INTRODUCTION TO CRYPTOGRAPHY – QUIZ 2

B.Tech. Computer Science and Engineering (Cybersecurity)

|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of submission: 14/01/2021 |

Quiz 2

1. (4 points) Suppose that k= (9,22) is a key in an Affine Cipher over Z26. Write the decryption function in the form dk(y) =ry+s, where r,s ∈ Z26. Your answer should be exactly in this form where 0≤r,s≤25.

-> k=(9,22)

ek(x) =9x+22

dk(y) =3(y-22)=3y-66=3y+(-66)=3y+12

Therefore, dk(y) = 3y + 12

2. (6 points) By using the decryption function d(y) = 7y+ 10, decrypt the message: WZWZWF

-> W Z W Z W F

initial 22 25 22 25 22 5

dk 164 185 164 185 164 45

final 8 3 8 3 8 19

letter i d i d i t

Plaintext: ididit

3. (4 points) Suppose that k= (25,2) is a key in an Affine Cipher over Z26. Write the decryption function in the form dk(y) =ry+s, where r,s ∈ Z26. Your answer should be exactly in this form where 0≤r,s≤25.

-> k=(25,2)

ek(x) =25x+2

dk(y) =25(y-2) {Inverse of 25 in mod 26 = 25}

=25y-50=25y+(-50)=25y+2

Therefore, dk(y) = 25y + 2

4. (2 points) For a given key k, if the encryption function ek is identical to the decryption function dk, then the key k is called an involutory key. Say true or false: The key given in the previous problem is an involutory key.

-> True, the key given in the previous problem is an involutory key.

5. (2 points) True or False: If the encryption function is given by ek(x) =x+ 13 mod 26, then the corresponding key is an involutory key.

-> ek(x) =x+ 13

k=(1,13)

dk(y) =1(y-13) {Inverse of 1 in mod 26 = 1}

=y-13=y+(-13)=y+13

dk(y) =y+13 which is same as ek(x) =x+ 13

Therefore, TRUE, the corresponding key is an involutory key.

6. (2 points) Compute the value of Euler phi function φ(100).

-> Now, 100=22x52

φ(100) = (22 - 21)(52 – 51)= (4-2)(25-5) = (2)(20) = 40