עבודת 1:

שאלה 1
יהיו $a,b,c \in \mathbb{Z}$ ונכתוב כי $b \mid a$ כדי לציין ש a מחלק את b **ללא** שארית, כלומר קיים שלם q כך ש: $b = qa$.
הוכיחו את הטענות הבאות.

א) אם $d = \gcd(a,b)$ אז $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

ב) אם $a \mid c$ וגם $b \mid c$ וגם $\gcd(a,b) = 1$ אז $ab \mid c$.

ג) אם $a \mid bc$ ו- $\gcd(a,b) = 1$ אז $a \mid c$.

ד) יהי p ראשוני כלשהו כך ש- $p \mid ab$ אזי $p \mid a$ או $p \mid b$.

ה) יהי $m \neq 0$ אז $a \mid b$ אם ורק אם $ma \mid mb$.

שאלה 2
יהיו a,b מספרים שלמים זרים. הוכיחו כי כל מחלק ראשוני משותף של $a^2 + b^2$ ו- $a+b$ שייך לקבוצה $\{1,2\}$.

שאלה 3
יהיו a,b,n שלמים חיוביים. הוכיחו כי $\gcd(a^n, b^n) = \gcd(a,b)^n$.

שאלה 4
(10 נקודות)
נתון את הטקסט מוצפן

ETCLPRLWCTGGVVCSIKASLAVFL

אשר מוצפן על ידי צופן ויז'נר עם המפתח SPY. מצאו את הטקסט גלוי.

שאלה 5
(10 נקודות)
נתון הטקסט מוצפן

PEBUSSPZIIDUKOEKIPEONUSS

אשר מוצפן על ידי צופן אפיני עם המפתח $a = 23, b = 20$. מצאו את הטקסט גלוי.

שאלה 6
נתון צופן עם כלל מצפין $e_k(x)$ וכלל מפענח $d_k(y)$. אומרים כי הצופן ניתן לפענוח אם ורק אם $d_k(e_k(x)) = x \bmod 26$ לכל $x \in \mathbb{Z}_{26}$.

א) הוכיחו כי צופן האפיני ניתן לפענות.

ב) הוכיחו כי צופן היל ניתן לפענות.

שאלה 7

א) יהי $e_k(x) = 23x + 28 \bmod 30$ צופן האפיני מעל אלפבית בת 30 אותיות. מצאו את הכלל מפענח.

ב) חשבו כמה מפתחות האפשריות קיימות של צופן האפיני מעל אלפיבית בת m אותיות.

שאלה 8

(10 נקודות)

נתון הטקסט מוצפן

`YZUSKKOPE`

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} .$$

מצאו את הטקסט גלוי.

פתרונות

שאלה 1

א) נניח ש: $\gcd(a,b)=d$. אזי קיימים שלמים x,y עבורם

$$xa+yb=d\ .$$

מכיוון ש- $d=\gcd(a,b)$ אזי $a \mid d$ וגם $b \mid d$ לכן

$$x\left(\frac{a}{d}\right)+y\left(\frac{b}{d}\right)=1$$

ז"א קיימים שלמים x,y כך ש: $x\left(\frac{a}{d}\right)+y\left(\frac{b}{d}\right)=1$ ולכן לפי משפט בזו $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$.

ב) נניח ש: $c \mid a$ וגם $c \mid b$ וגם $\gcd(a,b)=1$.
ז"א קיימים שלמים q ו- k עבורם $c=ak$ ו- $c=bq$.

צריך להוכיח כי קיים m שך ש: $c=mab$.

ידוע כי $\gcd(a,b)=1$ ולכן לפי משפט בז'ו ניתן לרשום $1=ax+by$.
ולכן

$$\begin{aligned}
c =&(c)(1)\\
=&c(xa+yb)\\
=&cxa+cyb\\
=&(bq)(ax)+(ak)(by)\\
=&ab\,(qx+ky)\ .
\end{aligned}$$

ולכן עבור $m=(qx+ky)$ נקבל את מה שצריך להוכיח.

ג) ידוע כי $\gcd(a,b)=1$ ולכן לפי משפט בז'ו קיימים שלמים n,m עבורם

$$an+bm=1\ .$$

כמו בסעיף הקודם, נרשום

$$c=(c)(1)=c\,(an+bm)=can+cbm\ .$$

נשים לב כי $a \mid can$. והיות ונתון $a \mid bc$ מתקיים $a \mid cmb$ ולכן $a \mid (can+cmb)=c$.

ד) אם $a \mid p$ סיימנו ולכן נניח כי p לא מחלק את a.
היות ו- p ראשוני מתקיים $\gcd(a,p)=1$ ולכן לפי סעיף ג' נקבל $b \mid p$.

