LIST OF TABLES

Table 1.1 Encryption decryption Sub keys for IDEA 12
Table 1.2 NIST recommended key sizes 21
Table 1.3 Relative computation costs of Diffie-Hellman and Elliptic Curves 22
Table 1.4 Key sizes v/s MIPS years needed for attack 23
Table 3.1 Strength of Diffie Hellman V/s Elliptic Curve Keys. 102
Table 3.2 NIST recommended key length 127
Table 4.1 Irreducible trinomials and pentanomials over GF(2^m) 155
Table 4.2 A simple representation of GF(2^4) numbers. 157
Table 4.3 Various situations considered to add variable length numbers 160
Table 5.1 Speed analysis of rshift() function 184
Table 5.2 Time optimization of function add() in µ seconds 189
Table 5.3 Storage optimization of add() and rshift() 189
Table 5.4 Speed of modular multiplication for NIST numbers in µ seconds 190
Table 5.5 x/y mod 13 in GF(2^{13}) 192
Table 5.6 Computing for verify_pt_on_curve() function 193
Table 5.7 Function calls to implement operations of table 5.6 194
Table 5.8 Implementation of point double in projective coordinates 195
Table 5.9 Function wise timing for point double. 195
Table 5.10 Implementation of point add in mixed coordinates. 196
Table 5.11 Function wise timing for mixed point add. 197
Table 5.12 Optimization of timings for point add for B163 numbers. 198
Table 5.13 Optimized timing results for NIST numbers. 198