CS60065: Cryptography and Network Security Total: 70 *points*

Assignment 1

Name: Anit Mangal Due: *Aug 12, 2024*

Note: The basic policies are stated in the course page. Using GPT (or similar tools) to solve problems from the assignment is **strictly prohibited**. Use of any other (possibly online) source(s) **must** be clearly stated in the solution. **Any dishonesty, if caught, will yield zero credits for the entire assignment.**

A. [**Modular Arithmetic : 3 × 3 = 9 points**.]

Answers

A.1

$$25 \equiv 1 \pmod 8$$

We know that, if $a \equiv b \pmod m \Rightarrow ac \equiv bc \pmod m$.
Multiplying by 25

$$\begin{aligned} \Rightarrow 25^2 &\equiv 25 \pmod 8 \\ &\equiv 1 \pmod 8 \\ 25^3 &\equiv 25 \pmod 8 \\ &\equiv 1 \pmod 8 \\ &\vdots \\ 25^n &\equiv 1 \pmod 8 \\ 5^{2n} &\equiv 1 \pmod 8 \end{aligned}$$

Using $a \equiv b \pmod m \Rightarrow a + c \equiv b + c \pmod m$

$$\begin{aligned} \Rightarrow 5^{2n} + 7 &\equiv (1 + 7) \pmod 8 \\ &\equiv 0 \pmod 8 \end{aligned}$$

+3

$\therefore 8 \mid (5^{2n} + 7), \forall n \in \mathbb{N}$.

A.2

$$7 \equiv 3 \pmod 4$$

We know that, if $a \equiv b \pmod m \Rightarrow ac \equiv bc \pmod m$.
Multiplying by 7

$$\begin{aligned}
\Rightarrow 7^2 &\equiv 3 \cdot 7 \pmod 4 \\
&\equiv 21 \pmod 4 \\
&\equiv 1 \pmod 4 \\
7^4 &\equiv 1 \cdot 7^2 \pmod 4 \\
&\equiv 49 \pmod 4 \\
&\equiv 1 \pmod 4 \\
7^6 &\equiv 1 \cdot 7^2 \pmod 4 \\
&\equiv 49 \pmod 4 \\
&\equiv 1 \pmod 4 \\
&\vdots \\
7^{32} &\equiv 1 \pmod 4 \\
\Rightarrow 6 \cdot 7^{32} &\equiv 6 \pmod 4 \equiv 2 \pmod 4 \qquad (1)
\end{aligned}$$

Now,

$$\begin{aligned}
9 &\equiv 1 \pmod 4 \\
\Rightarrow 9^2 &\equiv 1 \cdot 9 \pmod 4 \\
&\equiv 9 \pmod 4 \\
&\equiv 1 \pmod 4 \\
9^4 &\equiv 1 \cdot 81 \pmod 4 \\
&\equiv 81 \pmod 4 \\
&\equiv 1 \pmod 4 \\
&\vdots \\
9^{44} &\equiv 1 \pmod 4 \\
9^{45} &\equiv 1 \cdot 9 \pmod 4 \\
&\equiv 9 \pmod 4 \\
&\equiv 1 \pmod 4 \\
\Rightarrow 7 \cdot 9^{45} &\equiv 7 \pmod 4 \equiv 3 \pmod 4 \qquad (2)
\end{aligned}$$

Using $a \equiv b \pmod m$ and $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$
Adding (1) and (2)

$$\begin{aligned}
\Rightarrow (6 \cdot 7^{32} + 7 \cdot 9^{45}) &\equiv (2 + 3) \pmod 4 \\
&\equiv 5 \pmod 4 \\
&\equiv 1 \pmod 4
\end{aligned}$$

+3

$\therefore$ remainder when $6 \cdot 7^{32} + 7 \cdot 9^{45}$ is divided by 4 is 1.

