INTRODUCTION TO CRYPTOGRAPHY – QUIZ 3
B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of submission: 27/01/2022

Quiz 3

Problem 1 (2 points) : Calculate the value of Euler phi function $\varphi(10)$.

➔ $10 = 2^1 \times 5^1$

Therefore, $\varphi(10) = (2^1 - 2^0)(5^1 - 5^0) = (2-1)(5-1) = (1)(4) = 4$

Problem 2 (4 points): List all the numbers in Z_{10} which have multiplicative inverse.

➔ If a number A has a multiplicative inverse in Z_{10}, then gcd(A,10) must equal 1. Such a number would therefore be a prime relative of 10. As solved in the sum above, Z_{10} has 4 such values.

The 4 values are: 1, 3, 7, 9 (Not multiples of 2 or 5)

Problem 3 (4 points): Find the inverse of all the numbers in Z_{10} for which the inverse exists.

Hint: You need not create the division algorithm table here. Since Z^*_{10} is small, you can find the inverses by checking directly.

➔ The inverses:

For 1: 1

For 3: 7

For 7: 3

For 9: 9

Problem 4 (6 points): It is known that a key k= (a,b) in the Affine Cipher over Z_{26} (where gcd(a,26) = 1) is an involutory key if and only if $a^2 \equiv 1 \bmod 26$ and $b(a+1) \equiv 0 \bmod 26$. Assuming this fact, find all involutory keys in the Affine Cipher over 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.)

➔ For involuntary key (a,b)

$e_k(x) = ax+b$ & $d_k(y) = ay+b$

It is known that gcd(a,26)=1, therefore, 'a' has to be a prime relative of 26 which leaves us with 12 possible options for 'a' - (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25).

Now, it is also given that $a^2 \equiv 1 \bmod 26$, which reduces the values of a to 1, 25

a+1=2, 26

Another given fact is that b(a+ 1)≡0 mod 26, therefore, b = 0-25 for a=25 (Since 25+1=26 and any product would be 0 in mod 26) and b= 0,13 for a=1 (since 2x0=0 & 2x13 = 26)

The keys therefore are:
(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), (25,23), (25,24), (25,25)

Problem 5 (4points): Decrypt the following cipher text by using Vigenere cipher with the key "mrbond":

ORTWARDFZOYH

Write your plaintext that has two words.

➔	m	r	b	o	n	d						
	12	17	1	14	13	3						
	O	R	T	W	A	R	D	F	Z	O	Y	H
	14	17	19	22	0	17	3	5	25	14	24	7
	m	r	b	o	n	d	m	r	b	o	n	d
	12	17	1	14	13	3	12	17	1	14	13	3
			S	**U**	**B**	**T**	**R**	**A**	**C**	**T**		
	2	0	18	8	13	14	17	14	24	0	11	4
	c	a	s	i	n	o	r	o	y	a	l	e

Plaintext: casino royale