Assignment – 3 Date: August 29, 2018

Submission Deadline: September 12, 2018

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

PART-I

1. Write a program for *cipher-text only* statistical cryptanalysis of an Affine Cipher, given the following statistics about the English language (Assume the length of cipher text is at least 100 characters):

Table-1

letter	probability	letter	probability
A	.082	*N*	.067
B	.015	*O*	.075
C	.028	*P*	.019
D	.043	*Q*	.001
E	.127	*R*	.060
F	.022	*S*	.063
G	.020	*T*	.091
H	.061	*U*	.028
I	.070	*V*	.010
J	.002	*W*	.023
K	.008	*X*	.001
L	.040	*Y*	.020
M	.024	*Z*	.001

Hence decrypt the following cipher text obtained by Affine Encryption (You may use the Affine Decryption program written by you in Assignment-1):

```
KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP
KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKP
BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF
ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK
IVKSCPICBRKIJPKABI
```

PART-II

(In this part of the assignment consider plaintext, ciphertext and key-streams as bit sequences.)

1. A One-Time Pad (OTP) is a stream cipher which uses True Random Number Generator (TRNG) to generate its key-stream, hence the name OTP. It uses the XOR-operation as both encryption and decryption functions.

   a) Implement an OTP stream cipher.
   (You may use any Pseudo-Random Number Generator (PRNG) to generate the key-stream here considering that following a physical process is infeasible for this laboratory.)

   b) Assuming the PRNG looks like:

   $$S_0 = \text{seed}$$
   $$S_{i+1} \equiv AS_i + B \bmod m, \text{ where } i = 0,1, \ldots$$

   where $m = 26$ is public, the secrets are A, B and the seed, where all A, B, S_i belong to Z_{26}, and an outsider is provided with the knowledge of only first 15 bits of plaintext, implement a way for (known-plaintext) cryptanalysis of the OTP.
   [Hint: Note that $2^4 < 26 < 2^5$]