

קריפטוגרפיה למדמ"ח

מועד א'
ד"ר ירמיהו מילר.

תשפ"ו סמסטר א'

השאלון מכיל 4 עמודים (כולל עמוד זה).

בצלחה!

הנחיות לסטודנטים כולל חומר עזר

- ניתן להשתמש במחשבון מדעי לא גרפי עם צג קטן.
- ניתן להשתמש בדף נוסחאות (13 עמודים בפורמט A4) מצורפים לשאלון.
- יש לענות על השאלות במחברת בלבד.

הנחיות למדור בחינה

- לשאלון הבחינה יש לצרף מחברת.

אחר / הערות

- סטודנטים במתווה רגיל: נדרש לפתרו 4 מתוך השאלות 1 עד 5.
- סטודנטים במתווה **מילואים**: נדרש לפתרו 4 מתוך השאלות 1 עד 6.
- יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר ולא נימוק, אפילו נכון, לא תתקבל.
- סדר התשובות אינו משנה, אך יש לרשום ליד כל תשובה את מספרה.
- יש לרשום בראש המחברת أيזה שאלות לבדוק.

שאלה 1 (25 נקודות)

$$k = (p = 41, \quad a = 30, \quad \alpha = 13, \quad d = 4) .$$

א) (8 נק')

נתון הטקסט גליי $x = 12$. אליס מצפינה את הטקסט גליי זהה עם צופן El-Gamal ועם המפתח k . הוכחו כי הטקסט המוצפן המתקבל הוא $(y_1, y_2) = (25, 12)$.

ב) (8 נק')

ובב מקבל את הטקסט המוצפן ואת המפתח הציבורי מלאיס והוא מפענח את הטקסט המוצפן. הוכחו כי הטקסט גליי שהוא מקבל הוא $x = 12$.

ג) (4 נק')

הוכחו את הטענה הבאה:
אם m, a, b מספרים שלמים חיוביים אז

$$((a + b) \bmod m - b) \bmod m = a \bmod m .$$

ד) (5 נק') הוכחו כי צופן אפיני ניתן לפענוח.

כלומר, יהיו $e_k(x)$ הכלל מצפין של צופן אפיני ויהי $d_k(y)$ הכלל מפענח של צופן אפיני. הוכחו כי

$$d_k(e_k(x)) = x \bmod 26$$

לכל $x \in \mathbb{Z}_{26}$

שאלה 2 (25 נקודות)

א) (13 נק')

תהי X האלפבית $\{a, b, c, d, e, f\}$ ותהי פונקציית ההסתברות של האלפבית X

$$\begin{aligned} P_X(a) &= \frac{1}{12}, & P_X(b) &= \frac{1}{48}, & P_X(c) &= \frac{1}{8}, \\ P_X(d) &= \frac{7}{48}, & P_X(e) &= \frac{7}{24}, & P_X(f) &= \frac{1}{3}. \end{aligned}$$

מצאו הצפנה בינהרית של האלפבית X עבורה תוחלת אוריך ההצפנה של האותיות תהיה מינימלית.

ב) (12 נק')

יהי m מספרשלם חיובי. הוכחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
 m מספר ריבועי אם ורק אם כל מספר ראשוןי בפרק ראשוןונים של m מופיע בחזקה זוגית.

שאלה 3 (25 נקודות)

א) (12 נק')

בוב מקבל את הטקסט מוצפן $y = 41$ מאليس שהוצפן ע"י צופן RSA עם המפתח הציבורי (n, e) אשר $n = pq$, $p = 7$, $q = 13$. חשבו את הטקסט גלי המקורי אשר אליס שלחה לבוב.

ב) (6 נק')

הוכחו כי צופן El-Gamal ניתן לפענוח. כלומר, אם $e_k(x) = (y_1, y_2)$ הוא הכלל מצפין של צופן El-Gamal אז הכלל מפענה של צופן El-Gamal איזי $x = d_k(y_1, y_2)$.

$$d_k(e_k(x)) = x \bmod p$$

כאשר p מספר ראשוני.

ג) (7 נק')

תהי $\Sigma \rightarrow \Sigma$: π תמורה מעל אלפבית Σ . הוכחו את הטענה הבאה:
אם π היא מחזור של אורך k אז $\text{id} = \pi^k$.

שאלה 4

א) (11 נק')

אליס שולחת לבוב את הטקסט המוצפן VMUHBB אשר הוצפן ע"י צופן היל עם המפתח $.k = \begin{pmatrix} 3 & 14 \\ 7 & 9 \end{pmatrix}$.
חשבו את הטקסט גלי המקורי של הטקסט המוצפן זהה.

ב) (10 נק')

נתונות התמורות כפولات הבאות של צופן אניגמה:

$$\Delta_4\Delta_1 = (\text{JNVU}) (\text{ZRTE}) (\text{GCXKSYMPI}) (\text{ALHOFWDQ}) ,$$

$$\Delta_5\Delta_2 = (\text{HO}) (\text{XG}) (\text{DJEYT}) (\text{MZIBL}) (\text{FVPRNW}) (\text{AQCSUK}) ,$$

$$\Delta_6\Delta_3 = (\text{MOS}) (\text{CNK}) (\text{BXZW}) (\text{TGAP}) (\text{FLIYJV}) (\text{QHDREU}) .$$

התמורות $\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6$ הן בסדר ריבסקי. נתנו הטקסט הבא שהוצפן ע"י צופן אניגמה:

PIWVBY

חשבו את הטקסט המקורי.

ג) (4 נק')

יהיו a, b, m שלמים חיוביים. הוכחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:

$$\gcd(ma, mb) = m \gcd(a, b) .$$

שאלה 5 (25 נקודות)
א) (10 נק')

אליס שולחת את הטקסט המוצפן הבא לבוב:

FMBBMYOMIXPXKEWS .

הtekst המוצפן ע"י צופן אפיני עם המפתח ($a = 21, b = 4$). חשבו את הטקסט גלי המקורי אשר אליס שלחה לבוב.

ב) (8 נק')

תהי $e_k(x) = (ax + b) \bmod m$ כלל מצipher של צופן אפיני מעל אלפבית של m אותיות. הוכחו את הטענה הבאה:
 קיימים כלל מפענה $d_k(y)$ המקיים את התנאי $d_k(e_k(x)) \bmod m$ אם ורק אם $\gcd(a, m) = 1$.

ג) (7 נק')

יהיו a, b, c שלמים חיוביים. הוכחו את הטענה הבאה:
 אם a, b לא זרים אז לא קיים c עבורו $ac \equiv 1 \pmod{b}$.

שאלה 6 (25 נקודות) שאלת בחירה לסטודנטים במתווה מילואים בלבד
א) (13 נקודות)

נתון הטקסט מוצפן

PEBUSSPZIIDUKOEKIPEONUSS

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

ב) (12 נקודות) יהיו a, b, n שלמים חיוביים. הוכחו כי $\gcd(a^n, b^n) = \gcd(a, b)^n$.