A.3

$$4n^2 + 1 \equiv 0 \pmod{65}$$
$$4n^2 \equiv -1 \pmod{65}$$
$$4n^2 \equiv 64 \pmod{65}$$
$$n^2 \equiv 16 \pmod{65}$$

One solution for this is

$$n \equiv \pm 4 \pmod{65}$$

$\Rightarrow n = 65k + 4$ or $65k + 61, \forall k \in \mathbb{N}_0$.
Hence, there exist infinitely many $n \in \mathbb{N}$ such that $4n^2 + 1$ is divisible by 65.
+3

B. [GCD and Euclid's Algorithm : $5 + 2 + (3 \times 3) = 16$ points.]

Answers

B.1 $a = -85652,\ b = 16261$
Using *Euclidean division algorithm*, computing $GCD(a, b)$
Since $a < b$, swapping a and b

$$
\begin{aligned}
16261 &= -85652 \times 0 \ + 16261 \\
-85652 &= 16261 \times -6 \ + 11914 \\
16261 &= 11914 \times 1 \ + 4347 \\
11914 &= 4347 \times 2 \ + 3220 \\
4347 &= 3220 \times 1 \ + 1127 \\
3220 &= 1127 \times 2 \ + 966 \\
1127 &= 966 \times 1 \ + 161 \\
966 &= 161 \times 6 \ + 0
\end{aligned}
$$

So, $GCD(a, b) = 161$.

Using *Extended Euclidean Algorithm*,

$$GCD(a, b) = GCD(b, a\%b),\ a \geq b$$

And, by *Bézout's Identity*,

$$\exists x, y \in \mathbb{Z} \text{ such that } GCD(a, b) = ax + by$$

Let x_1, y_1 be Bézout's coefficients for $GCD(b, a\%b)$

$$
\begin{aligned}
\therefore ax + by &= bx_1 + (a - \left\lfloor \frac{a}{b} \right\rfloor b)y_1 \\
ax + by &= ay_1 + b(x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1)
\end{aligned}
$$

$$\boxed{\Rightarrow x = y_1, y = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1} \tag{3}$$

Using this result recursively, Bézout's coefficients for a, b can be found.
For $a = -85652,\ b = 16261$,

$$
\begin{aligned}
&GCD(-85652, 16261) && \longrightarrow x_1, y_1 \\
&= GCD(16261, 11914) && \longrightarrow x_2, y_2 \\
&= GCD(11914, 4347) && \longrightarrow x_3, y_3 \\
&= GCD(4347, 3220) && \longrightarrow x_4, y_4 \\
&= GCD(3220, 1127) && \longrightarrow x_5, y_5 \\
&= GCD(1127, 966) && \longrightarrow x_6, y_6 \\
&= GCD(966, 161) && \longrightarrow x_7, y_7 \\
&= 161
\end{aligned}
$$

Since $966 \cdot (1) + 161 \cdot (-5) = 161$

$$x_7 = 1, y_7 = -5$$

Using result (3) recursively,

$$x_6 = -5, y_6 = 1 - \left\lfloor \frac{1127}{966} \right\rfloor \cdot (-5) = 6$$
$$x_5 = 6, y_5 = -5 - \left\lfloor \frac{3220}{1127} \right\rfloor \cdot (6) = -17$$
$$x_4 = -17, y_4 = 6 - \left\lfloor \frac{4347}{3220} \right\rfloor \cdot (-17) = 23$$
$$x_3 = 23, y_3 = -17 - \left\lfloor \frac{11914}{4347} \right\rfloor \cdot (23) = -63$$
$$x_2 = -63, y_2 = 23 - \left\lfloor \frac{16261}{11914} \right\rfloor \cdot (-63) = 86$$
$$x_1 = 86, y_1 = -63 - \left\lfloor \frac{-85652}{16261} \right\rfloor \cdot (86) = 453$$

$\therefore GCD(a, b)$ expressed as linear combination of a and b is

$$-85652 \cdot 86 + 16261 \cdot 453 = 161 \tag{4}$$

Now, $LCM(-85652, 16261) = -8650852$,
Adding and subtracting $-8650852k$ in (4), $\forall k \in \mathbb{Z}$

$$(-85652) \cdot 86 + 16261 \cdot 453 + (-8650852k) - (-8650852k) = 161$$
$$(-85652) \cdot 86 + 16261 \cdot 453 + (-85652) \cdot (101k) - 16261 \cdot (-532k) = 161$$
$$(-85652) \cdot (86 + 101k) + 16261 \cdot (453 + 532k) = 161$$
$$\Rightarrow x = 86 + 101k, y = 453 + 532k, \forall k \in \mathbb{Z}$$

