CONCLUSION AND SUGGESTION FOR FUTURE WORK

Encryption by an efficient technique is the backbone of security mechanism while storing the sensitive data and while transmitting the same. Efficient encryption technique is the one which gives maximum security as far as eaves dropping and cryptanalysis is concerned. One such technique is TDMRC code. TDMRC code is a technique that was specially devised to defeat eaves dropping.

For improving the security of any data in communication or store mode the data can be transliterated in to TDMRC mode and the original information can be obtained by reverse transliteration to ASCII mode.

This research study analyzed the working of TDMRC code and tried to bring out a method to search in an encrypted database encrypted using TDMRC code. Method developed is a key based method in which the whole database is thought to be divided into many section based on the username and keyword. For the access control mechanism algorithm for generating username is also developed which is based on matrix substitution mapping depending on data and key value.

The working of TDMRC code was studied in depth and the software developed for the study had the logic of TDMRC code as the central concept. The published work of TDMRC code was learned and the scope for improving
it was looked upon. For this the vulnerability of TDMRC code was checked and found that the logic of the code behaved even stronger when implemented and tested. But in certain special cases it was found that from the output of the code the data can be predicted. The possible cause of this behavior was traced and a modification of TDMRC code is proposed which can withstand this.

As a part of the study the logic of TDMRC code was applied on Unicode to develop TDMRU code. Here instead of treating data as a chain of ASCII characters, UNICODE characters are used. It was developed to study the application of TDMRC code on Natural Language Processing. Since UNICODE has 65536 characters, these characters could be arranged in $65536!$ different number of ways. Out of these only $P$ number of series are chosen based on the combination of System time and keys. Like TDMRC code virtual character set obtained for transliteration in TDMRU code is purely random.

**Suggestion for Future Work**

The method developed to Search in an encrypted database encrypted using TDMRC code is capable to work in a multi user environment but sharing of the data records are not considered/allowed. The study was limited to the assumption that the data records were at most important to the user and none other than the user should have access to them. The software can however be extended with a secret key sharing among the users to get such facilities.
Cryptanalysis on TDMRC code can be done further to find any other vulnerability of the system. The technique used in this research can be used to analyze the working of other block based or substitution based cryptographic technique. It is kept open to the fellow researchers in the field of cryptography and high speed data communication to develop these techniques further.

**Conclusion:**

This chapter gave the conclusion remarks and discussed the scope for further work.