Assignment – 1 Date: August 5, 2015

FM – 20

Submission Deadline: August 19, 2015

(No assignment will be evaluated after the deadline)

1. Implement the following in Modular Arithmetic:
    a. Additive inverse of a number
    b. Multiplicative inverse of a number
    c. Inverse of an m×m matrix with $m \leq 3$

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

3. Write programs to carry out exhaustive key search attacks on the *Shift Cipher* and the *Multiplicative 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:

    BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

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

    WFEJBYOFAJZEYDCMRBKJRKWABKXSWKJZSFQ