מבחן בהנדסה לאחור - 236496

סמסטר חורף תש"ף

מועד ב׳, 17.03.2020

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.

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.pdf עם התשובות בכתב <u>לכל</u> השאלות.
2. קובץ בשם crackme.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 (20 נקודות) - יבש:

לפניכם הפונקציה ABC. קראו את הקוד וענו על השאלות שאחריו.

```
ABC proc near (int)

401000: 55                      push   ebp
401001: 89 e5                   mov    ebp, esp
401003: 83 ec 10                sub    esp, 0x10
401006: c7 45 fc 00 00 00 00    mov    DWORD PTR [ebp-4], 0
40100d: c7 45 f8 01 00 00 00    mov    DWORD PTR [ebp-8], 1
401014 <L1>:
401014: 8b 45 08                mov    eax, DWORD PTR [ebp+8]
401017: 89 c2                   mov    edx,eax
401019: c1 ea 1f                shr    edx,0x1f
40101c: 01 d0                   add    eax,edx
40101e: d1 f8                   sar    eax,1
401020: 39 45 f8                cmp    DWORD PTR [ebp-8],eax
401023: 7d 19                   jge    L3
401025: 8b 45 08                mov    eax, DWORD PTR [ebp+8]
401028: 99                      cdq
401029: f7 7d f8                idiv   DWORD PTR [ebp-8]
40102c: 89 d0                   mov    eax, edx
40102e: 85 c0                   test   eax, eax
401030: 75 06                   jne    L2
401032: 8b 45 f8                mov    eax, DWORD PTR [ebp-8]
401035: 01 45 fc                add    DWORD PTR [ebp-4], eax
401038 <L2>:
401038: 83 45 f8 01             add    DWORD PTR [ebp-8], 1
40103c: eb d6                   jmp    L1
40103e <L3>:
40103e: 8b 45 fc                mov    eax, DWORD PTR [ebp-4]
401041: 3b 45 08                cmp    eax, DWORD PTR [ebp+8]
401044: 0f 94 c0                sete   al
401047: 0f b6 c0                movzx  eax, al
40104a: c9                      leave
40104b: c3                      ret
```

א. בכתובות 0x40101E – 0x401014 מתבצעת חלוקה של מספר ב 2.

הסבירו מהו תפקידן של הפקודות המודגשות בין כתובות אלו.

ב. מהו ערך החזרה של הפונקציה ABC עבור הקלט 6?

ג. הסבירו מה עושה הפונקציה ABC.

מה משותף לקלטים אשר ערך החזרה שלהם זהה לזה שרשמתם בסעיף הקודם?

שאלה 2 (30 נקודות) - CrackMe:

למבחן מצורף הקובץ crackme.exe. חקרו את הקובץ וענו על השאלות שלהלן. את התשובות המילוליות יש לרשום בקובץ part1.pdf ואילו את הקלט המבוקש בסעיף ג', **יש לרשום הן בקובץ part1.pdf והן בקובץ crackme.txt.**

א. תרגמו את הפונקציות **sub_401427** ו- **sub_40146A** לפונקציה **בודדת** הכתובה בשפת C. אין להשתמש בכלי decompilation אלא לתרגם בעצמכם לקוד אשר המתכנת הסביר היה כותב. מה מטרת הפונקציה **sub_40146A** בתכנית? מה היא מקבלת כקלט, מחזירה כפלט, וכיצד היא מבצעת את פעולותיה?

ג. התכנית שקיבלתם הינה משחק. תארו את פעולת המשחק על פי הסעיפים הבאים:

1. מהם מבני הנתונים במשחק? כיצד הם מאותחלים? (שימו לב, ישנם שני מבני נתונים)
2. איזה קלט מהמשתמש נחשב חוקי?
3. בהינתן קלט חוקי, מהי השפעתו על המשחק? למשל, אם ישנו לוח, כיצד מושפע הלוח? איך משתנים מבני הנתונים כתוצאה מקלט זה?
4. מהם חוקי המשחק? בנוסף, מהם התנאים המובילים לניצחון במשחק?

ד. מצאו ארגומנטים וקלט המובילים לניצחון במשחק.עליכם להגיש קובץ crackme.txt המכיל את הקלט. שימו לב שעל הקלט לעבוד, כלומר, להוציא פלט המעיד על הצלחה, עבור הרצת השורה הבאה ב Windows Command Line:

crackme.exe < crackme.txt

יש לצטט את הקלט גם ב part1.pdf.