מבחן בהנדסה לאחור - 236653

סמסטר חורף תשע״ט

מועד ב׳, 28.02.2019

מרצה: עומר קדמיאל

מתרגל: טל שנקר

חלק ראשון

משך חלק זה של הבחינה: 3 שעות.

בחלק זה של הבחינה ישנן 2 שאלות. ענו על כולן.

בחלק זה 3 עמודים, כולל עמוד זה. וודאו שכל הדפים נמצאים (יש הדפסה משני צידי הדף).

מותר להשתמש בכל חומר עזר, אך אין לשוחח, להתייעץ, לקבל רמז, לתת רמז, או להיעזר בשום אדם אחר על המבחן, על תוכנו, והתשובות לשאלות. <u>יש לפתור את השאלות לבד.</u>

נא לכבות מכשירים סלולריים ושעונים חכמים.

בכל מקרה של שימוש בחומר חיצוני יש לתת הפניה אליו.

תוכנות מותרות: התוכנות אשר נלמדו בקורס. בפרט, אין להשתמש בכלי `decompilation`!

ענו תשובות ברורות ככל האפשר. **<u>נמקו את כל תשובותיכם</u>**. במידה שניתן לענות על שאלה במספר דרכים, **<u>ניקוד מלא יינתן לפתרונות קצרים ופשוטים</u>**.

<u>השאלות והקבצים המצורפים דומים אך אינם זהים לכל הסטודנטים</u>.

הגשה אלקטרונית באתר המקצוע עד השעה 12:00. יש להגיש קובץ ZIP (ואך ורק ZIP) ובו כל קבצי ההגשה. ההגשה כוללת בדיוק את הקבצים הבאים:

1. **קובץ בשם part1_sol.pdf עם התשובות בכתב <u>לכל</u> השאלות.**
2. **קובץ בשם input.txt אותו תצרו בשאלה 2.**

<u>הערה לכל המבחן: בתרגילים הרטובים, אם אינכם מצליחים להגיע לפתרון שרץ בפועל, תארו במילים מה ניסיתם לעשות - זה עשוי לזכות אתכם בניקוד חלקי!</u>

בהצלחה!

שאלה 1 (25 נקודות) - יבש:

לפניכם הפונקציה do_foo. מיקום התווית LOOP הושמט. קראו את קטע הקוד וענו על השאלות שאחריו.

```
Func do_foo (arg_0, arg_1, arg_2)
                                  ... (prologue)
401E00:  8b 3d XX XX XX XX        mov    edi, arg_0
401E06:  8b 0d XX XX XX XX        mov    ecx, arg_1
401E0c:  8b 15 XX XX XX XX        mov    edx, arg_2
401E12: 31 db                     xor    ebx,ebx
401E14: 8b 07                     mov    eax, DWORD PTR [edi]
401E16: 8b 32                     mov    esi, DWORD PTR [edx]
401E18: 01 d8                     add    eax, ebx
401E1a: 31 db                     xor    ebx, ebx
401E1c: 01 f0                     add    eax, esi
401E1e: 11 db                     adc    ebx, ebx
401E20: 89 07                     mov    DWORD PTR [edi], eax
401E22: 83 c7 04                  add    edi, 0x4
401E25: 83 c2 04                  add    edx, 0x4
401E28: 49                        dec    ecx
401E29: 83 f9 00                  cmp    ecx, 0x0
401E2c: 0f 8f XX XX XX XX         jg     LOOP
401E32: 31 c0                     xor    eax,eax
401E34: 40                        inc    eax
                                  ... (epiloge)
```

א. היכן צריך להוסיף את ה label (התווית) LOOP?

ב. מה מבצעות השורות המודגשות? האם ניתן להחליפן בפקודה הבודדת - adc eax, esi? הסבירו.

ג. מה מבצעת הפונקציה? מה תפקיד כל משתנה / רגיסטר? אילו מהמשתנים הינם ערכים ואילו מצביעים?

ד. כתבו בשפה לבחירתכם, את הפונקציה undo_foo המבצעת את הפונקציונליות ההפוכה.

שאלה 2 (25 נקודות) - CrackMe:

למבחן מצורף הקובץ crackme.exe. חקרו את הקובץ וענו על השאלות שלהלן. את התשובות המילוליות יש לרשום בקובץ part1_sol.pdf ואילו את הקלט המבוקש בסעיף ד׳, יש לרשום הן בקובץ part1_sol.pdf והן בקובץ input.txt.

א. תרגמו את הפונקציה **sub_401541** לקוד דמוי C. אין להשתמש בכלי decompilation אלא לתרגם בעצמכם לקוד אשר המתכנת הסביר היה כותב. מה מטרת פונקציה זו בתכנית? מה היא מקבלת כקלט, מחזירה כפלט, וכיצד היא מבצעת את פעולותיה?

ב. חזרו על סעיף א׳ עבור הפונקציה **sub_4015A4**. כיצד שתי הפונקציות שתרגמתם קשורות זו לזו?

ג. תארו את פעולת המשחק על פי הסעיפים הבאים:

a. מהם מבני הנתונים במשחק? כיצד הם מאותחלים? ומה ערכם לאחר האתחול? **ציירו**.
b. איזה קלט מהמשתמש נחשב חוקי?
c. בהינתן קלט חוקי, מהי השפעתו על המשחק? למשל, אם ישנו לוח, כיצד מושפע הלוח? איך משתנים מבני הנתונים כתוצאה מקלט זה?
d. מהם התנאים המובילים לניצחון במשחק?

ד. הגישו קובץ input.txt המוביל לניצחון במשחק. שימו לב שעל הקלט לעבוד, כלומר, להוציא פלט המעיד על הצלחה, עבור הרצת השורה הבאה:

```
crackme.exe < input.txt
```

יש לצטט את הקלט גם ב-part1_sol.pdf.