תוכן העניינים

5	1 תורת המספרים
7	2 חוגים
8	3 צפוני בסיסיים
9	4 צופן RSA
10	5 צופן ElGamal
10	6 צופן אניגמה
12	7 תורת שאנו וסודות מושלמת
13	8 צופן פיביטל
14	9 צופן IDEA
15	10 צופן DES

1 תורת המספרים

$a \equiv b \pmod{m}$ אם ורק אם קיימים שלמים q, r כך ש $a = qm + r$ ו $m | m - b$.
 קיימים שלמים q, r כך ש: $a = qb + r$, $0 \leq r < |b|$.
 אם a, b שלמים חיוביים אז השארית של a בחלוקת b , מסומנת ב- $a \bmod b$.

משפט החלוקת של אוקלידס: לכל זוג שלמים a, b קיימים שלמים q, r כך ש: $a = qb + r$, $0 \leq r < |b|$.

אם $a, b \geq 0$ אז $q = \left\lfloor \frac{a}{b} \right\rfloor$ ו- $r = a \bmod b$.

האלגוריתם של אוקלידס: לכל שלמים $a, b \geq 0$ האלגוריתם הבא נותן את $\gcd(a, b)$.

Algorithm 1 האלגוריתם של אוקלידס

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a, r_1 \leftarrow b, n \leftarrow 1$ 
3: while  $r_n \neq 0$  do
4:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
5:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
6:    $n \leftarrow n + 1$ 
7: end while
8:  $n \leftarrow n - 1$ 
9: Output:  $r_n = \gcd(a, b)$ 
```

שלב	q_n	r_n
$n = 1$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$
$n = 2$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$
\vdots		
$n - 1$	$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = r_{n-2} - q_{n-1} r_{n-1}$
n	$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = r_{n-1} - q_n r_n$

משפט ב'ו: לכל זוג שלמים a, b קיימים שלמים s, t, d כך ש:
 $sa + tb = d$, $d = \gcd(a, b)$.

בהתנאי $a \geq b \geq 0$ **האלגוריתם המוכל של אוקלידס** נותן את השלמים (s, t, d) בפרק $sa + tb = d$ באופן הבא:

Algorithm 2 האלגוריתם המוכל של אוקלידס

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a, r_1 \leftarrow b$ 
3:  $s_0 \leftarrow 1, s_1 \leftarrow 0$ 
4:  $t_0 \leftarrow 0, t_1 \leftarrow 1, n \leftarrow 1$ 
5: while  $r_n \neq 0$  do
6:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
7:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
8:    $s_{n+1} \leftarrow s_{n-1} - q_n s_n$ 
9:    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$ 
10:   $n \leftarrow n + 1$ 
11: end while
12:  $n \leftarrow n - 1$ 
13: Output:  $d = r_n, s = s_n, t = t_n$ 
```

שלב	q_n	r_n	s_n	t_n
$n = 1$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$
$n = 2$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$
\vdots				
$n - 1$	$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = r_{n-2} - q_{n-1} r_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} t_{n-1}$
n	$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = r_{n-1} - q_n r_n$	$s_{n+1} = s_{n-1} - q_n s_n$	$t_{n+1} = t_{n-1} - q_n t_n$

מסומן $a^{-1} \in \mathbb{Z}_m$.
תנאי לאיבר הופכי בחוג: נתון $a \in \mathbb{Z}_m$ קיימים איבר הופכי a^{-1} אם ורק אם $\gcd(a, m) = 1$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & & & & & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & & & & \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix} \Rightarrow C_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & & & & & \\ \cancel{a_{i1}} & a_{i2} & \cdots & \cancel{a_{ij}} & \cdots & a_{in} \\ \vdots & & & & & \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn} \end{vmatrix}$$

מטריצה הקופקטורים של מטריצה A היא המטריצה שבה רכיב ה- ij הוא הקופקטור ה- $-ij$ של A :

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}.$$

$$A^{-1} = (\det A)^{-1} C^t \quad \text{נוסחת קרימר למטריצה הופכית:}$$

איברים הפיכים ב- \mathbb{Z}_{26} :

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

3 צפוי בסיסיים

ערכיהם הкриיפטוגרפיים של האותיות:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

לוח הכפל של 26:

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$26 \times m$	26	52	78	104	130	156	182	208	234	260	286	312	338	364	390
m	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$26 \times m$	416	442	468	494	520	546	572	598	624	650	676	702	728	754	780

כפניהם בסיסיים:

צופן	כלל מצפין	כלל מפענה	מפתח
קיסר	$e_k(x) = x + k \pmod{26}$	$d_k(x) = x - k \pmod{26}$	$k \in \mathbb{Z}_{26}$
תמורה	$e_\pi(x_1 \dots x_m) = x_{\pi(1)} \dots x_{\pi(m)} \pmod{26}$	$d_\pi(y_1 \dots y_m) = y_{\pi^{-1}(1)} \dots y_{\pi^{-1}(m)} \pmod{26}$	π תמורה של אורך m
החלפה	$e_\pi(x) = \pi(x) \pmod{26}$	$d_\pi(y) = \pi^{-1}(y) \pmod{26}$	π תמורה של אורך 26
אפייני	$e_k(x) = (ax + b) \pmod{26}$	$d_k(y) = a^{-1}(y - b) \pmod{26}$	$k = (a, b)$, $\gcd(a, 26) = 1$.
וויינר	$e_k(x_1, \dots, x_m) = (x_1 + k_1, \dots, x_m + k_m) \pmod{26}$	$d_k(y_1, \dots, y_m) = (y_1 - k_1, \dots, y_m - k_m) \pmod{26}$	$k = (k_1, \dots, k_m) \in \mathbb{Z}_{26}^m$
היל	$e_k(x_1 \dots x_m) = (x_1 \dots x_m) \cdot k \pmod{26}$	$d_k(y_1 \dots y_m) = (y_1 \dots y_m) \cdot k^{-1} \pmod{26}$	$k \in \mathbb{Z}_{26}^{m \times m}$, $\gcd(\det(k), 26) = 1$.

4 RSA צופן

- מפתח ציבורי: (n, e) כאשר $pq = n$ כאשר p, q מספרים ראשוניים שונים.
- מפתח סודי: (a, p, q) כאשר $a \equiv b^{-1} \pmod{\phi(n)}$, כאשר ϕ הפונקציית אוילר של n .
- $\phi(n) = \phi(pq) = (p-1)(q-1)$ כאשר q, p מספרים שלמים אז $a \equiv b^{-1} \pmod{(p-1)(q-1)}$.
- כלל מצפין: $e_k(x) = x^b \pmod{n}$ לכל מספר שלם x .
- כלל מפענה: $d_k(y) = y^a \pmod{n}$ לכל מספר שלם y .