ה) כיוון ראשון:

נניח $b \mid a$ ונראה $ma \mid mb$.

ידוע כי קיים שלם k כך ש: $b = ak$.

נשים לב כי
$$mb = m(ak) = (ma)k$$

ולכן $ma \mid mb$.

כיוון שני :

נניח $ma \mid mb$ ונראה $a \mid b$.

ידוע כי קיים שלם q כך ש: $mb = q(ma)$.

וידוע כי $m \neq 0$ ולכן $b = aq$ ולכן $a \mid b$.

שאלה 2 נניח ש- a, b זרים. אזי $\gcd(a, b) = 1$. יהי p מספר ראשוני שמחלק $a^2 + b^2$ וגם $a + b$.

$\Leftarrow$ אם $p \mid (a + b)$ אזי $p \mid (a + b)^2$.

$\Leftarrow$ $p \mid (a + b)^2$ וגם $p \mid (a^2 + b^2)$.

$\Leftarrow$ $p \mid (a + b)^2 - (a^2 + b^2)$

$\Leftarrow$ $p \mid 2ab$.

מכאן יש 3 מקרים:

1) $p \mid a$,
2) $p \mid b$,
3) $p \mid 2$.

1) נניח ש- $p \mid a$. מכיוון שנתון בשאלה כי $p \mid (a + b)$ אזי $p \mid [(a + b) - a]$, ולכן $p \mid b$.
אז מצאני שאם $p \mid a$ אז גם $p \mid b$ ומכיוון ש- $\gcd(a, b) = 1$ אז בהכרח $p = 1$.

2) כעת נניח ש- $p \mid b$. מכיוון שנתון בשאלה כי $p \mid (a + b)$ אזי $p \mid [(a + b) - b]$, ולכן $p \mid a$.
אז מצאני שאם $p \mid b$ אז גם $p \mid a$ ומכיוון ש- $\gcd(a, b) = 1$ אז בהכרח $p = 1$.

3) נניח ש- $p \mid 2$. בגלל ש- p ראשוני אזי $p = 1$ או $p = 2$.

לכן הוכחנו שהאפשרויות ל- p הן $p=1$ או $p=2$, כנדרש.

שאלה 3 יהי $d=\gcd(a,b)$. ז"א $d \mid a$ וגם $d \mid b$. לכן קיימים שלמים q_1,q_2 עבורם

$$a=q_1 d\ ,\quad b=q_2 d\ .$$

מכאן

$$\gcd(q_1,q_2)=\gcd\left(\frac{a}{d},\frac{b}{d}\right)\overset{\text{שאלה 1א'}}{=}1$$

ז"א q_1,q_2 לא חולקים גורמים משותפים (לפי פירוק לגורמים לראשוניים) ולכן גם

$$\gcd(q_1^n,q_2^n)=1\ .$$

נשים לב:

$$\begin{aligned}\gcd(a^n,b^n)&=\gcd(q_1^n d^n,q_2^n d^n)\\&=d^n\gcd(q_1^n,q_2^n)\\&=d^n\\&=\gcd(a,b)^n\ .\end{aligned}$$

שאלה 4 הטקסט מוצפן הוא:

	E	T	C	L	P	R	L	W	C	T	G	G	V	V	C	S	I	K	A	S	L	A	V	F	L
y	4	19	2	11	15	17	11	22	2	19	6	6	21	21	2	18	8	10	0	18	11	0	21	5	11

המפתח הוא

$$k_1=18\ ,\quad k_2=15\ ,\quad k_3=24\ .$$

הכלל מפענח הוא

$$d_k(y_i)=y_i-k_{i \bmod 3+1} \mod 26$$

	E	T	C	L	P	R	L	W	C	T	G	G	V	V	C	S	I	K	A	S	L	A	V	F	L
y	4	19	2	11	15	17	11	22	2	19	6	6	21	21	2	18	8	10	0	18	11	0	21	5	11
x	12	4	4	19	0	19	19	7	4	1	17	8	3	6	4	0	19	12	6	3	13	8	6	7	19
	m	e	e	t	a	t	t	h	e	b	r	i	d	g	e	a	t	m	i	d	n	i	g	h	t

