1) (20 נק')

נתונה מערכת עם 3 משתמשים ו-2 קבצים לפי מודל BLP דלהלן:

משתמש	U_1	עם רמה	C
משתמש	U_2	עם רמה	S
משתמש	U_3	עם רמה	TS
קובץ	f_1	עם רמה	S
קובץ	f_2	עם רמה	TS

א. רשום את מטריצת הגישה עבור מערכת זו.

ב. רשום את המטריצה בצורה של ACL ובצורה של C-list.

ג. האם ניתן לממש מטריצה ז ב- Unix? אם כן הראה כיצד, אם לא הצע שנוי קל במערכת Unix שיאפשר ממוש זה.

ד. האם ניתן לממש מטריצה זו ב- Windows-NT? אם כן, הסבר כיצד.

2) (20 נק')
נתונה התוכנית

```
if (X = =Y)
then Z = Y + 1
else  Z = 2 + X
```

א. נניח שרמת X היא l_1 ורמת Y היא l_2 מה צריכה להיות רמת Z המינימלית אם הבדיקה נעשית בזמן קומפילצייה.

ב. נניח שערכי X ו-Y הם 0 או 1 בהסתברות זהה. חשב את כמות האנפורמציה שזרמה עבור כל אחד מערכי Z האפשריים.

3) (10 נק')

בהתייחס לפרוטוקול של Dening בעמוד 53:

1) $A \rightarrow KDC : ID_A ID_B$

2) $KDC \rightarrow A : E_{K_a}\left[K_S ID_B\, T\; E_{K_b}[K_S ID_A\, T]\right]$

3) $A \rightarrow B : \quad E_{K_b}[K_S\; ID_A\, T]$

4) $B \rightarrow A: \; E_{K_S}[N_1]$

5) $A \rightarrow B : \quad E_{K_s}[f(N_1)]$

א. מה המטרה של הפרוטוקול?

ב. מה החשיבות של T בצעד 2?

ג. מה החשיבות של צעד 5?

ד. מדוע לדעתכם פרוטוקול קרברוס הרבה יותר מסובך?

4) (10 נק')

פרטו את היתרונות והחסרונות של צופן זרם לעומת צופן גושי. תנו דוגמה אחת לכל אחד מצפנים אלו.

באיזה מצפנים אלו כדאי להשתמש עבור בסיס נתונים? נמקו.

5) (10 נק')

ציינו ונמקו עבור אילו מהמנגנונים הבאים ניתן ו/או קל לייצג את ההרשאות הבאות:

a) Ken wants his files readable by everyone except his office mate.

b) Mitch and Steve want to share some secret files

c) Same as b) but one file owned by Mitch is readable by everyone except Steve.

המנגנונים הם:

א. רשימות גישה (ACL).

ב. רשימות יכולת (c-list).

ג. הרשאות קבצים ב- Unix.

ד. הרשאות קבצים ב- WINDOWS - NT.

---

6) (10 נק')

נתונות ההרשאות הבאות:

Time:

10:	A GRANTS	R,I	ON EMP TO B WITH GRANT OPTION
20:	A GRANTS	R,D	ON EMP TO C WITH GRANT OPTION
30:	B GRANTS	R,I	ON EMP TO C WITH GRANT OPTION
40:	C GRANTS	R,I,D	ON EMP TO D
50:	B GRANTS	R,I	ON EMP TO D
60:	A GRANTS	R,I	ON EMP TO C WITH GRANT OPTION

א. רשמו את גרף ההרשאות.

ב. עכשיו A מבצע:

REVOKE ALL RIGHTS FROM B CASCADE

תארו את התוצאה:

1) ב- system R

2) ב- SQL 92