Institute of Engineering Science and Technology, Shibpur.
IT Department
Information and Systems Security Lab 2020
Assignment – 2

Date: 23.01.2020

Last Date of Submission: 29.01.2020

1. Implement the following traditional symmetric ciphers.
    a. Shift Cipher
    b. Multiplicative Cipher
    c. Affine Cipher
    d. Playfair Cipher
    e. Hill Cipher

2. Write programs to carry out exhaustive key search attacks on the *Shift Cipher, Multiplicative Cipher* and *Affine Cipher* that you have implemented. (Aim to attack a cipher is to break its key.)

    a. Hence use an exhaustive key search to decrypt the following ciphertext, which was encrypted using a Shift Cipher:

       BMMTDXLTANZXXYYHKMMHYKXXRHNKLXEYYKHF
       FXFHKR

    b. Use an exhaustive key search to decrypt the following ciphertext, which was encrypted using a Multiplicative Cipher:

       WFEJBYOFAJZEYDCMRBKJRKWABKXSWKJZSFQ

    c. Use an exhaustive key search to decrypt the following ciphertext, which was encrypted using a Affine Cipher:

       EFXECFBDQGGXRADQTFFUFSPGAHQTDGGAFZDJFG
       HJFBDQGHGDCCGXSFJDHQGAFZDJF