PSG College of Technology

Department of Applied Mathematics and Computational Sciences

MSc Theoretical Computer Science

15XT68 -Security in Computing Lab

Problem Sheet 2

Task 1: Key establishment

Build an application that combines the Diffie-Hellman Key Exchange with AES encryption algorithm. Like many of the real world cryptography supported applications, build an application that first uses Diffie-Hellman Key Exchange to achieve the goal of exchanging shared secret key. Then use the private-key encryption mechanism, AES in this lab, to encrypt the rest of the communication in a client server environment.

The application will first use Diffie-Hellman Key Exchange to create a shared secret key between Alice and Bob by using the user entered p, g, Alice's private key and Bob's private key. Then, the application will continue using AES encryption algorithm with the generated shared secret key to encrypt the user's message. At last, the application will also decrypt the cipher text and show the user about the decrypted result.

***Task 2: Secure data transfer*:**

Implement a client /server module with proper UI for the following scenario:

The client system requests the file stored in the server by sending the name of the file to the server module. The server in turn would encrypt the requested file and send it to the client system. The modules shall use AES as a security mechanism. Write a separate module for the key generation to be used.