroups of large order are given. They are, Generation of Quasigroups using Isotopies, Affine Isotopies , Non–Affine Isotopies, Linear Mapping, Keyed Permutation, Complete Mapping, Affine Complete Mapping , Non- Affine Complete Mapping. Here, each scheme is illustrated with interesting examples.

Chapter III is devoted to the study of the different types of quasigroups. In this chapter, Medial Quasigroups, Idempotent Medial Quasigroups, Hexagonal Quasigroups, Golden– Section Quasigroups, Crossed – Inverse Quasigroups, Ternary Quasigroups are studied.

Chapter IV deals with Applications of quasigroups in Cryptography.

Basic encryption and decryption using quasigroups are explained with simple examples in section 4.1.

In section 4.2, some ideas how to use a quasigroup in order to construct hash functions are proposed.

Section 4.3 deals with Authentication Schemes using Quasigroups. Here two schemes namely Denes and keedwell scheme and Meyer scheme which are used for creating Message Authentication Codes by using quasigroups are described with examples.

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.

Absolute dependence on electronic media, in the present computer world, adds much significance to cryptography which is relied upon to ensure secured transmission of electronic transactions. Quasigroups applications in cryptography have gained momentum in the present scenario. Other than cryptography, quasigroups theory is used in many applications such as coding theory, design theory and so on.