שיטת הריבועיים לחישוב חזקה מודולרית:
 בהינתן n $b = b_k \dots b_1 b_0 = x^b \pmod{n}$. יהי $b = b_k \dots b_1 b_0 = y^b \pmod{n}$. אזי קיים אלגוריתם הנקרא שיטת הריבועיים שנונון ערך של $y = x^b \pmod{n}$ באופן הבא:

Algorithm 3 האלגוריתם שיטת הריבועים

```

1: Input: Integers  $x, b_0, \dots, b_k, n$  .
2:  $i \leftarrow 1$ 
3:  $z_0 \leftarrow x$ 
4: while  $i \leq k$  do
5:    $z_i \leftarrow z_{i-1}^2 \bmod n$ 
6: end while
7:  $i \leftarrow 0$ 
8:  $y \leftarrow 1$ 
9: while  $i \leq k$  do
10:   if  $b_i = 1$  then
11:      $y \leftarrow z_i y \bmod n$ 
12:   end if
13: end while
14: return:  $y$             $\triangleright y = x^b \bmod n$ 

```

האלגוריתם לפענוח של צופן : RSA

האלגוריתם הבא נותן את הפתרון x של הכלל מפענה $n = x = y^a \bmod p$ לפי השלבים הבאים:

$$x_1 = (y \bmod p)^{a \bmod (p-1)} \bmod p.$$

שלב [1] מחשבים $p \bmod y$ ו- $a \bmod (p-1)$ ואז מחשבים

$$x_2 = (y \bmod q)^{a \bmod (q-1)} \bmod q.$$

שלב [2] מחשבים $q \bmod y$ ו- $a \bmod (q-1)$ ואז מחשבים

$$\begin{cases} x = x_1 \bmod p \\ x = x_2 \bmod q \end{cases}$$

שלב [3] בעזרת המשפט השאריות הסיני פותרים את המערכת

5 צופן ElGamal

- המפתח הוא $k = (p, a, \alpha, d)$ כאשר:

- p מספר ראשוני
- a, d, α מספרים שלמים חיוביים עבורם $2 \leq a, d, \alpha \leq p - 2$
- $\beta = \alpha^a \bmod p$
- כלל מצפין: $y_1 = \alpha^d \bmod p, y_2 = x\beta^d \bmod p$ לכל x שלם חיובי.
- כלל מפענה: $x = (y_1^a)^{-1} y_2 \bmod p$

6 צופן אניגמה

תמורה על קבוצה סופית $\Sigma = \{x_1, \dots, x_n\}$ היא פונקציה $\Sigma \rightarrow \Sigma : \pi$ חד-חד ערכית ו"על" Σ .

- על Σ : לכל Σ קיימים $x \in \Sigma$ כך ש: $y = \Sigma(x)$

- חד-חד-ערכית: לכל Σ $x, y \in \Sigma$ מתקיים:

$$x \neq y \Rightarrow \Sigma(x) \neq \pi(y).$$

התמורה זהה מסומנת $\Sigma \rightarrow \Sigma : \text{id}(x) = x$ ומוגדרת כך שלכל $x \in \Sigma$:

תמורה הופכית: אם $\Sigma \rightarrow \Sigma : \pi$ תמורה על הקבוצה Σ , התמורה ההופכית מסומנת π^{-1} מקיימת את התנאי:
 $\forall x \in \Sigma \quad \pi\pi^{-1}(x) = x = \pi^{-1}\pi(x)$.

המורה $\Sigma \rightarrow \rho$ היא **תמורה משקפת** אם התנאי הזה מתקיים:

$$\forall x, y \in \Sigma : \quad \rho(x) = y \iff \rho(y) = x .$$

הgelglim ומשקף הקבוע של צופן איניגמה:

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\alpha_1(x)$	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
$\alpha_2(x)$	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
$\alpha_3(x)$	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
$\rho(x)$	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

כלל מצפן וככל מפענה של צופן איניגמה:

- בהינתן מילה $x_1x_2\dots x_k$ של טקסט גלי, הכלל מצפן של האות ה- i הוא:
כאשר Δ_i היא התמורה הכתובה למיטה.
- בהינתן מילה $y_1y_2\dots y_k$ של טקסט מוצפן הכלל מפענה של האות ה- i הוא:
• לכל i שלים:

$$\Delta_i = \tau_i^{-1} \rho \tau_i ,$$

כאשר

- ρ היא התמורה המשקפת הקבועה של צופן איניגמה,
- $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi$, $\tau_i^{-1} = \pi \alpha_1^{-1} \alpha_2^{-1} \sigma_{-i} \alpha_3^{-1} \sigma_i$

כאשר $\alpha_1, \alpha_2, \alpha_3$ הן התמורות של הgelglim של צופן איניגמה הנتونות בטבלה לעיל, π היא תמורה המשקפת המשתנה,

- $\sigma_i(x) = x + i \bmod 26$ היא תמורה הזאת של i אותיות קדימה באלפבית:
- $\sigma_{-i}(x) = x - i \bmod 26$ היא תמורה הזאת של i אותיות אחורה באלפבית:

מילה משוכפלת היא מילה סימטרית של טקסט גלי באורך 6 אותיות מהצורה:
 $xyzzxy$.

מילה אופיינית היא ההצפנה של מילה משוכפלת ע"י צופן איניגמה:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) .$$

משפט ריבסקי I: יהי $\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6$ מילה אופיינית של צופן האיניגמה. אז:
 $\sigma_4 = \Delta_4\Delta_1(\sigma_1)$, $\sigma_5 = \Delta_5\Delta_2(\sigma_2)$, $\sigma_6 = \Delta_6\Delta_3(\sigma_3)$.

משפט ריבסקי II:

עבור כל אחת של התמורות $\Delta_4\Delta_1, \Delta_5\Delta_2, \Delta_6\Delta_3$ של צופן איניגמה, קיים סידור של הפירוק לראשונים שנקרה סדר ריבסקי כך שהתנאים הבאים מתקיימים:

- לכל זוג מחרוזות $(a_1 \ a_2 \ \dots \ a_{k-1} \ a_k)$ $(b_1 \ b_2 \ \dots \ b_{k-1} \ b_k)$ $b_k = \Delta_1(a_1)$, $b_{k-1} = \Delta_1(a_2)$, \dots , $b_2 = \Delta_1(a_{k-1})$, $b_1 = \Delta_1(a_k)$.
- לכל זוג מחרוזות $(a_1 \ a_2 \ \dots \ a_{k-1} \ a_k)$ $(b_1 \ b_2 \ \dots \ b_{k-1} \ b_k)$ $b_k = \Delta_1(a_1)$, $b_{k-1} = \Delta_1(a_2)$, \dots , $b_2 = \Delta_1(a_{k-1})$, $b_1 = \Delta_1(a_k)$.
- לכל זוג מחרוזות $(a_1 \ a_2 \ \dots \ a_{k-1} \ a_k)$ $(b_1 \ b_2 \ \dots \ b_{k-1} \ b_k)$ $b_k = \Delta_1(a_1)$, $b_{k-1} = \Delta_1(a_2)$, \dots , $b_2 = \Delta_1(a_{k-1})$, $b_1 = \Delta_1(a_k)$.