לכן הטקסט הגלוי הוא

```
meet at the bridge at midnight
```

שאלה 5 הכלל מצפין של צופן אפיני הינו $e_k(x)=ax+b \bmod 26$ לכל $x\in\mathbb{Z}_{26}$ והכלל מפענח הוא $d_k(y)=a^{-1}(y-b) \bmod 26$ לכל $y\in\mathbb{Z}_{26}$. בדוגמה הזו $a=23$ ו- $b=20$. לכן:

$$d_k(y)=a^{-1}(y-b) \bmod 26=23^{-1}(y-20) \bmod 26\ .$$

לפי הדף הנוסחאות האיבר ההופכי של 23 ב- $\mathbb{Z}_{26}$ הוא 17. לסיכך:

$$d_k(y)=17(y-20) \bmod 26=17y-340 \bmod 26=17y+24 \bmod 26\ .$$

הערכים של הטקסט מוצפן הם כמפורט בטבלה למטה:

y	P	E	B	U	S	S	P	Z	I	I	D	U	K	O	E	K	I	P	E	O	N	U	S	S
y	15	4	1	20	18	18	15	25	8	8	3	20	10	14	4	10	8	15	4	14	13	20	18	18

נחשב את הערכים של האותיות של הטקסט הגלוי בעזרת הכלל מפענח:

$$\begin{aligned}
d_k(\mathtt{P}) &= d_k(15) = 17(15) + 24 \bmod 26 = 279 \bmod 26 &&= 19 = \mathtt{t}\\
d_k(\mathtt{E}) &= d_k(4) = 17(4) + 24 \bmod 26 = 92 \bmod 26 &&= 14 = \mathtt{o}\\
d_k(\mathtt{B}) &= d_k(1) = 17(1) + 24 \bmod 26 = 41 \bmod 26 &&= 15 = \mathtt{p}\\
d_k(\mathtt{U}) &= d_k(20) = 17(20) + 24 \bmod 26 = 364 \bmod 26 &&= 0 = \mathtt{a}\\
d_k(\mathtt{S}) &= d_k(18) = 17(18) + 24 \bmod 26 = 330 \bmod 26 &&= 18 = \mathtt{s}\\
d_k(\mathtt{Z}) &= d_k(18) = 17(25) + 24 \bmod 26 = 459 \bmod 26 &&= 17 = \mathtt{r}\\
d_k(\mathtt{I}) &= d_k(18) = 17(8) + 24 \bmod 26 = 160 \bmod 26 &&= 4 = \mathtt{e}\\
d_k(\mathtt{D}) &= d_k(3) = 17(3) + 24 \bmod 26 = 75 \bmod 26 &&= 23 = \mathtt{x}\\
d_k(\mathtt{K}) &= d_k(10) = 17(10) + 24 \bmod 26 = 194 \bmod 26 &&= 12 = \mathtt{m}\\
d_k(\mathtt{O}) &= d_k(14) = 17(14) + 24 \bmod 26 = 262 \bmod 26 &&= 2 = \mathtt{c}\\
d_k(\mathtt{N}) &= d_k(14) = 17(13) + 24 \bmod 26 = 245 \bmod 26 &&= 11 = \mathtt{l}
\end{aligned}$$

y	P	E	B	U	S	S	P	Z	I	I	D	U	K	O	E	K	I	P	E	O	N	U	S	S
y	15	4	1	20	18	18	15	25	8	8	3	20	10	14	4	10	8	15	4	14	13	20	18	18
x	19	14	15	0	18	18	19	7	4	4	23	0	12	2	14	12	4	19	14	2	11	0	18	18
x	t	o	p	a	s	s	t	h	e	e	x	a	m	c	o	m	e	t	o	c	l	a	s	s

לכן הטקסט הגלוי הוא:

`to pass the exam come to class.`

שאלה 6

א) הכלל מצפין של צופן אפיני הינו $e_k(x) = ax + b \bmod 26$ לכל $x \in \mathbb{Z}_{26}$ כאשר $a, b \in \mathbb{Z}_{26}$ כך ש- $\gcd(a, 26) = 1$. הכלל מפענח הוא $d_k(y) = a^{-1}(y - b) \bmod 26$ לכל $y \in \mathbb{Z}_{26}$.

ראשית נציין משפט הקיום איבר הופכי בחוג $\mathbb{Z}_m$ כאשר m שלם כלשהו:
לכל $a \in \mathbb{Z}_m$ קיים איבר ההופכי a^{-1} אם ורק אם $\gcd(a, m) = 1$.
ז"א מכיוון ש- $\gcd(a, 26) = 1$ $\Leftarrow$ קיים ההופכי $a^{-1} \in \mathbb{Z}_{26}$ $\Leftarrow$ הכלל מפענח קיים.

