Lab Practical – Phase 4

Execute following programs using gmp library in C.

Note: Do not use predefined functions from any Library or Header file, as far as possible. Instead write your own user define function for it.

Q1) Implement Diffie-Hellman Key exchange.

Q2) Implement Kerberos using any symmetric cryptosystem.

Q3) Implement Needham–Schroeder protocol using any symmetric cryptosystem.

Q4) Implement the digital certificate system.