MATH1064 Assignment 2

SID: 530328265 - Tutorial: 16.00 TUE

Due Date: Thursday 2023/10/19

1.

(a) We have the following options.

$$(p, q) \in \{(3, 5), (3, 7), (3, 11), (3, 13), (5, 7), (5, 13)\}$$

From this options, I choose $(p, q) = (5, 13)$. We have:

$$n = pq$$

Thus, my n is equal to:

$$n = pq = 5 \times 13 = 65$$

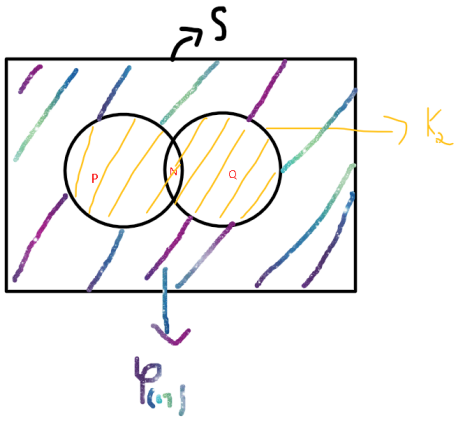

Figure 1: Ex: 1b

(b) (i). We call $S = \{k \in \mathbb{N}, 0 < k < n\}$

We also have: $n = pq$

Then, $|S|$ is equal to:

$$|S| = pq - 1 \tag{1}$$

We call $P = \{k, p \in \mathbb{N}, 0 < k \leq n,$ k is divisible by p$\}$

Then, $|P|$ is equal to:

$$|P| = \lfloor (\frac{pq}{p}) \rfloor = q \tag{2}$$

We call $Q = \{k, q \in \mathbb{N}, 0 < k \leq n,$ k is divisible by q$\}$

Then, $|Q|$ is equal to:

$$|Q| = \lfloor (\frac{pq}{q}) \rfloor = p \tag{3}$$

We call $N = \{k, pq \in \mathbb{N}, 0 < k \leq n,$ k is divisible by pq$\}$

Then, $|N|$ is equal to:

$$|N| = \lfloor (\frac{pq}{pq}) \rfloor = 1 \tag{4}$$

We call $K_1 = \{k, p, q \in N, 0 < k \leq n,$ k is divisible by p or q$\}$

From (2), (3) and (4), by the principle of inclusion-exclusion, we can determine the quanitity of numbers that divisible by p or q.

$$|K_1| = |P| + |Q| - |N| = p + q - 1 \tag{5}$$

However, In order to find the number of numbers greater than 0 but less than pq that are divisible by either p or q, we subtract the number pq from the set of numbers divisible by p or q.

We call $K_2 = \{k, p, q \in N, 0 < k < n,$ k is divisible by p or q$\}$.

Then, from (5), we have:

$$|K_2| = |K_1| - 1 = p + q - 1 - 1 = p + q - 2 \tag{6}$$

As the set of all numbers which share a factor with pq are complement of the set of pq's coprimes, we can determine the number of positive integers $0 < k < n$ such that $\gcd(k, n) = 1$.

Thus, from (1) and (6), we have:

$$\varphi(n) = |S| - |K_2| = pq - 1 - (p + q - 2) = pq - p - q + 1 = (p - 1)(q - 1) \quad \blacksquare$$

(ii). From my choice in (a), $n = 65$ and $(p, q) = (5, 13)$. Thus, my $\varphi(n)$ is equal to:

$$\varphi(n) = (p - 1)(q - 1) = (5 - 1)(13 - 1) = 4 \times 12 = 48$$

(c) Choose $e = 7$ since:

$$\gcd(e, \varphi(n)) = \gcd(7, 48) = 1$$

Therefore 7 and 48 are relatively prime.

Thus, my public key is $(e, n) = (7, 65)$

2.

(a) Because e and d are allowed to be the same number, d is choosen to be 7 We have:

$$ed \equiv 1 \pmod{\varphi(n)}$$

Then,

$$7d \equiv 1 \pmod{48}$$

Then,

$$7 \times 7 \equiv 1 \pmod{48}$$

Equal to:

$$49 \equiv 1 \pmod{48}$$

Thus, my private key is $(7, 65)$

3.

(a) My student number is 530328265.Thus my last eight individual digits of my student number is 30328265.

To encode the last eight individual digits of my student number, We then calculate the coded message c by finding.

$$c \equiv m^e \pmod{n},\ 0 \leq c < n$$

Thus, we have:

$$c_1 \equiv m_1^e \pmod{n}$$

Then:

$$c_1 \equiv 3^7 \pmod{65} \implies c_1 = 42$$

Similar to count c_1, we can calculate c_2, c_3, c_4, c_5, c_6, c_7, c_8

$$c_2 \equiv 0^7 \pmod{65} \implies c_2 = 0$$

$$c_3 \equiv 3^7 \pmod{65} \implies c_3 = 42$$

$$c_4 \equiv 2^7 \pmod{65} \implies c_4 = 63$$

$$c_5 \equiv 8^7 \pmod{65} \implies c_5 = 57$$

$$c_6 \equiv 2^7 \pmod{65} \implies c_6 = 63$$

$$c_7 \equiv 6^7 \pmod{65} \implies c_7 = 46$$

$$c_8 \equiv 5^7 \pmod{65} \implies c_8 = 60$$

(b) To decode a message c using my private key $(7, 65)$, we calculate m using the following equation.

