# CS553 Cryptography

BitBees

Question 4

## Question 4

### Part A

The Affine cipher is defined as follows:

$$enc_{a,b} : Z_m \rightarrow Z_m$$
$$x \rightarrow ax + b \,\epsilon\, Z_m$$

$$dec_{a,b} : Z_m \rightarrow Z_m$$
$$y \rightarrow a^{-1}.(y - b) \,\epsilon\, Z_m$$

Given, K $(= (a, b))$ is called involutary if $enc_{a,b}(x) = dec_{a,b}(x)$

$$\implies enc_{a,b}(x) = dec_{a,b}(x)$$
$$\implies (a.x + b) \pmod m = a^{-1}.(x - b) \pmod m$$
$$\implies a.x \pmod m + b \pmod m = a^{-1}.x \pmod m - a^{-1}.b \pmod m$$
$$\implies a.x \pmod m - a^{-1}.x \pmod m + b \pmod m + a^{-1}.b \pmod m = 0 \pmod m$$
$$\implies (a - a^{-1}).x \pmod m + (b + a^{-1}.b) \pmod m = 0 \pmod m$$

Which is only possible if:

$$\implies a - a^{-1} = 0 \pmod m$$
$$\implies a = a^{-1} \pmod m \tag{1}$$

(Because gcd(a,m) = 1, a $\bmod m = a$)
$And : \implies b + a^{-1}.b = 0 \pmod m$

$$\implies b.(a^{-1} + 1) \equiv 0 \pmod m \tag{2}$$

From 1:

$$\implies b.(a + 1) \equiv 0 \pmod m \tag{3}$$

## Part B

In order to find the possible involutory keys in $Z_{15}$, simply run the python file **q4b.py**. They come out to be:
(1, 0)
(4, 0)
(11, 0)
(14, 0)
(14, 1)
(14, 2)
(4, 3)
(14, 3)
(14, 4)
(11, 5)
(14, 5)
(4, 6)
(14, 6)
(14, 7)
(14, 8)
(4, 9)
(14, 9)
(11, 10)
(14, 10)
(14, 11)
(4, 12)
(14, 12)
(14, 13)
(14, 14)
Total number of keys are 24.

## Part C

Since we know that the condition $gcd(a, m) = 1$ must be satisfied. To calculate all valid $a$ we can take help of Euler Toitent function

$$\Phi(n) = |\{1 \leq a < n|(a, n) = 1\}|$$

And

$$\Phi(p) = p - 1$$

for prime numbers, we can factorize our given $m$ to its prime factors.

$$\Phi(mn) = \Phi(m)\Phi(n)$$

Similarly there are total $m$ possible values for $b$ since $b \in \{0, ..., m-1\}$
So therefore, the number of possible keys for Affine Cipher can be written as

$$N(m) = m \cdot \Phi(m)$$

$$\begin{aligned}N(30) &= 30 \cdot \Phi(30)\\ N(30) &= 30 \cdot 8\\ N(30) &= 240\end{aligned}$$

$$\begin{aligned}N(100) &= 100 \cdot \Phi(100)\\ N(100) &= 100 \cdot 40\\ N(100) &= 4000\end{aligned}$$

$$\begin{aligned}N(1225) &= 1225 \cdot \Phi(1225)\\ N(1225) &= 1225 \cdot 840\\ N(1225) &= 1029000\end{aligned}$$