$\therefore\ S = \{(86 + 101k, 453 + 532k) \mid k \in \mathbb{Z}\}$
Let $GCD(a, b) = d$ and $p \in \mathbb{P}$ be the smallest prime number greater than d
Since p is prime, $GCD(d, p) = 1$
Using Bézout's Identity,

$$\exists x, y \in \mathbb{Z} \text{ such that } dx + py = 1$$
$$\Rightarrow dx \equiv 1 \pmod{p}$$
$$\Rightarrow x \equiv (d^{-1}) \pmod{p}$$

So, x (Bézout's coefficient of d) is d^{-1}.

For $a = -85652,\ b = 16261,$

$d = 161 \Rightarrow p = 163$

$GCD(163, 161) \longrightarrow x, y$

$= GCD(161, 2) \longrightarrow x_1, y_1$

$= 1$

Now, $161 \cdot (1) + 2 \cdot (-80) = 1$

$\Rightarrow x_1 = 1, y_1 = -80$

$x = -80, y = 1 - \left\lfloor \frac{163}{161} \right\rfloor \cdot (-80) = 81$

$163 \cdot (-80) + 161 \cdot (81) = 1$

$\therefore (161)^{-1} \pmod{163} = 81$

+5

B.2 $gcd^+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Checking if $gcd^+$is injective.

It is sufficient to show that if $\forall (a_1, b_1), (a_2, b_2) \in \mathbb{N}^2$,
$gcd^+(a_1, b_1) = gcd^+(a_2, b_2) \Rightarrow a_1 = a_2$ and $b_1 = b_2$

Take $a_1 = 2, b_1 = 4$

$\Rightarrow gcd^+(a_1, b_1) = 2$

Take $a_2 = 2, b_2 = 6$

$\Rightarrow gcd^+(a_2, b_2) = 2$

So, $\exists (a_1, b_1), (a_2, b_2) \in \mathbb{N}^2$ such that $gcd^+(a_1, b_1) = gcd^+(a_2, b_2)$ and $(a_1, b_1) \neq (a_2, b_2)$.

$\therefore gcd^+$ is not injective.

Checking if gcd^+ is surjective.

Take any $d \in \mathbb{N}$.

We need to prove that $\exists (a, b) \in \mathbb{N}^2$ such that $gcd^+(a, b) = d$.

Let $a = d, b = 2d$

$\Rightarrow gcd^+(a, b) = gcd^+(d, 2d) = d$

So, $\forall d \in \mathbb{N}, \exists (a, b) \in \mathbb{N}^2 : gcd^+(a, b) = d$.

$\therefore gcd^+$ is surjective.

+2

B.3 a

$gcd(a,b) = d$

So $a = dk_1,\ b = dk_2;\ gcd(k_1,k_2) = 1$(by definition of gcd)

$\Rightarrow a^2 = d^2k_1^2, b^2 = d^2k_2^2$

Since k_1 and k_2 are co-prime ($gcd(k_1,k_2) = 1$),

$gcd(k_1^2,k_2^2) = 1$ (No common factors)

