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 π−1=π. In other words,π(i) =j⇐⇒π(j) =i. For m= 3, there are four involutory keys. Find them.

-> Consider p = (1 2 3)

Involuntary keys (π) include :



Eg: CAT encrypted using π = -> TAC

Now π (TAC) -> CAT

1. (4 points) For the key K= in Hill Cipher, find K−1.

-> K= is a 2x2 matrix, therefore inverse of such matrix -> K-1=(1/det|k|)

|K| =21-10=11

1/|K|=11-1 = 19

K-1=(19)= = =

Therefore, K-1=

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 25) = (5 17)

(13 11) = (8 3)

(16 12) = (0 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 zi+2=zi+zi+1mod 2 for i≥1. For the initial vector (z1,z2) = (1,1) find the first six bits of the key stream.

->

zi+2 = zi + zi+1

z1 = 1, z2 = 1

z3 = z1+2 = z1 + z1+1 = z1 + z2 = 1+1 = 2 mod 2 = 0

z4 = z2+2 = z2 + z2+1 = z2 + z3 = 1+0 = 1 mod 2 = 1

z5 = z3+2 = z3 + z3+1 = z3 + z4 = 0+1 = 1 mod 2 = 1

z6 = z4+2 = z4 + z4+1 = z4 + z5 = 1+1 = 2 mod 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 2m-1 where m is the initial key length. The initial key length in the previous question is m=2, therefore

Period = 22-1 = 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