הוכחנו שקיים כלל מפענח. כעת נוכיח כי $d_k(e_k(x)) = x \bmod 26$ לכל $x \in \mathbb{Z}_{26}$:
יהי $y = e_k(x) = ax + b \bmod 26$.
נפעיל הכלל מפענח על y:

$$d_k(y) = a^{-1}(y - b) \bmod 26 \ .$$

נציב $y = ax + b \bmod 26$:

$$d_k(y) = a^{-1}\left([ax + b \bmod 26] - b\right) \bmod 26 = a^{-1}\left(ax + b - b\right) \bmod 26 = a^{-1}\left(ax\right) \bmod 26 = a^{-1}ax \bmod 26 \ .$$

לפי ההגדרה של a^{-1}, מתקיים $a^{-1}a \bmod 26 = 1$ לכן

$$d_k(y) = x \bmod 26 \ .$$

לבסוף נחזיר את $y = e_k(x)$ ואז נקבל

$$d_k\left(e_k(x)\right) = x \bmod 26 \ .$$

כנדרש.

ב) הכלל מצפין של צופן היל הינו $e_k(x) = xk \bmod 26$ לכל $x \in \mathbb{Z}_{26}^n$ כאשר $k \in \mathbb{Z}_{26}^{n\times n}$ כך ש- $\gcd(\det k, 26) = 1$. הכלל מפענח הוא $d_k(y) = yk^{-1} \bmod 26$ לכל $y \in \mathbb{Z}_{26}^n$.

ראשית נציין כי לפי הנוסחה למטריצה ההפוכה:

$$k^{-1} = (\det k)^{-1}\, C^t \bmod 26$$

כאשר C המטריצה של קופקטורים של k ו- $(\det k)^{-1}$ האיבר ההופכי של $\det k$ ב- $\mathbb{Z}_{26}$. לפי משפט הקיום איבר הופכי, $(\det k)^{-1}$ קיים אם ורק אם $\gcd(\det k, 26) = 1$ לכן תנאי הכרחי לקיום כלל מפענח הוא ש: $\gcd(\det k, 26) = 1$. הוכחנו שקיים כלל מפענח. כעת נוכיח כי $d_k\left(e_k(x)\right) = x \bmod 26$ לכל $x \in \mathbb{Z}_{26}$. יהי $x \in \mathbb{Z}_{26}^n$ וקטור שורה באורך n. אם $k \in \mathbb{Z}_{26}^{n\times n}$ עבורו $\gcd(\det k, 26) = 1$ מתקיים:

$$\begin{aligned} d_k\left(e_k(x)\right) &= d_k\left(xk \bmod 26\right) \bmod 26 \\ &= d_k\left(xk\right) \bmod 26 \\ &= \left(xk\right) k^{-1} \bmod 26 \\ &= xkk^{-1} \bmod 26 \\ &= x \bmod 26 \ . \end{aligned}$$

שאלה 7

א) הכלל מצפין הוא מעל אלפבית בת 30 אותיות:

$$e_k(x) = ax + b \bmod 30$$

לכל $x \in \mathbb{Z}_{30}$ כאשר $a, b \in \mathbb{Z}_{30}$ כך ש- $a = 23$, $b = 28$. הכלל מפענח הוא

$$d_k(y) = a^{-1}(y - b) \bmod 30$$

כאשר a^{-1} הוא האיבר ההופכי של 23 של $\mathbb{Z}_{30}$. נחשב אותו באמצעות האלגוריתם לאיבר ההופכי:

Algorithm 1 האלגוריתם לאיבר ההופכי

Input: Integers A, B .
$r_0 \leftarrow A$
$r_1 \leftarrow B$
$t_0 \leftarrow 0$
$t_1 \leftarrow 1$
$n \leftarrow 1$
while $r_n \neq 0$ **do**
    $q_n \leftarrow \left\lfloor \dfrac{r_{n-1}}{r_n} \right\rfloor$
    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$
    $n \leftarrow n+1$
end while
$n \leftarrow n-1$
if $r_n \neq 1$ **then**
    B has no inverse modulo A
else
    return: t_n ▷ $t_n = B^{-1} \pmod{A}$
end if

נשים $A = 30, B = 23$. נאתחל את המשתנים של האלגוריתם:

$$r_0 = A = 30 \ , \qquad r_1 = B = 23 \ ,$$
$$t_0 = 0 \ , \qquad t_1 = 1 \ .$$

אזי האיטרציות של האלגוריתם הם כמפורט למטה:

