Assignment – 1 Date: August 1, 2018

Submission Deadline: August 8, 2018

All assignments will be marked out of 20. Assignments submitted after the deadline will be penalized with 5 marks for each week delay.

1. Implement the Euclidean algorithm for finding GCD of two numbers.

2. 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 $m \leq 3$

3. Implement the following traditional symmetric ciphers.
    a. Shift Cipher
    b. Multiplicative Cipher
    c. Affine Cipher

4. Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a Shift Cipher, where the plaintext is supposed to be in English language:

    BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

    Print out the sequence of decrypted texts in your console.