VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

BCSE309L – Cryptography and Network Security

Digital Assignment 2

Submission Deadline: 09/10/2024 (Softcopy and Hardcopy)

1. Suppose Alice and Bob use an ElGamal scheme with a common prime q=71 and a primitive root α=7. If Bob has public key Y_B=3 and Alice chooses the random integer k=2, Compute the ciphertext for the message, M. The message M is computed as the sum of the four digits of your register number after the program code. E.g., if your register number is 21BRS1058 then M=1+0+5+8= 14.

2. Srini, Shrish, and Saina are part of a group chat application where they want to establish a shared secret key for secure communication using the Diffie-Hellman key exchange algorithm. They agree to use a prime number p=17 and a primitive root g=7. Srini chooses his secret key a=7, Shrish chooses b=11, and Saina chooses c=13. Perform the multiparty Diffie-Hellman key exchange and compute the shared secret key.

3. Assume a secure communication happens between User A and B using elliptic curve cryptosystem. The cryptosystem parameters are E_{11}(1, 7) and G=(3,2). B’s private key is n_B=7. Compute B’s public key P_B. A wishes to encrypt the message P_m=(10, 7) and chooses a random value k=2. Determine the ciphertext C_m. Show the calculation by which B recovers P_m from C_m.

*****