שלב $n = 1$:	$t_2 = 0 - 1 \cdot 1 = -1$	$r_2 = 30 - 1 \cdot 23 = 7$	$q_1 = 1$
שלב $n = 2$:	$t_3 = 1 - 3 \cdot (-1) = 4$	$r_3 = 23 - 3 \cdot 7 = 2$	$q_2 = 3$
שלב $n = 3$:	$t_4 = -1 - 3 \cdot (4) = -13$	$r_4 = 7 - 3 \cdot 2 = 1$	$q_3 = 3$
שלב $n = 4$:	$t_5 = 4 - 2 \cdot (-13) = 30$	$r_5 = 2 - 2 \cdot 1 = 0$	$q_4 = 2$

לכן ההאיבר ההופכי של 23 ב- $\mathbb{Z}_{30}$ הוא $t_4 = -13 \pmod{30} = 17 \pmod{30}$. לפיכך האיבר ההופכי של 23 ב- $\mathbb{Z}_{30}$ הוא 17. לכן:

$$d_k(y) = 23^{-1}(y-28) \bmod 30 = 17(y-28) \bmod 30 = 17y - 476 \bmod 30 = 17y + 4 \bmod 30 \ .$$

ב) קיים כלל מפענח $\iff$ קיים $a^{-1} \in \mathbb{Z}_{30}$ $\iff$ $\gcd(a,30)=1$. המספר האיברים זרים ביחס ל- 30 נתון ע"י הפונקציית אוילר $\phi(30)$. הפירוק לראשונים של 30 הוא

$$30 = (2^1)(3^1)(5^2) \ .$$

לכן:

$$\phi(30) = (2^1-2^0)(3^1-3^0)(5^1-5^0) = 8 \ .$$

לפיכך מספר המפתחות הוא:

$$b\phi(a) = (28)(8) = 224 \ .$$

שאלה 8

y $\in C$	Y	Z	U	S	K	K	O	P	E
$y \in \mathbb{Z}_{26}$	24	25	20	18	10	10	14	15	4

הדטרמיננטה של k היא $\det\ k \bmod 26 = 25$.
$\gcd(25,26)=1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 16 & 10 \\ 17 & 15 \end{vmatrix} \bmod 26 = 70 \bmod 26 = 18 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 13 & 10 \\ 20 & 15 \end{vmatrix} \bmod 26 = 5 \bmod 26 = 5 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 13 & 16 \\ 20 & 17 \end{vmatrix} \bmod 26 = -99 \bmod 26 = 5 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 24 & 1 \\ 17 & 15 \end{vmatrix} \bmod 26 = -343 \bmod 26 = 21 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 6 & 1 \\ 20 & 15 \end{vmatrix} \bmod 26 = 70 \bmod 26 = 18 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 6 & 24 \\ 20 & 17 \end{vmatrix} \bmod 26 = 378 \bmod 26 = 14 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \qquad \Rightarrow \qquad C_{31} = (-1)^{3+1} \begin{vmatrix} 24 & 1 \\ 16 & 10 \end{vmatrix} \bmod 26 = 224 \bmod 26 = 16 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \qquad \Rightarrow \qquad C_{32} = (-1)^{3+2} \begin{vmatrix} 6 & 1 \\ 13 & 10 \end{vmatrix} \bmod 26 = -47 \bmod 26 = 5 \ .$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \qquad \Rightarrow \qquad C_{33} = (-1)^{3+3} \begin{vmatrix} 6 & 24 \\ 13 & 16 \end{vmatrix} \bmod 26 = -216 \bmod 26 = 18 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 18 & 5 & 5 \\ 21 & 18 & 14 \\ 16 & 5 & 18 \end{pmatrix} \ .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix} \ .$$

$$k^{-1} \bmod 26 = (\det\ k)^{-1}\, \text{adj}(k) \ .$$

$$(\det\ k)^{-1} \bmod 26 = 25^{-1} \bmod 26 = 25 \ .$$

$$k^{-1} = 25 \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix} = \begin{pmatrix} 450 & 525 & 400 \\ 125 & 450 & 125 \\ 125 & 350 & 450 \end{pmatrix} \bmod 26 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

$$(24, 25, 20) \cdot k^{-1} = (1137, 560, 925) \bmod 26 = (19, 14, 15)$$

$$(18, 10, 10) \cdot k^{-1} = (564, 290, 470) \bmod 26 = (18, 4, 2)$$

$$(14, 15, 4) \cdot k^{-1} = (511, 238, 487) \bmod 26 = (17, 4, 19)$$

y $\in C$	Y	Z	U	S	K	K	O	P	E
$y \in \mathbb{Z}_{26}$	24	25	20	18	10	10	14	15	4
$x \in \mathbb{Z}_{26}$	19	14	15	18	4	2	17	4	19
x $\in P$	t	o	p	s	e	c	r	e	t