7 תורת שאנון וסודיות מושלמת

הסתברויות של האותיות:

אות	הסתברות								
a	0.082	f	0.022	k	0.008	p	0.019	u	0.028
b	0.015	g	0.02	l	0.04	q	0.001	v	0.01
c	0.028	h	0.061	m	0.024	r	0.06	w	0.023
d	0.043	i	0.07	n	0.067	s	0.063	x	0.001
e	0.127	j	0.002	o	0.075	t	0.091	y	0.02
								z	0.001

קבוצות תדריות של האותיות בטקסט:

	אות	הסתברות
1.	e	$p = 0.127$
2.	t, a, o, i, n, s, h, r	$0.06 \lesssim p \lesssim 0.09$
3.	d, l	$p \approx 0.04$
4.	c, u, m, w, f, g, y, p, b	$0.015 \lesssim p \lesssim 0.028$
5.	v, k, j, x, q, z	$p < 0.01$

זוגות האותיות הנפוצים ביותר:

th	he	in	er	an	re	ed	on	es	st
en	at	to	nt	ha	nd	ou	ea	ng	as
or	ti	is	et	it	ar	te	se	hi	of

שלשות של אותיות הנפוצים ביותר:

the	ing	and	her	ere	ent	tha	nth	was	eth	for	dth
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

מידע של מ"מ בדיד X :

אנטロפייה של מ"מ בדיד X :

נוסחת בייס:

$$P(X = x|Y = y)P(Y = y) = P(X = x \cap Y = y) = P(Y = y|X = x)P(X = x).$$

סודיות:

נתונה קרייפטו-מערכת בעלת קבוצת טקסט גליי X , קבוצת טקסט מוצפן Y וקבוצת מפתחות K , כלל מצפין $.x = d_k(y)$ וככל מפענה $y = e_k(x)$

$$P(Y = y) = \sum_{k \in K} P(K = k) P(X = d_k(y)) ,$$

$$P(Y = y | X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) ,$$

$$P(X = x | Y = y) = \frac{P(X = x) \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k)}{\sum_{k \in K} P(K = k) P(X = d_k(y))} .$$

סודיות מושלמת: לкриpto-מערכת יש סודיות מושלמת אם התנאי הבא מתקיים:

$$P(X = x | Y = y) = P(X = x) \iff P(Y = y | X = x) = P(Y = y) .$$

אנטロפייה מותנית:

$$H(X|Y = y) = - \sum_{x \in X} P(X = x | Y = y) \log_2 P(X = x | Y = y) ,$$

$$H(X|Y) = - \sum_{y \in Y} \sum_{x \in X} P(Y = y) P(X = x | Y = y) \log_2 P(X = x | Y = y) ,$$

$$H(X, Y) = H(Y) + H(X|Y) , \quad H(X|Y) \leq H(X) .$$

משפט האנטרופיה לкриpto-מערכות:

$$H(K|C) = H(K) + H(P) - H(C) .$$

טבלת אמת:

p	q	$p \wedge q$	$p \vee q$	$\sim p$	$p \oplus q$
1	1	1	1	0	0
1	0	0	1	0	1
0	1	0	1	1	1
0	0	0	0	1	0

8 צופן פיבסטל

ספרות הקסדצימליות:

hex	0	1	2	3	4	5	6	7
binary	0000	0001	0010	0011	0100	0101	0110	0111
hex	8	9	A	B	C	D	E	F
binary	1000	1001	1010	1011	1100	1101	1110	1111

משוואות פיסטול להצפנה:

נתון טקסט גלי $x = L_0 R_0$. לכל N :

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i), \quad y = R_N L_N.$$

משוואות פיסטול לפענוח:

נתון טקסט גלי $y = R_N L_N$. לכל N :

$$R_i = L_{i+1}, \quad L_i = R_{i+1} \oplus f(R_i, k_{i+1}), \quad x = L_0 R_0.$$

9 צופן IDEA

תזמון מפתח של IDEA

r	k_1	k_2	k_3	k_4	k_5	k_6
1	0 – 15	16 – 31	32 – 47	48 – 63	64 – 79	80 – 95
2	96 – 111	112 – 127	25 – 40	41 – 56	57 – 72	73 – 88
3	89 – 104	105 – 120	121 – 8	9 – 24	50 – 65	66 – 81
4	82 – 97	98 – 113	114 – 1	2 – 17	18 – 33	34 – 49
5	75 – 90	91 – 106	107 – 122	123 – 10	11 – 26	27 – 42
6	43 – 58	59 – 74	100 – 115	116 – 3	4 – 19	20 – 35
7	36 – 51	52 – 67	68 – 83	84 – 99	125 – 12	13 – 28
8	29 – 44	45 – 60	61 – 76	77 – 92	93 – 108	109 – 124
9	22 – 37	38 – 53	54 – 69	70 – 85	–	–

אלגוריתם הצפנה IDEA

- נתון טקסט גלי $P \in \{0, 1\}^{64}$. של אורך 64 ביטים.
- מחלקיים P לארבע בלוקים $P_i \in \{0, 1\}^{16}$: $P = P_1 P_2 P_3 P_4$.
- בתחילת מהזור ה- r (1) מסמנים את הטקסט מוצפן המתקבל ממהזור הקודם (מהזור $r - 1$) ב- $C^{(1)}$, בלבד מ- $C^{(r)}$.
- כל מהזור r מורכב מהשלבים הבאים:

$$Y_1 = C_1^{(r)} \odot k_1^{(r)} = C_1^{(r)} \cdot k_1^{(r)} \pmod{(2^{16} + 1)} \quad [1]$$

$$Y_2 = C_2^{(r)} \boxplus k_2^{(r)} = C_2^{(r)} + k_2^{(r)} \pmod{2^{16}} \quad [2]$$

$$Y_3 = C_3^{(r)} \boxplus k_3^{(r)} = C_3^{(r)} + k_3^{(r)} \pmod{2^{16}} \quad [3]$$

$$Y_4 = C_4^{(r)} \odot k_4^{(r)} = C_4^{(r)} \cdot k_4^{(r)} \pmod{(2^{16} + 1)} \quad [4]$$

$$Y_5 = Y_1 \oplus Y_3 \quad [5]$$

$$Y_6 = Y_2 \oplus Y_4 \quad [6]$$

$$Y_7 = Y_5 \odot k_5^{(r)} = Y_5 \cdot k_5^{(r)} \pmod{(2^{16} + 1)} \quad [7]$$

$$Y_8 = Y_6 \boxplus Y_7 = Y_6 + Y_7 \pmod{2^{16}} \quad [8]$$

$$Y_9 = Y_8 \odot k_6^{(r)} = Y_8 \cdot k_6^{(r)} \pmod{2^{16} + 1} \quad [9]$$

$$Y_{10} = Y_7 \boxplus Y_9 = Y_7 + Y_9 \pmod{2^{16}} \quad [10]$$

$$C_1^{(r+1)} = Y_1 \oplus Y_9 \quad [11]$$

$$C_2^{(r+1)} = Y_3 \oplus Y_9 \quad [12]$$

$$C_3^{(r+1)} = Y_2 \oplus Y_{10} \quad [13]$$

$$C_4^{(r+1)} = Y_4 \oplus Y_{10} \quad [14]$$

- בכדי לקבל את הטקסט מוצפן הסופי, אחרי ביצוע של כל המחוירים r מבצעים את השלב התפוקה:

$$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \pmod{2^{16} + 1} \quad [1]$$

$$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \pmod{2^{16}} \quad [2]$$

$$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \pmod{2^{16}} \quad [3]$$

$$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \pmod{2^{16} + 1} \quad [4]$$