$$m \equiv c^d \pmod{n},\ 0 \leq m < n$$

Thus, we have:

$$m_1 \equiv c_1^d \pmod{n} \tag{7}$$

Then:

$$m_1 \equiv 42^7 \pmod{65}$$

We have:

$$42^7 \equiv (42^2 \times 42^2 \times 42^2 \times 42) \pmod{65}$$

Which equal to:

$$42^7 \equiv (9 \times 9 \times 9 \times 42) \pmod{65} \tag{8}$$

From (8), we have:

$$42^7 \equiv 3 \pmod{65}$$

Thus, $m_1 = 3$

Similar to count m_1, we can calculate m_2, m_3, m_4, m_5, m_6, m_7, m_8

$$\begin{aligned}
m_2 &\equiv 0^7 \pmod{65} \implies m_2 = 0 \\
m_3 &\equiv 42^7 \pmod{65} \implies m_3 = 3 \\
m_4 &\equiv 63^7 \pmod{65} \implies m_4 = 2 \\
m_5 &\equiv 57^7 \pmod{65} \implies m_5 = 8 \\
m_6 &\equiv 63^7 \pmod{65} \implies m_6 = 2 \\
m_7 &\equiv 46^7 \pmod{65} \implies m_7 = 6 \\
m_8 &\equiv 60^7 \pmod{65} \implies m_8 = 5
\end{aligned}$$

4.

(a) I find a friend that have different public key from mine. His public key is $(e, n) = (5, 39)$

(b) Because my friend's public key is $(5, 39)$ so $e = d = 5$ and $n = 39$

I choose **EUCLID** is the last name of a famous mathematician from history.

Then, convert each letter of **EUCLID** to a 2-digit number (i.e A = 1, B = 2, ..., Z = 26). Thus, we have the table below.

Letter	Number	Letter	Number	Letter	Number	Letter	Number
A	1	H	8	O	15	V	22
B	2	I	9	P	16	W	23
C	3	J	10	Q	17	X	24
D	4	K	11	R	18	Y	25
E	5	L	12	S	19	Z	26
F	6	M	13	T	20		
G	7	N	14	U	21		

From the table, we can see that $E = 5$, $U = 21$, $C = 3$, $L = 12$, $I = 9$, $D = 4$.

Thus, when convert **EUCLID** to 2-digit number, we have,

$$\textbf{EUCLID} \implies 5|21|3|12|9|4$$

Then, I will encode this name by using friend's public key $(5, 39)$ by using:

$$c \equiv m^e \pmod{n},\ 0 \leq c < n$$

Which equal to:

$$c \equiv m^5 \pmod{39},\ 0 \leq c < 39$$

1. Encode E:
$$E = 5 \implies c_E \equiv 5^5 \pmod{39} \implies c_E = 5$$
2. Encode U:
$$U = 21 \implies c_U \equiv 21^5 \pmod{39} \implies c_U = 21$$
3. Encode C:
$$C = 3 \implies c_C \equiv 3^5 \pmod{39} \implies c_C = 9$$
4. Encode L:
$$L = 12 \implies c_L \equiv 12^5 \pmod{39} \implies c_L = 12$$
5. Encode I:
$$I = 9 \implies c_I \equiv 9^5 \pmod{39} \implies c_I = 3$$
6. Encode D:
$$D = 4 \implies c_D \equiv 4^5 \pmod{39} \implies c_D = 10$$

(c) My friend send me a code is 45|60|59|38|1 by using my public key.

Now I will decode the message that my peer sent to me by using my private key (7, 65), I calculate m using the following equation

$$m \equiv c^d \pmod{n},\ 0 \leq m < n$$

Which equal to:

$$m \equiv c^7 \pmod{65},\ 0 \leq m < 65$$

1. Decode 45
$$c_1 = 45 \implies m_1 \equiv 45^7 \pmod{65}$$

We have:

$$45^7 \equiv (45^2 \times 45^2 \times 45^2 \times 45) \pmod{65}$$

Which equal to:

$$45^7 \equiv (10 \times 10 \times 10 \times 49) \pmod{65} \tag{9}$$

From (9), we have:

$$45^7 \equiv 20 \pmod{65}$$

Thus,

$$m_1 = 20 \implies m_1 \text{ is T}$$

Similar to calculate m_1, we can find the value of m_2, m_3, m_4, m_5

$$\begin{aligned}
m_2 &\equiv 60^7 \pmod{65} \implies m_2 = 5 \implies m_2 \text{ is E} \\
m_3 &\equiv 59^7 \pmod{65} \implies m_3 = 19 \implies m_3 \text{ is S} \\
m_4 &\equiv 38^7 \pmod{65} \implies m_4 = 12 \implies m_4 \text{ is L} \\
m_4 &\equiv 1^7 \pmod{65} \implies m_5 = 1 \implies m_5 \text{ is A}
\end{aligned}$$

After decode, the message that my friend sent to me is **TESLA**