Lab Specification
B.Sc. Engg. Part 4, Even Semester, Session: 2017-2018, Examination 2021
CSE-4232P (Cryptography and Network Security)

1. **Suppose you are given a line of text as a plaintext, find out the corresponding Caesar Cipher (i.e. character three to the right modulo 26). Then perform the reverse operation to get original plaintext.**

2. **Find out the Polygram Substitution Cipher of a given plaintext (Consider the block size of 3). Then perform the reverse operation to get original plaintext.**

3. **Consider the plaintext "DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLY UNIVERSITY OF RAJSHAHI BANGLADESH", find out the corresponding Transposition Cipher (Take width as input). Then perform the reverse operation to get original plaintext.**

4. **Find out corresponding double Transposition Cipher of the above plaintext. Then perform the reverse operation to get original plaintext.**

5. **You are supplied a file of large nonrepeating set of truly random key letter. Your job is to encrypt the plaintext using ONE TIME PAD technique. Then perform the reverse operation to get original plaintext.**

6. Use the Lehmann algorithm to check whether the given number P is prime or not?

7. Use the Robin-Miller algorithm to check whether the given number P is prime or not?

8. Write a program to implement MD5 one way hash function.

9. Write a program to implement Secured Hash Algorithm (SHA) one way hash function.

10. **Encrypt the plaintext message using RSA algorithm. Then perform the reverse operation to get original plaintext.**

11. Write a program to implement Diffie-Hellman Key Exchange.

(Md. Tohidul Islam)
Associate Professor
Dept. of CSE
University of Rajshahi