# MATH1064 Assignment2

SID:530157791

October 13, 2023

## Answer to question1

(a) $(p, q) = (5, 13)$ , $n = p \cdot q = 65$

(b)

(i)

1. All numbers less than n and divisible by p are not coprime to n since they share a factor with p.So we have:
   $A = \{p, 2p, 3p, ....., (q-1)p\}$ and $|A| = q - 1$
2. Similarly, all numbers less than n and divisible by q are not coprime to n. $B = \{q, 2q, 3q, ....., (p-1)q\}$ and and $|B| = p - 1$
3. $|A \cap B| = 0$
4. Thus there are $(p-1)+(q-1)$(Inclusion-Exclusion Principle) numbers are not coprime to n.
5. Therefore there are $pq - 1 - (p + q - 2) = (p - 1)(q - 1)$ numbers are coprime(gcd(k, n) = 1) to n when $0 < k < n$.

(ii) $\varphi(n) = (5 - 1)(13 - 1) = 48$

(c) $e = 7$, public key : (7,65)

==========

==========

## Answer to question2

In this case,I choose $d = 7$ such that $7 \cdot 7 \equiv 1(mod 48)$
Private key : (7, 65)

## Answer to question3

Imformation :

- Public key : (7,65)
- Private key : (7,65)
- SID : 530157791
- Last 8 digit : 30157791($M = \{m_1, m_2, ..., m_8\}$ = {3,0,1,5,7,7,9,1})
- d = 7
- e = 7

(a) $c_i \equiv m_i^7 \pmod{65}$,$0 \leq c < n$

- $c_1 = 3^7 \text{mod } 65 = 42$
- $c_2 = 0^7 \text{mod } 65 = 0$
- $c_3 = 1^7 \text{mod } 65 = 1$
- $c_4 = 5^7 \text{mod } 65 = 60$
- $c_5 = 7^7 \text{mod } 65 = 58$
- $c_6 = 7^7 \text{mod } 65 = 58$
- $c_7 = 9^7 \text{mod } 65 = 9$
- $c_8 = 1^7 \text{mod } 65 = 1$

==========

(b)$m_i^{'} \equiv c_i^7 \pmod{65}$,$0 \leq m < n$ ,$1 \leq i \leq 8, i \in \mathbb{N}$

- $m_1^{'} = 42^7 \text{mod } 65 = 3$
- $m_2^{'} = 0^7 \text{mod } 65 = 0$
- $m_3^{'} = 1^7 \text{mod } 65 = 1$
- $m_4^{'} = 60^7 \text{mod } 65 = 5$
- $m_5^{'} = 58^7 \text{mod } 65 = 7$
- $m_6^{'} = 58^7 \text{mod } 65 = 7$
- $m_7^{'} = 9^7 \text{mod } 65 = 9$
- $m_8^{'} = 1^7 \text{mod } 65 = 1$

$M^{'} = \{3, 0, 1, 5, 7, 7, 9, 1\}$

$M = M^{'}$

==========

==========

## Answer to question4

(a) James's(my friend) public key : (7 , 33)

(b) Perelman.

- P = 16
- E = 5
- R =18
- E = 5
- L = 12
- M = 13
- A = 1
- N = 14

Then encode $M = \{16, 5, 18, 5, 12, 13, 1, 14\}$ by public key (7,33).
Encoded messages $c_i \equiv m_i^7$ mod n, $1 \leq i \leq 8, i \in \mathbb{N}$
$C = \{25, 14, 6, 14, 12, 7, 1, 20\}$

(c)Encoded messages from James:
$CJ = \{50, 16, 16, 60, 14, 57, 60, 9, 52, 60, 47\}$
My private key : (7,65)
So that $MJ_i \equiv CJ_i^7$ (mod 65):
$MJ = \{15, 16, 16, 5, 14, 8, 5, 9, 13, 5, 18\}$
Which is Oppenheimer!
==========