ארכיטקטורת מחשב – תרגיל בית 05

אסמבלי – מחסנית מתקדם

כללי:

נושאי התרגול:

- עבודה זו מסכמת את כל החומר שנלמד השנה באסמבלי

לאורך כל הסמסטר העבודה היא אישית - אסור לשבת לעבוד ביחד. עם זאת, מותר ואפילו מומלץ להתייעץ אחד עם השני.
במידה ואתם מתקשים נסו להעזר בגוגל ובמידה ועדיין אתם מתקשים פנו למדריך!

הוראות להגשת התרגיל:

1. עבור כל התכניות שתכתבו באסמבלי, אנא השתמשו בתבנית הבאה:

```
org 100h
[your code here]
mov ah, 0
int 16h
ret
```

2. יש לשמור את הקבצים עם סיומת asm, כאשר שם הקובץ כולל את מספר השאלה. לדוגמא, תוכנית עבור שאלה מס' 1, ישמר בקובץ שנקרא 1.asm.
3. לאחר שכתבתם את הקוד, הריצו את תכניתכם ועקבו אחר פעולתה באמצעות כפתור emulate. וודאו כי תכניתכם פועלת כראוי ומבצעת את הנדרש.
4. יש להגיש קובץ zip (בלבד!) המכיל את כל התוכניות. יש להקפיד על השם של הקובץ לפי התבנית הבאה: 05_israel_israeli.zip (כאשר 05 מציין את מס' העבודה, וישראל ישראלי הוא שם פרטי ומשפחה).

המשך בעמוד הבא

שאלה 1 – קונבנציות קריאה לפונקציות

לפניכם קוד פונקציה.

א. מהי קונבנציית הקריאה לפונקציה? הסבירו לפי מה קבעתם זאת
ב. כיתבו את הפונקציה בשפת C
ג. כיתבו קוד אסמבלי שקורא לפונקציה, דגש על העברת פרמטרים נכונה ומחסנית מאוזנת בסיום הקריאה

```
mystery:
   push    bp
   mov     bp, sp
   mov     ax, [bp+6]
   imul    ax
   mov     dx, ax
   mov     ax, [bp+4]
   shl     ax, 2
   imul    [bp+8]
   sub     dx, ax
   mov     ax, dx
   pop     bp
   ret
```

שאלה 2 – CrackMe's

קרדיט לחידות: יאיר מירסקי, חגי לוי

במשימה זו תקבלו ארבעה קבצים המכילים קוד בשפת מכונה. תצטרכו להשתמש בתוכנת הדיס-אסמבלר על מנת לפענח מה הקלט שהמשתמש נדרש להזין כדי להגיע למסר ההצלחה.

א. הורידו את הקבצים CODE01, CODE02, CODE03, CODE04
ב. עיקבו אחרי ריצת התוכניות
ג. כיתבו במסמך word מה הבדיקה שמתבצעת על הקלט של המשתמש, ומה הסיסמה הנדרשת.

שאלה 3 – תכנות יצירת זוג מפתחות אלגוריתם RSA

אלגוריתם RSA הוא אלגוריתם נפוץ להצפנת מידע שנשלח באינטרנט. האלגוריתם מבוסס על זוג מפתחות, מפתח ציבורי ומפתח פרטי, שיש ביניהם קשר מתימטי מסוים. תוכלו לצפות בהסבר על האלגוריתם ותהליך יצירת המפתחות בסרטון הבא:

https://www.youtube.com/watch?v=Pq8gNbvfaoM

בתרגיל זה תתכנתו יצירת זוג מפתחות.

בקוד יוגדרו הקבועים הבאים: מספר ראשוני P, מספר ראשוני Q. באמצעותם יחושב מספר הנקרא Totient, שערכו שווה ל-

(P-1)*(Q-1)

התכנית תקלוט מהמשתמש מפתח ציבורי, תבדוק אם הוא עומד בתנאים הנדרשים לפי אלגוריתם RSA, ותייצר מפתח פרטי.

התנאים הנדרשים למפתח ציבורי תקין:

- ראשוני (כיתבו פרוצדורה שמבצעת בדיקה אם מספר ראשוני, גירמו לה לרוץ מהר ככל האפשר באמצעות דילוג על בדיקה של מספרים מיותרים)
- קטן מה- Totient
- ה-Totient מודולו המפתח הציבורי אינו שווה לאפס

אם הבדיקה עברה בהצלחה, יחושב המפתח הפרטי על פי האלגוריתם הבא, שייכתב בפרוצדורה נפרדת:

- עוברים על כל המספרים שקטנים מה- Totient
- מחפשים מספר שכאשר כופלים אותו במפתח הציבורי ומבצעים לתוצאה מודולו עם ה-Totient, מתקבל 1, כמו בשורת הקוד הבאה:

  (pubkey*num) % TOTIENT == 1

  מספר זה הינו המפתח הפרטי. התכנית תדפיס אותו.

  שימו לב- כדי שזמן הריצה לא יהיה ארוך מדי מומלץ ש-P ו-Q יהיו קטנים יחסית, בני שתי ספרות.

בהצלחה!