Chapter 6

Conclusions

This chapter concludes the thesis. The major contributions of this thesis are as follows

- In Chapter 3, password-based remote user mutual authentication scheme using smart cards proposed by (Rajaram et al., 2009) is cryptanalysed. Next, we proved that Rajaram et al. scheme is still vulnerable to off-line password guessing attack, user impersonation attack and time synchronization problem. Moreover, the scheme does not provide an option to change/update the password and lacks efficient login, proper mutual authentication. We proposed a password-based remote user mutual authentication scheme using smart cards to rectify the security flaws found in Rajaram et al. scheme. Finally, the performance analysis of proposed scheme-I shows that it is simple and secure

- In Chapter 4, a dynamic ID-based remote user authentication scheme using smart cards proposed by Young-Hwa (Young-Hwa, 2013) is cryptanalysed. Then, we showed that Young-Hwa scheme is still vulnerable to off-line password guessing attack, user impersonation attack and time synchronization problem. Moreover, the scheme does not provide an option to change/update the password and lacks efficient login, proper mutual authentication. We proposed a dynamic ID-based remote user mutual authentication scheme using smart cards to eliminate the vulnerabilities found in Young-Hwa scheme. The performance of the proposed scheme-II is evaluated by comparing it with Young-Hwa and other related authentication schemes. It is clear that the proposed scheme-II is more suitable for application involving secure communications.

- In Chapter 5, we have cryptanalysed the scheme of (Rhee et al., 2011) and showed that this scheme did not provide perfect forward secrecy, user
friendliness and local password verification, and also it suffers from user impersonation attack, off-line password guessing attack. In order to overcome the weaknesses of Rhee et al. scheme, we proposed a secure authentication scheme with user anonymity for roaming service in global mobile networks. Performance and security analysis shows that the proposed scheme-III is secure against various attacks, and is well suited for secure mobile communications.