$\Rightarrow gcd(a^2,b^2) = gcd(d^2k_1^2, d^2k_2^2) = d^2gcd(k_1^2,k_2^2) = d^2$

+3 $\therefore gcd(a^2,b^2) = d^2.$

b

Let $gcd(a+b, a-b) = c$

$\Rightarrow a+b = cd,\ a-b = ce;\ gcd(d,e) = 1$

$cd + ce = (a+b) + (a-b)$ $\quad$ $cd - ce = (a+b) - (a-b)$

$c(d+e) = 2a$ $\quad$ $c(d-e) = 2b$

$\Rightarrow c$ is a factor of $2a$ and $2b$

Since $gcd(a,b) = 1 \Rightarrow\ gcd(2a,2b) = 2$

$\Rightarrow$ c is a factor of 2

+3 $\Rightarrow c = 1$ or 2

$\therefore gcd(a+b, a-b) = 1$ or 2

c

Let $gcd(3a+2b, 2a+5b) = c$

$\Rightarrow 3a+2b = cd,\ 2a+5b = ce;\ gcd(d,e) = 1$

$c(5d-2e) = 11a$ and $c(3e-2d) = 11b$

$\Rightarrow c$ is a factor of $11a$ and $11b$

Since $gcd(a,b) = 1 \Rightarrow\ gcd(11a,11b) = 11$

$\Rightarrow c$ is a factor of 11

$\Rightarrow c = 1$ or 11

+3 $\therefore gcd(3a+2b, 2a+5b) = 1$ or 11

C. [Algebraic Structures : $3 \times 5 = 15$ points.]

Answers

C.1

$$\begin{aligned}\text{Number of binary operations} &= \prod_{(a,b)\in S} (\text{Number of ways to choose } c \in S \text{ such that } a \star b = c) \\ &= \prod_{(a,b)\in S} (n) \\ &= n^{n^2}\end{aligned}$$

$$\begin{aligned}\text{Number of commutative operations} &= \prod_{(a,a)\in S} (n) \cdot \prod_{(a,b)\in S, a<b} (n) \quad [\text{Value for } b \star a = a \star b] \\ &= (n)^n \cdot (n)^{\frac{n^2-n}{2}} \\ &= n^{\frac{n^2+n}{2}}\end{aligned}$$

+5

C.2 Let the Group be $G = (P(X), \Delta)$

1. Checking for closure

   For $A, B \in P(X) \Rightarrow A, B \subseteq X$
   $\Rightarrow A \backslash B \subseteq X, B \backslash A \subseteq X$
   $\Rightarrow (A \backslash B) \cup (B \backslash A) \subseteq X$
   $\Rightarrow (A \backslash B) \cup (B \backslash A) \in P(X)$
   $\Rightarrow A \Delta B \in P(X)$

   $\therefore \Delta$ is closed.

2. Checking for associativity

   For $A, B, C \in P(X) \Rightarrow A, B, C \subseteq X$
   Define mutually disjoint sets $a, b, c, x, y, z, t \subseteq X$:
   $a = A \backslash (B \cup C),\ b = B \backslash (C \cup A),\ c = C \backslash (A \cup B),$
   $x = (A \cap B) \backslash C,\ y = (B \cap C) \backslash A,\ z = (C \cap A) \backslash B,\ t = A \cap B \cap C$
   So, $A = a \cup x \cup y \cup t,\ B = b \cup x \cup z \cup t,\ C = c \cup y \cup z \cup t$

   $$\Rightarrow A \Delta B = ((a \cup x \cup y \cup t) \backslash (b \cup x \cup z \cup t)) \cup ((b \cup x \cup z \cup t) \backslash (a \cup x \cup y \cup t))$$
   $$= (a \cup y) \cup (b \cup z)$$
   $$= (a \cup b \cup y \cup z)$$

   $$\Rightarrow (A \Delta B) \Delta C = ((a \cup b \cup y \cup z) \backslash (c \cup y \cup z \cup t)) \cup ((c \cup y \cup z \cup t) \backslash (a \cup b \cup y \cup z))$$
   $$= a \cup b \cup c \cup t$$

   Similarly, $B \Delta C = (b \cup c \cup x \cup y)$

   $$\Rightarrow A \Delta (B \Delta C) = ((a \cup x \cup y \cup t) \backslash (b \cup c \cup x \cup y)) \cup ((b \cup c \cup x \cup y) \backslash (a \cup x \cup y \cup t))$$
   $$= a \cup b \cup c \cup t$$

   $\Rightarrow (A \Delta B) \Delta C = A \Delta (B \Delta C)$
   $\therefore \Delta$ is associative.

3. Finding identity element 1

   $A, 1 \in P(X) : A \Delta 1 = A$
   Define mutually disjoint sets $a, b, c \subseteq X$:
   $a = A \backslash 1,\ b = 1 \backslash A,\ c = A \cap 1$
   So, $A = a \cup c,\ 1 = b \cup c$
   Since $A \Delta 1 = A$,
   $((a \cup c) \backslash (b \cup c)) \cup ((b \cup c) \backslash (a \cup c)) = a \cup c$
   $\Rightarrow a \cup b = a \cup c$
   $b = c = \phi$ is a solution for this identity.