- לבסוף הטקסט מוצפן 64- ביטים מתkowski מהארבע בלוקים 16- ביטים

$.C = C_1 C_2 C_3 C_4$

מפתחות פענוח של IDEA

$$DK_1^{(1)} = \left(K_1^{(9)} \right)^{-1}, \quad DK_2^{(1)} = -\left(K_2^{(9)} \right), \quad DK_3^{(1)} = -\left(K_3^{(9)} \right), \quad DK_4^{(1)} = \left(K_4^{(9)} \right)^{-1},$$

$$DK_5^{(1)} = K_5^{(8)}, \quad DK_6^{(1)} = K_6^{(8)}.$$

10 צופן DES

אלגוריתם הצפנה DES : נתון טקסט גלי 64 ביטים $x = x_1 \dots x_{64}$

שלב [1] מבצעים IP(x_1, x_2, \dots, x_{64}) כאשר IP הTransformation הIGINITAL:

$$IP = \begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 & 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 & 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 & 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 & 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$$

שלב [2] מחלקים IP(x) לשניים. IP(x) = $L_0 R_0$ כאשר L_0 ה-32 ביטים הראשונים של x וה-32 האחרונים:

$$L_0 = x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4$$

$$x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8,$$

$$R_0 = x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3$$

$$x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7.$$

שלב [3] מבצעים 16 מחוירים של אלגוריתם פיזטל:

כאשר k_1, \dots, k_{16} תת-מפתחות כל אחד 48 ביטים שמתכוילים ממפתח הIGINITAL: k .

שלב [4] IP $^{-1}$ IP $^{-1}$ ($R_{16} L_{16}$) $= y$ כאשר IP $^{-1}$ ההפוכה:

$$IP^{-1} = \begin{pmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 & 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 & 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 53 & 20 & 60 & 28 & 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 & 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{pmatrix}$$

הפונקציית ליבה של DES

$$f : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}.$$

נסמן הארגומנטים של f ב- $J \in \{0, 1\}^{48}, A \in \{0, 1\}^{32}$ כאשר $f(A, J)$ מתווארת על ידי האלגוריתם הבא:

$$E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$$

שלב [1] מגדילים A לרצף 48 ביטים באמצעות התמורה ההגדלה

שלב [2] מחשבים J ורושמים התשובה כשירשור של שמונה רצפים 6 ביטים:

$$B = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8 , \quad B_j \in \{0, 1\}^6 .$$

שלב [3] רושמים $B_j = b_1 b_2 b_3 b_4 b_5 b_6$ כאשר $b_i \in \{0, 1\}$.

שלב [4] בשלב זה משתמשים החחלפות S_j (S_1, \dots, S_8) הינה מטריצה מסדר 4×4 שנთן למטה. לכל $8 \leq j \leq 1$

$$C_j = (S_j(r, c))_2 , \quad r = (b_1 b_6)_{10} , \quad c = (b_2 b_3 b_4 b_5)_{10}$$

כאשר r בספרות דצמליות, c האיבר בשורה r ועמודה c של המטריצה S_j . לבסוף מmirים C_j בספרות ביניאריות.

$$P = \begin{pmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{pmatrix}$$

שלב [5] כאשר P התמורה $f(A, J) = P(C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8)$

התזמון המפתח של DES: נתון מפתח התחלתי 64 ביטים, $.k$.

$$PC_1 = \begin{pmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{pmatrix}$$

שלב [1] מבצעים התמורה

שלב [2] נסמן $PC_1(k) = C_0 D_0$ כאשר C_0 ה- 28 ביטים הראשונים ו- D_0 ה- 28 ביטים האחרונים.

$$C_i = LS_i(C_{i-1}) , \quad D_i = LS_i(D_{i-1}) , \quad k_i = PC_2(C_i D_i) .$$

שלב [3] לכל $1 \leq i \leq 16$, מחשבים

$$PC_2 - LS_i = \left\{ \begin{array}{ll} \text{זהה מקום אחד שמאליה} & i = 1, 2, 9, 16, \\ \text{זהה שתי מקומות שמאליה} & i = 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15 , \end{array} \right\} \text{ כאשר}$$

$$PC_2 = \begin{pmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{pmatrix} .$$

הבלוקים של החלפות של DES

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

פתרונות **שאלה 1**

א) (8 נק') ראשית נחשב את המפתח הסודי:

$$\beta = \alpha^a \pmod{p} = 13^{30} \pmod{41} .$$

נחשב את החזקה מודולרית בעזרת שיטת הריבועים:

$$30 = 16 + 8 + 4 + 2 \Rightarrow [30]_2 = 11110 .$$

$$i \leftarrow 0, z_0 \leftarrow 13$$

$$z_1 = z_0^2 \pmod{p} = 13^2 \pmod{41} = 5 ,$$

$$z_2 = z_1^2 \pmod{p} = 5^2 \pmod{41} = 25 ,$$

$$z_3 = z_2^2 \pmod{p} = 25^2 \pmod{41} = 10 ,$$

$$z_4 = z_3^2 \pmod{p} = 10^2 \pmod{41} = 18 .$$

$$i \leftarrow 0, y \leftarrow 1$$

$$y \leftarrow z_1 y \pmod{p} = 5 \pmod{41} = 5 ,$$

$$y \leftarrow z_2 y \pmod{p} = (5)(25) \pmod{41} = 2 ,$$

$$y \leftarrow z_3 y \pmod{p} = (10)(2) \pmod{41} = 20 ,$$

$$y \leftarrow z_4 y \pmod{p} = (18)(20) \pmod{41} = 32 .$$

לכן:

$$\beta = \alpha^a \pmod{p} = 13^{10} \pmod{41} = 32 .$$

כעת נבצע את ההצפנה. הכלל מצפין הוא:

$$y_1 = \alpha^d \pmod{p} = 13^4 \pmod{41} = 28561 \pmod{41} = 28561 - (41) \left\lfloor \frac{28461}{41} \right\rfloor = 25 .$$

$$\begin{aligned} y_2 &= x\beta^d \pmod{p} \\ &= (12)(32^4) \pmod{41} \\ &= (12 \pmod{41})(32^2 \pmod{41})(32^2 \pmod{41}) \\ &= (12)(40)(40) \pmod{41} \\ &= 19200 \pmod{41} \\ &= 12 . \end{aligned}$$

לכן הטקסט מוצפן הוא: $(y_1, y_2) = (25, 12)$

(ב) (8 נק')

$$x = (y_1^a)^{-1} (y_2) \bmod p = (25^{30})^{-1}(12) \bmod 41 .$$

$$(25^{30})^{-1} \bmod 41 = 25^{-30} \bmod 41 \stackrel{\text{משפט פרמה}}{=} 25^{41-1-30} \bmod 41 = 25^{10} \bmod 41 .$$

נפתרו את החזקה מודולרית ה- α בעזרת השיטת הריבועים הבא:

$$10 = 8 + 2 \Rightarrow [10]_2 = 1010 .$$

$$i \leftarrow 0, z_0 \leftarrow 25$$

$$z_1 = z_0^2 \bmod p = 25^2 \bmod 41 = 10 ,$$

$$z_2 = z_1^2 \bmod p = 10^2 \bmod 41 = 18 ,$$

$$z_3 = z_2^2 \bmod p = 18^2 \bmod 41 = 37 .$$

$$i \leftarrow 0, y \leftarrow 1$$

$$y \leftarrow z_1 y \bmod p = 10 \bmod 41 = 10 ,$$

$$y \leftarrow z_3 y \bmod p = (37)(10) \bmod 41 = 1 .$$

לכן:

$$25^{10} \bmod 41 = 1 .$$

ולכן

$$x = (y_1^a)^{-1} (y_2) \bmod p = (25^{30})^{-1}(12) \bmod 41 = 12 \bmod 41 = 12 .$$

