Indian Institute of Technology Delhi
COL 100 - Introduction to Computers and Programming
II Semester 2014-2015
Assignment 6: 2D Arrays – Encryption/Decryption

Question 1,2 are not graded.
Question 3 is graded.

Background:

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not by itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted.

Encryption is used to protect data in transit, for example, data being transferred via networks (e.g., the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

Let us try to implement a small encryption/decryption program.

Question 1 [Non Graded]

Given a square matrix A of order N, find its inverse.

Question 2 [Non Graded]

Write two functions :

```
input(array,rows,cols); // User inputs an array of rows*cols
print(array,rows,cols); // Print an array of rows*cols
```

Question 3. [Graded]
Given:

- a plaintext A consisting of an input sequence of ASCII characters,
- a map table MAP,
- an integer marker M, and
- an MxM key matrix K,

generate the ciphertext C. Then decrypt this ciphertext to obtain the original plaintext.

Follow the steps below for encryption and decryption. For the purpose of illustration let us take:
A = abcde
MAP = {{'a','A'},{'b','B'},{'c','C'},{'d','D'},{'e','2'},{'0','i'}}
M = 4
Key = K (4x4 matrix)

Step 1 : Padding with 0s
Pad with 0s if not divisible by marker M (= 4)
Example, A_Zero_Padded = (abcd)(e000)

Step 2 : Writing a map function
There is a map table MAP which maps and scrambles the input.
If A_Zero_Padded = (abcd)(e000)
then A_mapped_array is (ABCD)(2iii)

Step 3 : Using matrix multiplication to generate ciphertext C
Represent the A_mapped_array in 2D form as shown below.
Then multiply with the key matrix K.

'A','B','C','D' X K = C
'2','i','i','i'

Step 4 : Find inverse of K and find B
Calculate invK, the inverse of K, and determine B using:
C X invK = B
For this example we will get,
B = 'A','B','C','D'
'2','i','i','i'

Step 5 : Find decrypt_A_mapped_array

Using B and inverse map from table MAP, find decrypt_A_mapped_array.

In our example, decrypt_A_mapped_array = (abcd)(e000)

Step 6 : Find Decrypt_plain_text

Remove zero padding and find Decrypt_plain_text.

Decrypt_plain_text = abcde

The following are variables are to be calculated in the program:

```
1. Cipher Text,      C
2. Key Inverse,      invK
3. Decrpyted_plain_text
```

Follow the instructions below:

1. Comment the code
2. Do not add more STD libraries
3. Do study the sample/test outputs to get a better understanding of the program behaviour
4. Padding zero means ASCII zero '0'
5. Only [a-z] [A-Z] [0-9] are the acceptable inputs. (Why?)