NITTE EDUCATION TRUST
NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY
An Autonomous Institution Approved by UGC/AICTE/Govt. of Karnataka
Accredited by NBA (Tier – I) and NAAC 'A+' Grade
Affiliated to Visveswaraya Technological University, Belagavi
Post Box No. 6429, Yelahanka, Bengaluru – 560 064, Karnataka, India

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Cryptography and Network Security Laboratory (18CSL68)

Part A Lab Exercises

1. Implement Caesar Cipher encryption & Decryption technique which is by replacing eachcharacter by another character that will be some fixed number of positions down to it.
2. Demonstrate the Playfair cipher, consider the key table 5×5 grid of alphabets that acts asthe key for encrypting the plaintext.
3. Implement Data encryption and decryption using Hill Cipher method.
4. Encrypt the plaintext using a Vigenère table that consists of the alphabet from A to Z written out 26 times in different rows, further each alphabet must be shifted cyclically to the left compared to the previous alphabet.
5. Implement Rail fence cipher technique using the row & Column Transformation.
6. Demonstrate the Data Encryption Standard based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion).
7. Execute the program for simple RSA algorithm to encrypt and decrypt the data.
8. Implement Diffie Hellman (DH) key exchange algorithm as a method for securely exchanging cryptographic keys over a public communications channel.

Part B Lab Exercises

Design an android application for end-to-end encryption of short message service (SMS) using RSA that can conceal message regarding student's results/notification on placements/Department's updates of Nitte Meenakshi Institute of Technology (NMIT), while on transit to another mobile device using RSA on android operating system and implement it for security of mobile SMS.

The objectives to implement are shown below:

i) Develop an Android-based pattern unlocking messaging application by integrating existing RSA SecurID, a mechanism developed by RSA.

ii) Develop an android application for the NMIT that will ensure the encryption of every message transmitted within the network of an organization using RSA. This application will provide security measures whenever information is transmitted from one mobile device to another because it is important to protect the information while it is on transit.

Expected outputs:

Fig. 1: SMS service Dashboard on Mobile App

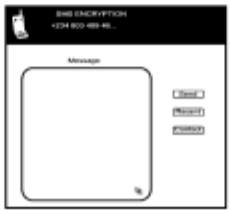

Fig. 2: SMS service to compose message at the sender end

Fig. 3: Display encrypted and Decrypted message at receiver end