   $\therefore 1 = \phi$ exists

4. Finding inverse of A

   Let $A^{-1} \in G$ be the inverse of A $\in G$

   Define mutually disjoint sets $a, b, c \subseteq X$:

   $$a = A \backslash A^{-1},\ b = A^{-1} \backslash A,\ c = A \cap A^{-1}$$

   So, $A = a \cup c,\ A^{-1} = b \cup c$

   Using $A \Delta A^{-1} = 1$

   $((a \cup c) \backslash (b \cup c)) \cup ((b \cup c) \backslash (a \cup c)) = \phi$

   $\Rightarrow a \cup b = \phi$

   $\Rightarrow a = b = \phi$

   $\Rightarrow A = A^{-1} = c$

   $\therefore A^{-1} = A$ is the inverse of $A, \forall A \in G$.

5. Checking for commutativity

   Take $A, B \in G$

   Define mutually disjoint sets $a, b, c \subseteq X$:

   $$a = A \backslash B,\ b = B \backslash A,\ c = A \cap B$$

   So, $A = a \cup c,\ B = b \cup c$

   $$A \Delta B = ((a \cup c) \backslash (b \cup c)) \cup ((b \cup c) \backslash (a \cup c))$$
   $$= a \cup b$$

   And, $B \Delta A = ((b \cup c) \backslash (a \cup c)) \cup ((a \cup c) \backslash (b \cup c))$
   $$= b \cup a$$
   $$= a \cup b$$

   $\Rightarrow A \Delta B = B \Delta A$

   $\therefore \Delta$ is commutative.

$\therefore G = (P(X), \Delta)$ is a commutative group.

+5

C.3 Let $\phi(m) = k, \mathbb{Z}_m^* = \{a_1, a_2 \dots a_k\}$

$\Rightarrow$ By definition, $gcd(a_i, m) = 1 \ \forall \ i \in [k]$

$\forall i \in [k]$,

$\forall a \in \mathbb{Z}_m^*, \ gcd(aa_i, m) = 1 \qquad (gcd(a, m) = 1$ and $gcd(a_i, m) = 1)$

Since $\forall x \in \mathbb{Z}_m, \ gcd(x, m) = 1 \Rightarrow x \in \mathbb{Z}_m^*$(by definition) and $gcd(aa_i, m) = gcd(m, aa_i \% m)$

$\Rightarrow \exists j \in [k]$ such that $aa_i \equiv a_j \pmod m$ this part is not clear

Multiplication by a permutes a_i

$\Rightarrow (aa_1)(aa_2) \dots (aa_k) \equiv (a_1)(a_2) \dots (a_k) \pmod m$

$\Rightarrow a^k \cdot (a_1)(a_2) \dots (a_k) \equiv (a_1)(a_2) \dots (a_k) \pmod m$

Since $a_i^{-1} \pmod m$ exists $(gcd(a_i, m) = 1)$, multiplying by $(a_1^{-1})(a_2^{-1}) \dots (a_k^{-1}) \Rightarrow a^k \equiv 1 \pmod m$

$\therefore a^{\phi(m)} \equiv 1 \pmod m$

+4

D. [Symmetric Key Encryption+Classical Ciphers : 30 points.]

Answers

D.1 There are 4 types of adversarial attacks:

1. Ciphertext-Only Attack (COA)
   The attacker knows a collection of ciphertexts through which he/she tries to find the encryption key and plaintexts.
2. Known Plaintext Attack (KPA)
   The attacker knows a collection of plaintext-ciphertext pairs and uses them to find the encryption key.
3. Chosen Plaintext Attack (CPA)
   The attacker is able to obtain the corresponding ciphertexts for some chosen plaintexts, to achieve the ultimate goal of finding the encryption key.
4. Chosen Ciphertext Attack (CCA)
   The attacker already has some plaintext-ciphertext pairs and is further able to obtain the corresponding plaintexts for some chosen ciphertexts. The aim is to find the encryption key.

The weakest one among these is COA and the strongest is CCA.
To help against exploitation by CPA and CCA, randomized encryption algorithms are absolutely needed. This makes prior knowledge of plaintext-ciphertext pairs less useful. If the algorithm is deterministic, the attacker can throw some carefully crafted plaintexts(ciphertexts) and obtain the ciphertexts(plaintexts) making it easy to recover the key.