(ג) (4 נק')

לפי משפט החלוק של אוקלידס קיימים שלמים r_1, q_1 כך ש:

$$a + b = q_1 m + r_1 , \quad 0 \leq r_1 < m ,$$

$$\text{כאשר } r_1 = (a + b) \bmod m \text{ וגם } q_1 = \left\lfloor \frac{a + b}{m} \right\rfloor \text{ מכאן:}$$

$$((a + b) \bmod m) - b = r_1 - b = a - q_1 m .$$

וזהו קיים שלם $Q = -q_1$ כך ש:

$$((a + b) \bmod m) - b = Qm + a$$

ולכן

$$((a + b) \bmod m) - b \equiv a \pmod{m}$$

ולפיכך, מכיוון שהשני שלמים $((a + b) \bmod m) - b$ ו- a שווים מודולריים ביחס ל- m , אז בהכרח יש להם אותה שארית בחלוקת ב- m :

$$[((a + b) \bmod m) - b] \bmod m = a \bmod m .$$

ד) (5 נק')

$$y = e_k(x)$$

$$\begin{aligned}
 d_k(e_k(x)) &= d_k(y) \\
 &= a^{-1}(y - b) \bmod 26 \\
 &= a^{-1}([(ax + b) \bmod 26] - b) \bmod 26 \\
 &\stackrel{\text{ככל הכפל}}{=} (a^{-1} \bmod 26)(([(ax + b) \bmod 26] - b) \bmod 26) \bmod 26 \\
 &\stackrel{\text{סעיף י'}}{=} (a^{-1} \bmod 26)(ax \bmod 26) \bmod 26 \\
 &\stackrel{\text{ככל הכפל}}{=} (a^{-1}ax \bmod 26) \bmod 26 \\
 &= x \bmod 26 .
 \end{aligned}$$

 שאלה 2

א) (13 נק')

ב) (12 נק')

כיוון ⇐

אם m מספר ריבוע אז קיימים שלם a חיובי כך ש: $m = a^2$.
 כל מספר שלם חיובי הוא מספר ראשוני או מתפרק למספרים ראשוניים.
 יהיו הפירוק לראשוניים של a :

$$a = p_1^{e_1} \cdots p_k^{e_k}$$

כאשר p_i מספר ראשוני ו- $e_i > 0$ לכל $1 \leq i \leq k$ ולכן
 $m = a^2 = p_1^{2e_1} \cdots p_k^{2e_k}$.

כיוון ⇒

אם בפירוק לראשוניים של m , כל מספר ראשוני מופיע עם חזקה זוגית אז

$$m = p_1^{2e_1} \cdots p_k^{2e_k} ,$$

כאשר p_i ראשוני ו- $e_i > 0$ לכל $1 \leq i \leq k$ ולכן
 $m = (p_1^{e_1} \cdots p_k^{e_k})^2 = a^2$,

כאשר $a = p_1^{e_1} \cdots p_k^{e_k}$
 לכן קיימים שלם חיובי a כך ש: $m = a^2$ וכאן m מספר ריבועי.

שאלה 3 (נקודות) 25

(א)

$$n = pq = 7 \times 13 = 91$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 6 \times 12 = 72 .$$

s, t, d ו- $A = 72, B = 11$ נשתמש באלגוריתם של אוקלידס. נסמן $a = 11^{-1} \pmod{72}$ ונחפש שלמים $uA + tB = d$.

$$\begin{aligned} r_0 &= 72, & r_1 &= 11 , \\ s_0 &= 1 , & s_1 &= 0 , \\ t_0 &= 0 , & t_1 &= 1 . \end{aligned}$$

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = 6$	$r_2 = 72 - (6)(11) = 6$	$s_2 = 1 - (6)(0) = 1$	$t_2 = 0 - (6)(1) = -6$: $i = 1$ שלב
$q_2 = 1$	$r_3 = 11 - (1)(6) = 5$	$s_3 = 0 - (1)(1) = -1$	$t_3 = 1 - (1)(-6) = 7$: $i = 2$ שלב
$q_3 = 1$	$r_4 = 6 - (1)(5) = 1$	$s_4 = 1 - (1)(-1) = 2$	$t_4 = -6 - (1)(7) = -13$: $i = 3$ שלב
$q_4 = 5$	$r_5 = 5 - (5)(1) = 0$	$s_5 = -1 - (5)(2) = -11$	$t_5 = 7 - (5)(-13) = 72$: $i = 4$ שלב

$$d = r_4 = 1 \quad t = t_4 = -13 \quad s = s_4 = 2$$

$$sA + tB = 1 \quad \Rightarrow \quad 2(72) + (-13)(11) = 1 .$$

לכן

$$11^{-1} \equiv -13 \pmod{72} \equiv 59 \pmod{72} .$$

לפיכך המפתח הסודי הוא:

$$a = b^{-1} \pmod{\phi(n)} = 11^{-1} \pmod{72} = 59 .$$

כעת נחשב את הטקסט הגלוי מהtekst מוצפן $y = 41$ על פי הכלל מפענה:

$$x = y^a \pmod{n} = 41 \pmod{91} = 41^{59} \pmod{91} .$$

נפתר את הכלל מפענה על פי האלגוריתם לפענוח של RSA:

$$\begin{aligned} x_1 &= (y \pmod{p})^{a \pmod{(p-1)}} \pmod{p} \\ &= ((41 \pmod{7})^{59 \pmod{6}}) \pmod{7} \\ &= 6^5 \pmod{7} \\ &= 6 . \end{aligned}$$

$$\begin{aligned}
 x_2 &= (y \bmod q)^{a \bmod (q-1)} \bmod q \\
 &= ((41 \bmod 13)^{59 \bmod (12)}) \bmod 13 \\
 &= 2^1 \bmod 13 \\
 &= 7.
 \end{aligned}$$

כעת נפתרו את המערכת הבאה בעזרת המשפט השאריות הסיני:

$$\begin{aligned}
 x &= x_1 \bmod 7 = 6 \bmod 7, \\
 x &= x_2 \bmod 11 = 7 \bmod 13.
 \end{aligned}$$

נסמן: $m_1 = 7, m_2 = 13, a_1 = 6, a_2 = 7$

$$\begin{aligned}
 x &= a_1 \bmod m_1 = 6 \bmod 7, \\
 x &= a_2 \bmod m_2 = 7 \bmod 13.
 \end{aligned}$$

נפתרו ע"י משפט השאריות הסיני:

$$M = m_1 m_2 = 91, \quad M_1 = \frac{M}{m_1} = 13, \quad M_2 = \frac{M}{m_2} = 7.$$

