CS553: Cryptography

Assignment 2: Solutions

Rohit Das (11910230)

September 20, 2019

1. How Many Keys?

$r = 23$ (formed from $2nd$ and $3rd$ digits of roll number)
$\therefore \mathbb{Z}_{23}^{+} = \{0, 1, ..., 22\}$
Let $K = (a, b)$ be the set of possible keys, such that $\forall k \in K$, $\gcd(r, a) = 1$.
So, given $r = 23$, $a = \{1, 2, ..., 22\}$. $\therefore |a| = 22$. Similarly, $b = \{0, 1, ..., 22\}$. $\therefore |b| = 23$. $\therefore |\mathbf{K}| = \mathbf{22} \times \mathbf{23} = \mathbf{506}$.

2. Euler Phi Function

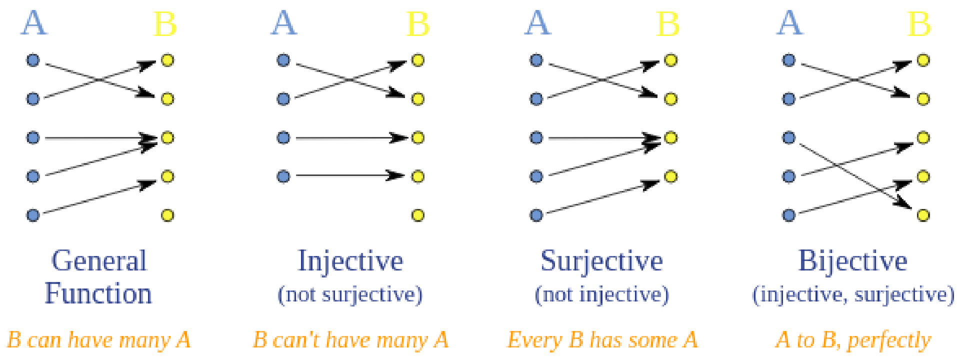
Euler Phi Function, also known as Euler's totient function, returns the count of integers less than and relatively prime to n. It is denoted by $\phi(n)$.
For prime positive integers, $\phi(n) = (n - 1)$. For other positive integers, if $n = pq$, where p,q $\in \mathbb{Z}^{+}$ and prime, $\phi(n) = (p - 1)(q - 1)$. In general, Euler's phi function can be written as:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

The number of keys, $|K|$, for an Affine Cipher defined over $\mathbb{Z}_{r}^{+}$ can be easily obtained by simply using Euler's totient function $\phi(r)$.
Since our r is prime, $\phi(r) = (r-1) = 22$. Given $|b| = 23$, $|\mathbf{K}| = \mathbf{22} \times \mathbf{23} = \mathbf{506}$.

3. Bijection

Given $X = \{x_1, x_2, ..., x_n\}, Y = \{y_1, y_2, ..., y_n\}$ and $|X| = |Y|$.
Also given, $f : X \to Y$ is injective, i.e. $\forall\ x \in X$, $f(x)$ is unique, or $f(x)$ is a one-to-one function. So naturally, $|X| \leq |Y|$.
But, we know $|X| = |Y|$, meaning, $\forall\ y \in Y$, $\exists\ x \in X$, s.t. $f(x) = y$. Hence, f is also surjective, i.e. onto.
$\therefore f$ is a bijection (Proved).



4. Euclidean GCD

Python code (Python3): Euclidean_gcd.py

```
def E_gcd(a,b): # function to calculate Euclidean GCD
    a,b = (b,a) if a < b else (a,b) # swaps a and b if a < b
    while True:
        r = a % b
        if (r == 0):
            break
        a = b
        b = r
    return b


try: # to allow only integer input
    a,b = [int(i)for i in(input("Enter two integers: ").split(" "))]
except ValueError:
    print("Please enter two integers!")
    exit(0)

print(E_gcd(a,b))
```

5. Involutory Key

5..1 Proof of involutory key

Given an Affine Cipher over $\mathbb{Z}_m$ with $K = (a, b)$.

Let $e_K(x) = (ax + b)$ mod m, $d_K(x) = a^{-1}(x - b)$ mod m be the encryption and decryption function respectively.

Proof 1: Assuming key K is involutory, i.e. $d_K(x) = e_K(x)$.......(1), to prove a^{-1} mod m $= a$, and $b(a + 1) \equiv 0$ mod m.

From (1), $(ax + b)$ mod m $= a^{-1}(x - b)$ mod m,

$\implies (ax + b)$ mod m $= (a^{-1}x - a^{-1}b)$ mod m

$\therefore a \equiv a^{-1}$ mod m....(2), and

$b \equiv -a^{-1}b$ mod m....(3) [$\because$ two functions $ax + b$ and $cx + d$ are equal if their coefficients are equal, i.e. a = c and b = d].

From (2), we get $a \equiv a^{-1}$ mod m (Proved).

From (3), we get $ab \equiv -b$ mod m,

$\implies b(a + 1) \equiv 0$ mod m (Proved)

Proof 2: Assuming $a \equiv a^{-1}$ mod m...(4), and $b(a + 1) \equiv 0$ mod m, to prove K is involutory, i.e. $e_K(x) = d_K(x)$

$b(a + 1) \equiv 0$ mod m

$\implies ba \equiv -b$ mod m, $\implies b \equiv -a^{-1}b$ mod m...(5)

Putting (4) and (5) in $e_K(x)$, we get

$e_K(x) = (ax + b)$ mod m $= \{a^{-1}x$ mod m $+ (-a^{-1}b)$ mod m$\}$ mod m

$= a^{-1}(x - b)$ mod m $= d_K(x) \implies$ Key K is involutory

$\therefore$ The above two proofs prove that Key K is involutory iff $a \equiv a^{-1}$ mod m, and $b(a + 1) \equiv 0$ mod m.(Proved)

5..2 Number of involutory keys

For an Affine Cipher defined over $\mathbb{Z}_{15}$, possible values for a, such that $a = a^{-1}$

mod m are $\{1, 4, 11, 14\}$(using a^2 mod 15). For each value of a, possible values of b such that $b(a+1) \equiv 0$ mod n follow:

For $a = 1$, $b\ (1 + 1) = 2b$, meaning, only possible value for b $\in \mathbb{Z}_{15}$ is 0. $|b| = 1$

For $a = 4$, $b\ (4 + 1) = 5b$. So, $b = \{0, 3, 6, 9, 12\}$. $|b| = 5$.

For $a = 11$, $b\ (11 + 1) = 12b$. $b = \{0, 5, 10\}$. $|b| = 3$.

For $a = 14$, $b\ (14 + 1) = 15b$. b can take any value from $\mathbb{Z}_{15}$. $|b| = 15$.

$\therefore$ Total no. of involutory keys = 1 + 5 + 3 + 15 = **24**.