+3

signifcance of these attack models?

D.2 Finding frequency of characters in c and sorting by it yields:

letter	frequency
q	10
h	7
c	6
b	5
w	5
r	5
v	4
n	3
l	3
i	2
d	2
j	1
a	1
s	1
e	1
z	1

It is clear to see that q can be mapped to e since it is most frequent by a significant difference.
h could be mapped to t, the next frequent letter. However, it is seen that h also appears in the middle of a few words, hinting that it is a vowel. So we will map it to a, the next frequent vowel.
c has a high frequency and appears only at ends of words and sometimes in doublets, indicating that it is a consonant and it could be l
Current state after replacing the mappings with uppercase letters : *iE ifLL vEEr fb rdE vfccLE nh rdE LfjwAwz Ar bnnbALL AwwAbsEvEbre AwE vAcE*
On hit and trial, the first two words only make sense if i is replaced by w and then f is mapped to i.
Current state after replacing the mappings with uppercase letters : *WE WILL vEEr Ib rdE vIccLE nh rdE LIjwAwz Ar bnnbALL AwwAbsEvEbre AwE vAcE*
Ar should be mapped to *AT* to make sense. So, r is t.
Doing similar analysis and hit and trials, the plain text comes to be:
we will meet in the middle of the library at noon all arrangements are made

+4

D.3 Inverse permutation $\sigma^{-1}(\cdot)$ is:

+2

y	1	2	3	4	5	6
$\sigma^{-1}(y)$	4	6	2	3	1	5

Computing the permutation matrix K_σ,

$$K_\sigma = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

+4

Computing the permutation matrix $K_{\sigma^{-1}}$,

$$K_{\sigma^{-1}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Taking blocks of $t = 6$

$m_0 = \begin{bmatrix} 9 & 20 & 9 & 19 & 20 & 18 \end{bmatrix}$ $(itistr)$

$$\Rightarrow c_0 = m_0 \cdot K_\sigma = \begin{bmatrix} 9 & 20 & 9 & 19 & 20 & 18 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 19 \\ 18 \\ 20 \\ 9 \\ 9 \\ 20 \end{bmatrix} \quad (srtiit)$$

right multiply K_sigma to column vector m_0

$m_1 = \begin{bmatrix} 21 & 5 & 20 & 8 & 1 & 20 \end{bmatrix}$ $(uethat)$

$$\Rightarrow c_1 = m_1 \cdot K_\sigma = \begin{bmatrix} 21 & 5 & 20 & 8 & 1 & 20 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 8 \\ 20 \\ 5 \\ 20 \\ 21 \\ 1 \end{bmatrix} \quad (htetua)$$

0

$$\Rightarrow c_2 = m_2 \cdot K_\sigma = \begin{bmatrix} 20 & 8 & 9 & 19 & 16 & 18 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 19 \\ 18 \\ 8 \\ 9 \\ 20 \\ 16 \end{bmatrix} \quad (srhitp)$$

$$\Rightarrow c_3 = \begin{bmatrix} 15 & 16 & 15 & 19 & 9 & 20 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 19 \\ 15 \\ 19 \\ 15 \\ 20 \\ 16 \end{bmatrix} \quad (stpooi)$$

$$\Rightarrow c_4 = \begin{bmatrix} 9 & 15 & 14 & 9 & 19 & 14 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 19 \\ 14 \\ 9 \\ 9 \\ 15 \end{bmatrix} \quad (inonis)$$

$$\Rightarrow c_5 = \begin{bmatrix}15 & 20 & 20 & 18 & 21 & 5\end{bmatrix} \cdot \begin{bmatrix}0&0&0&1&0&0\\0&0&0&0&0&1\\0&1&0&0&0&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&1&0\end{bmatrix} = \begin{bmatrix}21\\20\\18\\15\\5\\20\end{bmatrix} \quad \text{(rettou)}$$

