CONCLUSIONS
The aim of the thesis is two fold, namely generation of shared keys based on public key cryptosystems and to present fast multiplication methods using Montgomery Methods to public key cryptosystems, such as RSA and NTRU. Shared key concepts cannot be directly applied upon these cryptosystems. However the methods existing in literature require high computational capabilities and consume a large amount of time. The Montgomery Methods have been promising and provided results by increasing the speed of both RSA and NTRU. Difficulties were faced during implementation of NTRU, as NTRU being a patented cryptosystem, no clear version of the implementation parameters were found. Extensive study and experimentation have revealed that care is required while choosing the parameters p and q of the algorithm, if they are to be chosen other than the published values.

The work has also shown a new method of shared key generation using truncated polynomials and this could be more efficient by using Montgomery methods even in this case. In the process Montgomery methods were also applied to shared key generation using RSA and observed that if Shared key generation is implemented along with Montgomery methods it could move much ahead of the new public cryptosystems that are being introduced. Though it appears that Montgomery methods could be applied in general to any Public key cryptographic algorithm, care needs to be taken while implementing Montgomery methods in, since these methods mostly depend upon the residue theorem.

Authentication mechanisms have also been worked upon, and efficient methods of implementing Zero-Knowledge Protocols were illustrated in the work. Our method has
shown a drastic improvement in the speed of authentication, making it a better one based on zero-knowledge authentication. Another algorithm for digital signatures using truncated polynomials was designed and incorporated into the work.

However all these ideas and implementations of shared key generation were applied to database security and found to be very much useful.

The work could also proceed in applying zero knowledge based authentication to shared key generation applied to database security. The shared key generation applied to database security implemented in this work was executed upon RSA platform. However the same could be implemented using truncated polynomials, whose algorithm is given in this work.

Summarizing the ideas it can be concluded that

- Application of Montgomery Techniques on RSA and NTRU resulted in speed improvement

- A new design methodology for Shared key versions of NTRU method is proposed making it more superior than the shared key RSA

- Algorithm for speeding up the process of shared key authentication are presented in this work

- Effective and efficient methods of authentication are developed in the work

000