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.

27/1/22 K016 _ Dinesh - Crypto - Quiz - 3

Q1] Calculate the value of Euler phi function $\phi(10)$

Ans) 10 is a non-prime numbers

$$\begin{array}{r|l} 2 & 10 \\ \hline 5 & 5 \\ \hline & 1 \end{array}$$

$= \phi(2^1 \times 5^1)$ $\phi(m \times n)$

$\Downarrow$

$= \phi(2) \cdot \phi 5$ $\phi m \cdot \phi n$

$=$ 2 & 5 are prime no.s

So, we know that $\phi(P) = P - 1$

$= (2-1) \cdot (5-1)$

$= 1 \cdot 4$

$= 4$ //

Q2] List all the numbers in $Z_{10}$ which have multiplicative inverse

Ans] $Z_{10} = \{1, 2, 3 \ldots\ldots 9\}$

⇒ We know that inverse of the numbers only exist when they are coprime with the given number or the $GCD(a, (num)) = 1$

so,

$GCD(1, 10) = 1$

$GCD(3, 10) = 1$

$GCD(7, 10) = 1$

$GCD(9, 10) = 1$

$\{1, 3, 7, 9\}$ are the list of numbers in $Z_{10}$, which have multiplicative inverse

Q3]

In the previous question we had determined all the possible inverse of numbers belonging to $Z_{10}$. So the table goes like

| $x$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| $x^{-1}$ | 1 | 7 | 3 | 9 |

Q4]

Ans) Inverse in $Z_{26}$

| a | 1 | 3 | 5 | 7 | 11 | 17 | 25 |
|---|---|---|---|---|---|---|---|
| $a^{-1}$ | 1 | 9 | 21 | 15 | 19 | 23 | 25 |

For the key (a,b) to be involutory, the condition $a^2 \equiv 1 \mod 26$ should be satisfied

$a = \{1, 25)$

Similarly we find the values of b which satisfy the condition $b * (a+1) \equiv 0 \mod 26$

For a = 1, b will have $\{0, 13)$

for a = 25, $b = \{0, 1, 2, 3, 4, \ldots\ldots 25\}$

All the involutory key pair 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)

Q5] Given

Cipher text = ORTWARDFZOYH

Key = mrbond

{ 12,17, 1, 14,13, 3 }

To find

Plaintext and has to be grouped in 2 words

Decrypting using the key ((CT-K)mod26

| Cipher text | O | R | T | W | A | R | D | F | Z | O | Y | H |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Value | 14 | 17 | 19 | 22 | 0 | 17 | 3 | 5 | 25 | 14 | 24 | 7 |
| Key | 12 | 17 | 1 | 14 | 13 | 3 | 12 | 17 | 1 | 14 | 13 | 3 |
| Value | 2 | 0 | 18 | 8 | 13 | 14 | 17 | 14 | 24 | 0 | 11 | 4 |
| Plain Text | C | A | S | I | N | O | R | O | Y | A | L | E |

The derived plaintext has to be grouped in 2 words

So, Casino Royale.