Outline of the Program:

A. For Question 1:

1) We have included the following text files in our Program:

- Key.txt
- Messege.txt
- Cipher.txt
- Decrypted.txt

2) User Enters the size of key in “Key.txt” file with space separated by key elements. First element corresponds to the size of matrix then press Space tab to enter the key matrix values.

3) Program takes the Plaintext message from “message.txt” file where user will give the message which is to be encrypted. Then it removes all the spaces and special characters from the message. Depending on the size of the key if the message text length is not multiple of key, then it performs padding by inserting “x” at the remaining spaces.

4) Program then forms the Matrix “msg” of size (key, 1) by taking the key size letters at once.

5) Then it performs the Encryption process by multiplying the “Key Matrix” with “Msg Matrix” and generates the Ciphertext in a separate file name as “Cipher.txt”.

Here the Encryption Process gets completed.

6) Now to decrypt our message we first take the input from “Cipher.txt” file and forms the matrix of size(key,1) by taking the key size letters at once and named it as Matrix “cphr”.

7) For decryption process we need the inverse of our key matrix. Hence, we first find the determinant of key matrix. Then we need the multiplicative inverse of our determinant value. Thus, we passed the determinant value to the function “mulInverse” which gives the multiplicative inverse.

8) Now to find the Adjoint of matrix we pass the key matrix value to the Adjoint Function which in turn gives the Adjoint of key matrix. Finally, we calculate the Inverse of key matrix by Multiplying the Multiplicative inverse to the Adjoint of Key matrix.

9) We store this value in Matrix “keyInverse”. Then it performs the Decryption process by multiplying the “keyInverse” Matrix with “cphr Matrix” and generates the Plaintext in a separate file name as “decrypted.txt”

B. For Question 2:

1. Here in this question, we are given with some portion of the Plaintext and complete ciphertext. User can access it from “messege.txt” file and “cipher.txt” file respectively.
2. Now to perform the operation for finding the key size, we assume the initial key size to be 2 and then update it by one after every loop.
3. Then we form the Matrices namely “cphr” and “plaintext” from the corresponding “cipher.txt” and “msg.txt” file. Now as to determine the key size we have to have the Inverse of Plaintext matrix hence we pass it to inverse function where it calculates the inverse and stores the value in “plainInverse” Matrix.
4. Now we multiply the two matrices namely “cphr” and “plainInverse” to generate the key matrix. Now we decrypt our Cipher text using the obtained key and check the Index of coincidence for this key. If it Gives Index of coincidence close to 0.068 then we finalize this key and if it doesn’t give answer close to 0.068 then we increment the key by 1 and check for the rest key value as per the above process till we get the Closest Index of coincidence Value.