CHAPTER 7

CONCLUSION

Web technologies have revolutionized the delivery of information and services, providing commercial and noncommercial functions through the web demanding high level of authentication. This research work is concerned with a study on cryptography and provides new idea to build digital signature schemes and digital certification process for solving some of the existing problems in authentications.

In this thesis, two new type of digital signature schemes and two cryptographic protocol schemes are presented for providing authentication applications. The digital signature schemes are:

1. Proxy Blind Distributed Signature Scheme which is based on Discrete Log Problem (DLP)
2. Identity Based Proxy Blind Distributed Signature Scheme based on Bilinear Pairing.

Signatures alone will not solve some specific problems like contract problem, certified electronic mail, etc. instead; the right approach is to use cryptographic tools to build protocols. That is explicitly specified processes are required for solving such problems. This thesis presented two cryptographic protocol schemes.

1. The first one is Verifiable Encryption of Elliptic Curve Digital Signature Algorithm (ECDSA) Signature Scheme. This protocol is an Adjudicated protocol, that is, the Trusted Third Party (TTP) takes part in the protocol only when there is a dispute.

2. The second one is Verifiable encryption scheme based on Elliptic Curve Discrete Log Problem (ECDLP). This protocol does not require the intervention of the third party.

In this thesis, implementation of all schemes is done using Java programming language and performance evaluation has been made and the results shows that the newly proposed schemes does not require additional overhead of time in their individual process. The following are some of the possible extensions of the models considered in this thesis for future research:

- The distributed digital signatures scheme can be studied using other hard problems.
- New application areas can be identified to fit the existing distributed digital signature schemes.
- A secured hash functions which is used for digital signing can be constructed.

Thus the present work is devoted to the construction of digital signature scheme and cryptographic protocols for intrinsic authentication applications.