נשים לב:

$$\begin{aligned}
 2(7) + (-1)13 &= 1 \\
 .13^{-1} \equiv -1 \pmod{7} &\equiv 6 \pmod{7} \quad \text{ו} \quad 7^{-1} \equiv 2 \pmod{13} \\
 \text{לכן}
 \end{aligned}$$

$$y_1 = M_1^{-1} \bmod m_1 = 13^{-1} \bmod 7 = 6, \quad y_2 = M_2^{-1} \bmod m_2 = 7^{-1} \bmod 13 = 2.$$

$$\begin{aligned}
 x &= a_1 M_1 y_1 + a_2 M_2 y_2 \bmod M \\
 &= (6)(13)(6) + (7)(7)(2) \bmod 91 \\
 &= 468 + 98 \bmod 91 \\
 &= 566 \bmod 91 \\
 &= 20.
 \end{aligned}$$

ב) (6 נק')

לפי ההגדרה של צופן El-Gamal, הכלל מצפין הוא

$$e_k(x) = (y_1, y_2) \quad y_1 = \alpha^d \bmod p, \quad y_2 = \beta^d x \bmod p,$$

כאשר p ראשוני ו- d שלם, והכלל מעפנה הוא

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \bmod p.$$

לפיכך:

$$d_k(e_k(x)) = d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \bmod p = [(\alpha^d \bmod p)^a]^{-1} (x \beta^d \bmod p) \bmod p. \quad (*1)$$

הזהות הבאה מתקיימת. אם n, m, z שלמים חיוביים אז

$$(z \bmod m)^n \equiv z^n \pmod{m} . \quad (*2)$$

הוכחה: לפי משפט החלוק של אטקלידס קיימים שלמים r, q כך ש- $z = qm + r$. לכן $(z \bmod m)^n = z^n + \sum_{k=1}^n \binom{n}{k} (-qm)^k z^{n-k} \equiv z^n \pmod{m}$.

ולכן

משמעותו $(z \bmod m)^n \equiv yz^n \pmod{m}$: y, z, m, n שלמים חיוביים.

$$y(z \bmod m)^n \bmod m = yz^n \bmod m . \quad (*3)$$

בנוסף להזהות הבאה מתקיימת. לכל שלמים חיוביים b, c, m

$$b \equiv c \pmod{m} \Rightarrow b^{-1} \equiv c^{-1} \pmod{m} . \quad (*4)$$

הוכחה: נניח $bb^{-1} \equiv 1 \pmod{m}$ או $bb^{-1} \equiv 1 \pmod{m}$. מכיוון ש- $b \equiv c \pmod{m}$ $b^{-1} \equiv c^{-1} \pmod{m}$ לכן

מן- $(*4)$, לכל z, m, n שלמים חיוביים:

$$[(z \bmod m)^n]^{-1} \equiv z^{-n} \pmod{m} . \quad (*5)$$

מכאן, לכל y שלם:

$$[(z \bmod m)^n]^{-1} \equiv z^{-n} \pmod{m} \Rightarrow [(z \bmod m)^n]^{-1} y \equiv z^{-n} y \pmod{m} . \quad (*6)$$

ולכן

$$[(z \bmod m)^n]^{-1} y \bmod m = z^{-n} y \bmod m . \quad (*7)$$

לפי משווה $(*7)$, אם נציב $y = x\beta^d \pmod{p}$, $m = p$, $z = \alpha^d$ נקבל:

$$[(\alpha^d \bmod p)^a]^{-1} (x\beta^d \bmod p) \bmod p = \alpha^{-ad} (x\beta^d \bmod p) \bmod p , \quad (*8)$$

ולכן לפי משווה $(*1)$:

$$d_k(e_k(x)) = \alpha^{-ad} (x\beta^d \bmod p) \bmod p . \quad (*9)$$

לכל שלמים b, c, m מתקיים:

$$b(c \bmod m) \bmod m = bc \bmod m \quad (*10)$$

ולכן

$$d_k(e_k(x)) = \alpha^{-ad} x\beta^d \bmod p . \quad (*11)$$

נציב את ההגדרה של $\beta = \alpha^a \pmod{p}$

$$d_k(e_k(x)) = \alpha^{-ad} x (\alpha^a \bmod p)^d \bmod p .$$

ואז לפי משווה $(*8)$ אנחנו נקבל ש:

$$d_k(e_k(x)) = \alpha^{-ad} x \alpha^{ad} \bmod p = x \bmod p .$$

ג) (7 נק')

נניח כי $\Sigma \rightarrow \Sigma$: π מחזיר באורך k . זו הפירוק למחזורים של π הוא:

$$\pi = (a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) ,$$

או, כפונקציה מעלה Σ :

$$\pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1 .$$

אפשר לרשום את זה בביטוי ייחיד:

$$\pi(a_i) = a_{(i \bmod k)+1} .$$

עבור π^2

$$\pi^2(a_1) = a_3, \quad \pi^2(a_2) = a_4, \quad \dots \quad \pi^2(a_{k-2}) = a_k, \quad \pi^2(a_{k-1}) = a_1, \quad \pi^2(a_k) = a_2 .$$

ובאותה מידת אפשר לרשום π^2 בביטוי ייחיד:

$$\pi^2(a_i) = a_{((i+1) \bmod k)+1} .$$

באופן כללי לכל $0 \leq j \leq k$ טבעי:

$$\pi^j(a_i) = a_{((i+j-1) \bmod k)+1} .$$

מכאן נציב $j = k$:

$$\pi^k(a_i) = a_{((i+k-1) \bmod k)+1} = a_{((i-1) \bmod k)+1} = \begin{cases} a_i & : i < k \\ a_k & : i = k \end{cases} .$$

וזהו נכון לכל $1 \leq i \leq k$

$$\pi^k(a_i) = a_i \Rightarrow \pi^k = \text{id}$$

 שאלה 4 (7 נקודות)

א) (11 נק') $\gcd(|k|, 26) = 1$. $|k| = 27 - 98 = -71 \bmod 26 = 7$ קיימת. נחשב את המטריצה של קופקטורים: $|k|^{-1} \bmod 26 = 7^{-1} \bmod 26 = 15$

$$C_{11} = 9, \quad C_{12} = -7, \quad C_{21} = -14, \quad C_{22} = 3 .$$

מכאן

$$\text{adj}(k) = C^t = \begin{pmatrix} 9 & -7 \\ -14 & 3 \end{pmatrix}^t \bmod 26 = \begin{pmatrix} 9 & 19 \\ 12 & 3 \end{pmatrix}^t \bmod 26 = \begin{pmatrix} 9 & 12 \\ 19 & 3 \end{pmatrix}$$

לכן

$$k^{-1} \bmod 26 = |k|^{-1} \text{adj}(k) \bmod 26 = 15 \begin{pmatrix} 9 & 12 \\ 19 & 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 135 & 180 \\ 285 & 45 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 24 \\ 25 & 19 \end{pmatrix} .$$

$y \in C$	V	M	U	H	B	B
$y \in \mathbb{Z}_{26}$	21	12	20	7	1	1

$$(21 \ 12) \begin{pmatrix} 5 & 24 \\ 25 & 19 \end{pmatrix} \bmod 26 = (405 \ 732) \bmod 26 = (15 \ 4)$$

$$(20 \ 7) \begin{pmatrix} 5 & 24 \\ 25 & 19 \end{pmatrix} \bmod 26 = (275 \ 613) \bmod 26 = (15 \ 15)$$

$$(1 \ 1) \begin{pmatrix} 5 & 24 \\ 25 & 19 \end{pmatrix} \bmod 26 = (30 \ 43) \bmod 26 = (4 \ 17)$$

