CHAPTER – 5

CONCLUSION AND FUTURE SCOPE
This chapter summarizes the contributions of this thesis and presents few of the problems of different difficulty and of different generality. These problems cover few specific topics of this thesis and also they address the problems related to the design and analysis of cryptographic hash functions in general.

5.1 Contribution of the thesis

The design and analysis of cryptographic hash functions is a challenging area of cryptography because there are a variety of platforms and they all have their own imposed constraints which make it difficult to specify generically the term “efficient” for all of them at the same time. But it is required to provide secure communication to the modern digital society.

Designing an efficient cryptographic hash function demands a vast research and effort. Every new design is influenced by existing and possible future designs and attacks. Thus, it requires a lot of time and effort to validate the security and the soundness of a design. To make it simpler, we focused on a very basic and natural question that is always argued in the crypto community: “What should be the basic properties while designing a secure cryptographic hash function?”

We can put many properties as follows, but these properties are not very easy to achieve simultaneously.

- The hash function should be simple to understand and analyze
- It should be efficiently implementable on various platforms
- It must be secure enough over the network to deal with various attacks

In this thesis we designed a cryptographic hash function meeting those above mentioned requirements.

Following is the chapter-wise discussion:

- The first chapter of the thesis deals with some basic definitions of hash functions. It tells about many of the preliminary requirements of a secured hash function design. We also present major classification of hash function based on some specific parameters.
• Second chapter talks about few existing popular hash construction methods and few of the hash functions, based on those construction methods. This chapter presents the literature review done before the proposal of new hash function.

• We propose the new design – “R-U Hash” in the third chapter. We put forward the argument of using a key component while designing a hash function. Then further we tested it on numerous sample data and files and analyzed its security. We also executed few popular existing hash functions for the same sample size on same machine configuration, and after comparison we further proved that if we take time as a major component while transferring data over network, our proposed algorithm is better than many existing hash functions, besides it also provides source authentication.

This thesis contributes towards more secure message transfer over internet while securing message integrity and source authenticity both. It clearly states that any attacker requires at least $2^{128}$ calculations before a successful brute force pre-image and brute force second pre-image attack to perform on R-U Hash. This is quite a large amount of calculation, which is considered among secure number of calculations (if calculation is more than $2^{64}$, it is considered to be safe), because practically it is not feasible to execute such a large number of test. Moreover it also safe from fixed point attack, and any other attack in which attacker tries to produce collision by inserting extra blocks into the input, by making padding rule compulsory.

Practical application of R-U Hash has also been shown using password hashing application. It may be used at any place where data is to be kept secure and also the sender’s information is also to be verified before dealing with data.

5.2 Limitations and Future Scope

During the performance analysis of proposed function, we compared it with other hash functions that use merely the operations addition, rotation and XOR. The population of RFID protocols that is based on random and complex combination of those operations make this area even more challenging. We leave this problem to the more patient and intelligent researcher.
The algorithm uses keyed function for a block of 64 bits. In future we may also perform the keyed function for smaller or larger block size and see whether it improves the security or time taken for overall processing of message.

The function runs well on 32 bit machine, as future enhancement, it should also work on 64-bit machine. Moreover the test and graphs can also be verified on MatLab or LabView. It should also be traceable by receiver that if the buffer value B1B2B3B4 got changed in the path or the message has been modified.

From the point of view of designing, there is always requirement of new types of hash functions. These new functions should offer a high level of security as well as their performance should also be better than previous ones. To possess more provable security properties for hash functions would also be desirable always. For block cipher based hash functions it is still an open problem to produce a secure hash function.