INTRODUCTION TO CRYPTOGRAPHY – QUIZ 4
B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of submission: 01/02/2022

Quiz

1. (2 points) An involutory key in a permutation cipher is a permutation π such that $\pi^{-1}=\pi$. In other words,$\pi(i) =j \Longleftrightarrow \pi(j) =i$. For m= 3, there are four involutory keys. Find them.

-> Consider p = (1 2 3)

Involuntary keys (π) include :

- $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
- $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
- $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Eg: CAT encrypted using π =$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ -> TAC

Now π (TAC) -> CAT

2. (4 points) For the key K=$\begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$ in Hill Cipher, find K^{-1}.

-> K=$\begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$ is a 2x2 matrix, therefore inverse of such matrix -> K^{-1}=(1/det|k|)$\begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$

|K| =21-10=11

1/|K|=11^{-1} = 19

K^{-1}=(19)$\begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$= $\begin{pmatrix} 133 & -38 \\ -95 & 57 \end{pmatrix}$= $\begin{pmatrix} 3 & -12 \\ -17 & 5 \end{pmatrix}$= $\begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix}$

Therefore, K^{-1}= $\begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix}$

3. (6 points) By using the Hill cipher with the key K as given in the previous problem, decrypt:

WZNLQM

->	W	Z	N	L	Q	M
	22	25	13	11	16	12

$(22 \quad 25) \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} = (5 \quad 17)$

$(13 \quad 11) \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} = (8 \quad 3)$

$(16 \quad 12) \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} = (0 \quad 24)$

5	17	8	3	0	24
F	R	I	D	A	Y

Therefore, decrypted text = friday

4. (2 points) Suppose that a key stream is generated for a stream cipher by using the following linear recurrence $z_{i+2}=z_i+z_{i+1} \bmod 2$ for $i \geq 1$. For the initial vector $(z_1,z_2) = (1,1)$ find the first six bits of the key stream.

->

$z_{i+2} = z_i + z_{i+1}$

$z_1 = 1$, $z_2 = 1$

$z_3 = z_{1+2} = z_1 + z_{1+1} = z_1 + z_2 = 1+1 = 2 \bmod 2 = 0$

$z_4 = z_{2+2} = z_2 + z_{2+1} = z_2 + z_3 = 1+0 = 1 \bmod 2 = 1$

$z_5 = z_{3+2} = z_3 + z_{3+1} = z_3 + z_4 = 0+1 = 1 \bmod 2 = 1$

$z_6 = z_{4+2} = z_4 + z_{4+1} = z_4 + z_5 = 1+1 = 2 \bmod 2 = 0$

Therefore, the first 6 bits of the key stream are : 1,1,0,1,1,0

5. (2 points) Find the period of the key stream generated by linear recurrence and initial vector as given in the previous problem.

-> Key stream's period is given by 2^m-1 where m is the initial key length. The initial key length in the previous question is m=2, therefore

Period = $2^2-1 = 4-1 = 3$

6. (4 points) By using auto key cipher with the key k = 7, decrypt:

LBFB

-> Auto key = 7

L	B	F	B
11	1	5	1
11-7=4	1-4=-3=23	5-23=-18=8	1-8=-7=19
4	23	8	19
E	X	I	T

Plaintext = exit