$\therefore$ Ciphertext: sr ti itht etua srhi tpstpooiino ni sre ttou

To decrypt, taking $t = 6$

$$m_0 = c_0 \cdot K_\sigma^{-1} = \begin{bmatrix}19 & 1 & 20 & 9 & 9 & 20\end{bmatrix} \cdot \begin{bmatrix}0&0&0&0&1&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&1&0&0&0&0\end{bmatrix} = \begin{bmatrix}9\\20\\9\\19\\20\\18\end{bmatrix} \quad \text{(itistr)}$$

$$m_1 = c_1 \cdot K_\sigma^{-1} = \begin{bmatrix}8 & 20 & 5 & 20 & 21 & 1\end{bmatrix} \cdot \begin{bmatrix}0&0&0&0&1&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&1&0&0&0&0\end{bmatrix} = \begin{bmatrix}21\\5\\20\\8\\1\\20\end{bmatrix} \quad \text{(uethat)}$$

$$m_2 = \begin{bmatrix}19 & 18 & 8 & 9 & 20 & 16\end{bmatrix} \cdot \begin{bmatrix}0&0&0&0&1&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&1&0&0&0&0\end{bmatrix} = \begin{bmatrix}20\\8\\9\\19\\16\\18\end{bmatrix} \quad \text{(thispr)}$$

$$m_3 = \begin{bmatrix}15\\16\\15\\19\\9\\20\end{bmatrix} \quad \text{(oposit)}$$

$$m_4 = \begin{bmatrix}9\\15\\14\\9\\19\\14\end{bmatrix} \quad \text{(ionisn)}$$

0

$$m_5 = \begin{bmatrix}15\\20\\20\\18\\21\\5\end{bmatrix} \quad \text{(ottrue)}$$

$\therefore m =$ *it is true that this proposition is not true*

$\Rightarrow$ Decryption verified.

D.4 Computing order of $GL_t(\mathbb{Z}_p)$

Let $A = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_t \end{bmatrix} \in GL_t(\mathbb{Z}_p),\ v_i \in {\mathbb{Z}_p}^n\ \forall\ i \in [t]$

Number of ways to choose $v_1 = p^t - 1$ (Excluding zero vector)
Number of ways to choose $v_2 = p^t - p$ (Excluding multiples of v_1)
$\vdots$
Number of ways to choose $v_n = p^t - p^{t-1}$
Number of ways to choose $A = (p^t - 1)(p^t - p)\dots(p^t - p^{t-1})$
$\therefore$ order of $GL_t(\mathbb{Z}_p) = (p^t - 1)(p^t - p)\dots(p^t - p^{t-1})$

+2 Order of $GL_2(\mathbb{Z}_{26}) = (26^2 - 1) \cdot (26^2 - 26) = 438750$

$$\begin{aligned}\text{Number of valid keys with even determinants} &= \text{Number of valid keys with at least 1 even row} \\ &= 2 \cdot (13^2 - 1) \cdot (26^2 - 13^2) + (13^2 - 1) \cdot (13^2 - 26) \\ &= 2 \cdot 168 \cdot 169 + 168 \cdot 143 \\ &= 194376\end{aligned}$$

+3 There are 194376 valid keys with even determinants.

Computing the number for $GL_2(\mathbb{Z}_p)$

$$\begin{aligned}\text{Number of valid keys with even determinants} &= \text{Number of valid keys with at least 1 even row} \\ &= 2 \cdot (\left\lceil \frac{p}{2} \right\rceil^2 - 1) \cdot (p^2 - \left\lfloor \frac{p}{2} \right\rfloor^2) + (\left\lceil \frac{p}{2} \right\rceil^2 - 1) \cdot (\left\lceil \frac{p}{2} \right\rceil^2 - p) \\ &= 2 \cdot (\left\lceil \frac{p}{2} \right\rceil^2 - 1) \cdot (p^2 - (p - \left\lceil \frac{p}{2} \right\rceil)^2) + (\left\lceil \frac{p}{2} \right\rceil^2 - 1) \cdot (\left\lceil \frac{p}{2} \right\rceil^2 - p) \\ &= 4 \cdot p \cdot \left\lceil \frac{p}{2} \right\rceil^3 - \left\lceil \frac{p}{2} \right\rceil^4 - 4 \cdot p \cdot \left\lceil \frac{p}{2} \right\rceil - (p-1) \cdot \left\lceil \frac{p}{2} \right\rceil^2 + p\end{aligned}$$

+5