מדריך מקוצר בעברית לשימוש ב- GDB

הפעלת הדיבאגר:

בהינתן קובץ אסמבלי file.s אנו ניצור ממנו קובץ ריצה ע"י:

```
gcc -g -o exeFile file.s
```

כעת נריץ את הדיבאגר ע"י

```
gdb exeFile
```

פקודות חשובות של הדיבאגר:

הסבר	הפקודה ב-GDB
	התחלה וסיום:
יציאה מ-GDB.	q[uit]
הרצת התוכנית.	r[un]
הפסקת הרצת התוכנית.	kill
	Breakpoints:
שם נקודת עצירה בכניסה לפונקציה XXX.	b[reak] XXX
שם נקודת עצירה בפקודה שנמצאת בכתובת המצוינת.	b[reak] *0x80483c3
מוחק את נקודת עצירה מספר N.	delete N
מוחק את כל נקודות העצירה.	delete
	התקדמות בקוד:
מתקדם פקודה אחת בקוד.	stepi
מתקדם N פקודות בקוד.	Stepi N
כמו stepi אבל מדלג מעל קריאה לפונקציה.	nexti
ממשיך להתקדם בקוד עד נקודת העצירה הבאה או עד סיום התוכנית (אם אין עוד נקודות עצירה).	c[ontinue]
רץ עד פקודת החזרה מהפונקציה הנוכחית (במידה והיא לא הפונקציה הראשית).	finish
(משמש בעיקר כדי להשיג כתובת פקודות ל-break ו-print).	***בחינת הקוד:***
מבצע disassemble לקוד הפונקציה הנוכחית.	disas
מבצע disassemble לקוד הפונקציה XXX.	disas XXX
מבצע disassemble לקוד הפונקציה שנמצאת סמוך לכתובת המצוינת.	disas 0x80483b7
מבצע disassemble לקוד בטווח הכתובת המצוין.	disas 0x80483b7 0x80483c7
	בחינת מידע:
מדפיס את תוכן האוגר %XXX בבסיס 10.	print $XXX

מדפיס את תוכן האוגר %XXX בבסיס 16.	`print /x $XXX`
מדפיס את תוכן האוגר %XXX בבסיס 2.	`print /t $XXX`
מדפיס את הערך של המספר 0x100 בבסיס 10.	`print 0x100`
מדפיס את הערך של המספר 555 בבסיס 16.	`print /x 555`
מדפיס את הערך של אוגר %XXX +8 בבסיס 16.	`print /x ($XXX+8)`
מדפיס את הערך של ה-int שנמצא בכתובת המצוינת.	`print *(int *) 0xbffff890`
מדפיס את הערך של ה-int שנמצא בכתובת %XXX+8	`print *(int *) ($XXX+8)`
בוחן את 2 המילים (4 בתים) המתחילים בכתובת המצוינת.	`x/2w 0xbffff890`
בוחן את 20 הבתים הראשונים בפונקציה XXX.	`x/20b XXX`
	פקודות נוספות:
נותן מידע על ה-frame stack הנוכחי.	`info frame`
מדפיס את הערכים של כל הרגיסטרים	`info registers`
מדפיס את תפריט העזרה של GDB	`help`

ל- GDB יש הרבה פקודות ואופציות, אך בטבלה הנ"ל נמצאות רוב הפקודות להן תזדקקו.

מקורות נוספים למידע לגבי GDB בשפת אסמבלי ובכלל:

http://www.gnu.org/software/gdb/documentation/

http://www.csee.umbc.edu/~cpatel2/links/310/nasm/gdb_help.shtml

http://heather.cs.ucdavis.edu/~matloff/UnixAndC/CLanguage/Debug.html

*web.cecs.pdx.edu/~apt/cs322_2005/**gdb**.pdf*