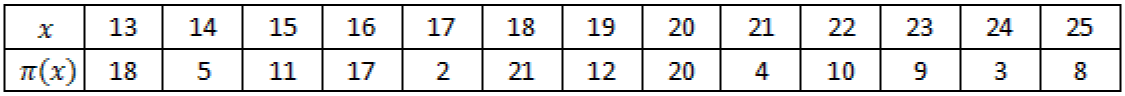
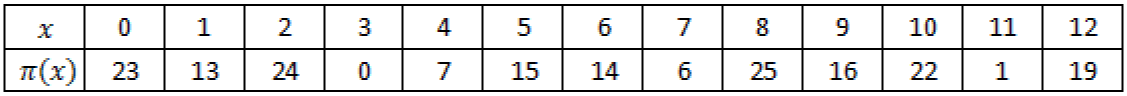
CRYPTOGRAPHY

ASSIGNMENT 1

1. Encrypt the plaintext “Frodo ran to the hill top” using Caesar cipher and shift cipher (key = 21).
2. Suppose π is following permutation of $\mathbb{Z}_{26}$:



x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	18	5	11	17	2	21	12	20	4	10	9	3	8



x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(x)$	23	13	24	0	7	15	14	6	25	16	22	1	19

Encrypt the message “Maybe there is no right choice ” using simple substitution cipher.

3. Encrypt the message “Have you seen boromir” using vigenere cipher. Use key: “aragorn”.
4. This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5..., then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on. Encrypt the plaintext sendmoremoney with the key stream

   0 1 7 23 15 21 14 11 11 2 8 9

5.
   a. Encrypt the message “meet me at the usual place at ten” using the Hill cipher with the key $\begin{pmatrix}9 & 4\\5 & 7\end{pmatrix}$. Show your calculations and the result.

   b. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. Also show how the inverse key is computed.
6. Encrypt the text “How do you do this riddle ” using Playfair cipher. Use the word “winterfell” as key.
7. Encrypt the plaintext “Is not it nice to think that tomorrow is a new day with no mistakes in it yet ” using railfence cipher with key = “4”. Also show the decryption.
8. Describe about security policy and mechanisms in brief.
9. Describe Security services provided by cryptography in brief.