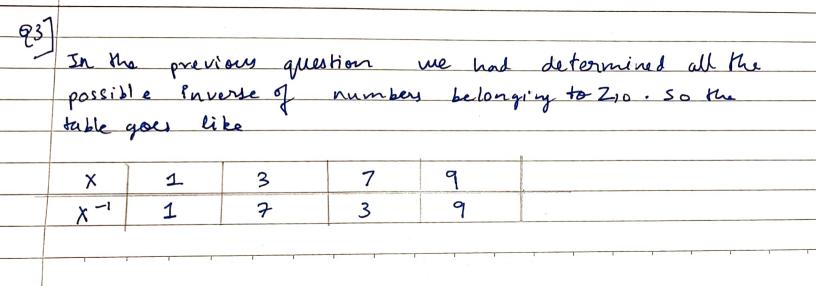
Cryptography Quiz 3

- Problem 1 (2 points): Calculate the value of Euler phi function $\phi(10)$.
- Problem 2 (4 points): List all the numbers in \mathbb{Z}_{10} which have multiplicative inverse.
- Problem 3 (4 points): Find the inverse of all the numbers in \mathbb{Z}_{10} for which the inverse exists. Hint: You need not create the division algorithm table here. Since \mathbb{Z}_{10}^* is small, you can find the inverses by checking directly.
- Problem 4 (6 points): It is known that a key k=(a,b) in the Affine Cipher over \mathbb{Z}_{26} (where $\gcd(a,26)=1$) is an involutory key if and only if $a^2\equiv 1 \mod 26$ and $b(a+1)\equiv 0 \mod 26$. Assuming this fact, find all involutory keys in the Affine Cipher over \mathbb{Z}_{26} . (Hint: There are 28 of them! Recall that an involutory key is the key for which the encryption and decryption rules are identical.)
- Problem 5 (4points): Decrypt the following cipher text by using Vigenere cipher with the key "mrbond":

ORTWARDFZOYH

Write your plaintext that has two words.

Page No. Date: KO16 - Dinesh - Cryptor - Quiz - 3 27/1/22 Q1] Calculate the value of Euler phi function \$ (10) Ans) 10 is a non-prime number. = \$ (2'x5') (mxn) = \$ (20 . \$ 5 = 2 d s are prime no.s 'So, we know that $\phi(P) = P-1$ = (2-1) (5-1) 2 1. 4 92] List all the numbers in Z10 which have multiplicative inverse Any 7 = 21, 2, 3 9 3 =) We know that inverse of the numbers only exist when they are coprime with the given number or the GCD (a, (num) = 1 SCD (1, 10) =1 GCO (3,10)=1 (nco (7,10)=1 GCD (9,10) = 1 {1,3,7,9} are the list of numbers in Zo, which have multiplicative inverse



Page No. Date:

Ans) Inverse in Z26

a= {1,25)

94]

21

condition b* (a+1) = 0 mod 26

Fora =1, b will have {0,13)

All the privaly tory key pair are.

(25,23) (25,24) (25,25)

for a = 25, b = fo, 1, 2, 3, 4, 25}

15

11

For the key (a, b) to be involutory, the condition a= 1 mod 26

should be satisfied

Similarly we find the values of b which satisfy the

(1,0) (1,13) (25,0) (25,1) (25,2) (25,3) (25,4) (25,5) (25,6)

(25,7) (25,8) (25,9) (25,10) (25,11) (25,12) (25,13) (25,14)

(25, 15) (25, 16) (25, 17) (25, 18) (25, 19) (25, 20) (25, 21) (25, 22)

23

17

2.5

25

| | | | | | 1 | | | | | | - | Page No. | | |
|---------------------------------------|----------------------|-------|----------------------|-------------|----|---|--|--|--|--------|----------|----------|-----------|---|
| <u>9</u> 5 | Copherte | = | 0 R mr { 12,19 | bone | 7 | | | | | | | | | |
| | To find Plaintext | | , | | | | 1 | 3 e ² . | | · · | <u>.</u> | | | |
| | Cophertext | 0 | R | T | W | A | R | D. | F | 2 | . 0 | Y | И | |
| | Value | 14 | 17 | 19 | 22 | 0 | 17 | 3 | .5 | 25 | 14 | 24 | 7 | |
| Decryptiony wing the | Key | 12 | 17 | 1 | 19 | 13 | 3 | 12 | 17 | 1 | 14 | 13 | 3 | |
| (CJ-15) mod 26 | | | | | | | or the same of the | | ļ | | | 1. | 1. | - |
| | Value | 2 | 0 | 18 | 8 | 13 | 14 | and the same of th | 14 | 24 | 0 | | . 4 | |
| | Plain Text | C | A | S | I | Ny | 0 | R | 0 | · | Α. | ト | E | |
| | | 17.00 | . (3) | <i>₩</i> .3 | | Total Control | A A COUNTY OF THE PARTY OF THE | demonstration and a contract of the contract o | manusco de Caración de Caració | | | | Little Co | |
| · · · · · · · · · · · · · · · · · · · | The deri | | pla R | | | | Ho | be | gra | u pe a | l in | 2000 | rds | |