$y \in C$	V	M	U	H	B	B
$y \in \mathbb{Z}_{26}$	21	12	20	7	1	1
$x \in \mathbb{Z}_{26}$	15	4	15	15	4	17
$x \in P$	p	e	p	p	e	r

ב) (10 נק') לפי משפט ריבסקי II:

$$\Delta_1(P) = L ,$$

$$\Delta_2(I) = E ,$$

$$\Delta_3(P) = T .$$

$$V = \Delta_4 \Delta_1(N) \Rightarrow \Delta_4(V) = \Delta_1(N) \Rightarrow \Delta_4(V) = T .$$

$$B = \Delta_5 \Delta_2(I) \Rightarrow \Delta_5(B) = \Delta_2(I) \Rightarrow \Delta_5(B) = E .$$

$$Y = \Delta_6 \Delta_3(P) \Rightarrow \Delta_6(Y) = \Delta_3(P) \Rightarrow \Delta_6(Y) = R .$$

לכן הטקסט גליי הוא:
LETTER .

ג) (4 נק') יהיו $d = \gcd(a, b)$. לפי משפט בז'ו קיימים שלמים s, t עבורם:

$$sa + tb = d .$$

נכפיל בשלים $m > 0$:

$$s(ma) + t(mb) = md .$$

מכיוון ש- $d \mid a, b$ אז $md \mid ma, mb$. הוכחנו כי md משותף של ma, mb . נכון כי הוא המחלק המשותף המקסימלי. נניח שקיימים שלם $D > md$ שמחלק ma ו- mb . אז:

$$D \mid s(ma) + t(mb) \Rightarrow D \mid md \Rightarrow md \geq D ,$$

בסתירה לכך ש: $D > md$

שאלה 5 (נקודות)

א) (10 נק') נתון המפתח של צופן אפיני $a = 21, b = 4$. הכלל מפענה הינו $d_k(y) = a^{-1}(y - b) \pmod{26}$. a^{-1} קיימת שכן $\gcd(a, 26) = \gcd(21, 26) = 1$:

$$a^{-1} \equiv 5 \pmod{26} .$$

$$d_k(y) = a^{-1}(y - b) \pmod{26} = 5(y - 4) \pmod{26} = 5y - 20 \pmod{26} = 5y + 6 \pmod{26} .$$

$$\begin{aligned} d_k(F) &= d_k(5) &= 5(5) + 6 \pmod{26} = 5 , \\ d_k(M) &= d_k(12) &= 5(12) + 6 \pmod{26} = 14 , \\ d_k(B) &= d_k(1) &= 5(1) + 6 \pmod{26} = 11 , \\ d_k(Y) &= d_k(24) &= 5(24) + 6 \pmod{26} = 22 , \\ d_k(O) &= d_k(14) &= 5(14) + 6 \pmod{26} = 24 , \\ d_k(I) &= d_k(8) &= 5(8) + 6 \pmod{26} = 20 , \\ d_k(X) &= d_k(23) &= 5(23) + 6 \pmod{26} = 17 , \\ d_k(P) &= d_k(15) &= 5(15) + 6 \pmod{26} = 3 , \\ d_k(K) &= d_k(10) &= 5(10) + 6 \pmod{26} = 4 , \\ d_k(E) &= d_k(4) &= 5(4) + 6 \pmod{26} = 0 , \\ d_k(W) &= d_k(22) &= 5(2) + 6 \pmod{26} = 12 , \\ d_k(S) &= d_k(18) &= 5(18) + 6 \pmod{26} = 18 , \end{aligned}$$

$y \in C$	F	M	B	B	M	Y	O	M	I	X	P	X	K	E	W	S
$y \in \mathbb{Z}_{26}$	5	12	1	1	12	24	14	12	8	23	15	24	10	4	22	18
$x \in \mathbb{Z}_{26}$	5	14	11	11	14	22	24	14	20	17	3	17	4	0	12	18
$x \in P$	f	o	l	l	o	w	y	o	u	r	d	r	e	a	m	s

ב) (8 נק') אם הכלל מצפין הוא $e_k(x) = (ax + b) \pmod{m}$ אז הפונקציה ההופכית שלה היא

אם קיימים האיבר ההפכי a^{-1} של a ב- \mathbb{Z}_m אז יש להוכיח שקיימים האיבר ההפכי a^{-1} של a ב- \mathbb{Z}_m אם ורק אם $\gcd(a, m) = 1$.

כיון ⇔

אם $d = \gcd(a, m)$ אז לפי משפט ב'ז' קיימים שלמים s, t, d כך ש- $sa + tm = d$ ו- $\gcd(a, m) = 1$ אם ורק אם $\gcd(a, m) = 1$.

$$sa + tm = 1 \Rightarrow sa = 1 - tm \Rightarrow sa \equiv 1 \pmod{m}.$$

לפיכך קיימים שלם s אשר הוא האיבר ההפכי של a ב- \mathbb{Z}_m .

כיון ⇒

אם קיימים איבר הופכי a^{-1} של a ב- \mathbb{Z}_m אז קיימים שלם q כך ש- $a \cdot a^{-1} \equiv 1 \pmod{m}$.

$$a^{-1}a = 1 + qm \Rightarrow a^{-1}a + (-q)m = 1.$$

לכן קיימים שלמים $t = -q$ ו- $s = a^{-1}$ וכך:

$$sa + tm = 1$$

ולכן לפי משפט ב'ז' $\gcd(a, m) = 1$.

ג) (7 נק')

. $ac \equiv 1 \pmod{b}$ לא זרים וכון וקיים c עבורו
ז"א קיימים שלם q :

$$ac = qb + 1 \Rightarrow ac - qb = 1.$$

לכן קיימים שלמים $s = c$ ו- $t = -q$ עבורם $sa + tb = 1$ זרים, בסתיו a ו- b זרים, בסתיו a ו- b לא זרים.

שאלה 6

א) (13 נקודות)

הכלל מצפין של צופן אפיי הינו $x \in \mathbb{Z}_{26}$ לכל $e_k(x) = ax + b \pmod{26}$ ולכל מפענה הוא $a = 23$ ו- $b = 20$ ו- $y \in \mathbb{Z}_{26}$. בדוקמה זו $a^{-1}(y - b) \pmod{26}$:

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

לפי הדף הנוסחאות האיבר ההפכי של 23 ב- \mathbb{Z}_{26} הוא 17. למסיק:

$$d_k(y) = 17(y - 20) \pmod{26} = 17y - 340 \pmod{26} = 17y + 24 \pmod{26}.$$

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 הגלי בעזרת הכלל מפענה:

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

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 הגלי הוא:

to pass the exam come to class.

ב) (12 נקודות)

יהי d_1, d_2 ו d . $d \mid b$ ו $d \mid a$. כלומר $d = \gcd(a, b)$

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

מכאן

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

לא $\exists q_1, q_2$ חולקים גורמים משותפים (לפי פירוק לגורמים הראשונים) ולכן גם

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

ניסיונות לב:

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