Number Theory and Cryptography

Assignment -2

Q. No.	Question	CO	BT
1	Explain the Chinese remainder theorem with an example.	3	L2
2	Explain the Pohlig–Hellman algorithm with an example.	3	L2
3	Explain the Pollard’s p−1 factorisation algorithm with an example.	3	L2
4	Explain RSA PKC with one example. Design a program to implement RSA PKC.	4	L2, L6
5	Explain Diffie-Hellman using Elliptic curve cryptography briefly and give one example. Develop a program to implement Diffie-Hellman using Elliptic curve cryptography.	5	L2, L6