

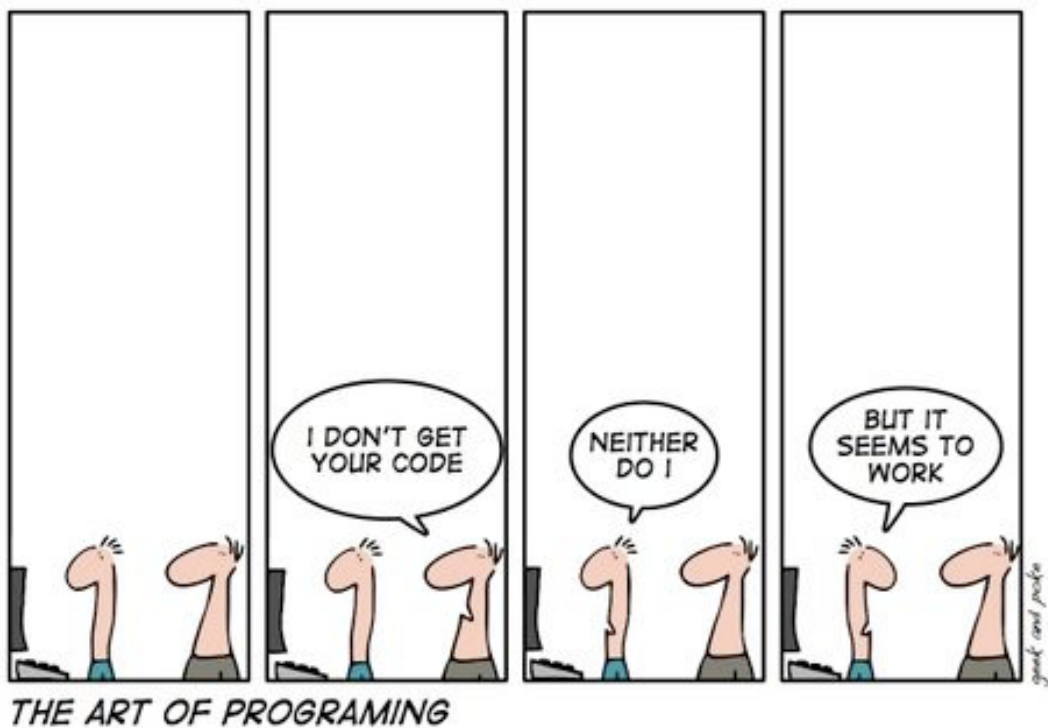
## תרגיל בית 1 בהנדסה לאחור

### הכרות עם אסמבלי ומבנה קובץ ההרצה

236496

סמסטר אביב תשפ"ג

הגשה בזוגות עד 30.04.2023 בשעה 23:59



לשאלות על התרגיל: [kinsbruner@cs.technion.ac.il](mailto:kinsbruner@cs.technion.ac.il)

נא לרשום כחלק מנושא ההודעה "236496" (ללא המרכאות).

הקפידו על הגשת קבצים עם השמות הנכונים כפי שמוגדר במסמך זה.

טעות בשם הקובץ תגרור ציון 0 ע"י הבודק האוטומטי בחלק הרלוונטי.

לפני ההגשה, ודאו שההגשה שלכם תואמת את הנחיות ההגשה בסוף התרגיל.

## חלק א' – התקנת תוכנות – לא להגשה

יש לעבוד בסביבת Windows. במידה ואין לכם אחת זמינה התקינו מכונה וירטואלית.

במהלך הקורס נשתמש במספר רב של תוכנות. אנו ממליצים להתקין אותן מוקדם ככל הניתן:

- **Visual Studio** - ניתן להוריד גרסת Express חינמית מאתר Microsoft (מתאימה לדרישות הקורס) או לחלופין לקבל גרסה מלאה דרך ה- MSDN (זמין בקישור <https://elms.cs.technion.ac.il>).
- **GCC** – ניתן להשתמש ב MinGW. שימו לב שתומך בקימפול ל - 32 ביט.
- **IDA free** – [https://www.hex-rays.com/products/ida/support/download\\_freeware.shtml](https://www.hex-rays.com/products/ida/support/download_freeware.shtml)
- **Immunity Debugger** - ניתן להוריד מ: <http://debugger.immunityinc.com>
- **VMWare** - ניתן להוריד גרסה חינמית "VMware Player" (מתאימה לדרישות הקורס) או גרסה מלאה דרך ה VMWare store (זמין בקישור - <https://elms.cs.technion.ac.il/>).
- **Windows 7 32 / 64bit** – ISO של Windows 7 להתקנה על ה VMWare. ניתן להוריד מתיקיית הדרייב הבאה בקישור מטה.
- **CFF Explorer** – ניתן להוריד מהקישור הבא: [https://ntcore.com/?page\\_id=388](https://ntcore.com/?page_id=388)

תוכלו למצוא את קבצי ההתקנה גם בתיקיית הדרייב הבאה:

<https://drive.google.com/drive/folders/1an0lVTb9F6uRwntPwXwzGluyTPDnjiuj?usp=sharing>

## חלק ב' – היכרות ראשונית עם קוד C מהודר

בתרגיל זה סופקו לכם שלושה קבצים:

- partb.nopt.s - קוד אסמבלי שנוצר ע"י GCC ללא אופטימיזציות
- partb.opt.s - קוד אסמבלי שנוצר ע"י GCC עם אופטימיזציות (עם הדגל -O2)
- partb.exe - תכנית מקומפלט שנוצרה ע"י GCC.

שלושת הקבצים כולם נוצרו מאותה תוכנית C. התכנית המקומפלט partb.exe תקינה, אך בשני קבצי האסמבלי נפלו טעויות, **במיקומים שאינם בהכרח זהים**, המפריעות לריצה התקינה של התכנית. עליכם לאתר את הטעויות ע"י השוואת קבצי הקוד וחקר קובץ ההרצה שקיבלתם.

כתבו תיאור קצר של כל אחת מהטעויות שמצאתם, וכיצד תיקנתם אותן. עליכם להגיש בנוסף גם את קבצי הקוד המתוקנים partb.nopt.s ו partb.opt.s.

## חלק ג' – Rivals of Catan.

בתרגיל זה נתחיל בהתמודדות עם קבוצה קטנה של סטודנטים המנסים לפגוע בפעילותו התקינה של עולם הקטאן האינטרנטי, הידוע גם כ Catan Universe. הסטודנטים המדוברים החליטו במצב של ייאוש כבד שנמאס להם להפסיד ללא הרף במשחק, ולכן החלו בהתארגנות ממוחשבת במטרה לשבש את המשחק ולמנוע את היכולת לנצח במשחק מכלל המשתמשים.

גילינו כי הם חלק מפעילותם או כולה, מרוכזת באתר שיועד להם בלבד ונגיש בכתובת הבאה:

<http://51.144.113.30:10224>

האתר אינו נגיש לכל אדם ויש צורך באימות חד פעמי על מנת לאפשר הרשאה למחשב שלכם לגשת לתוכן המצוי בכתובת זו. אל דאגה, הצלחנו לשים ידינו על סיסמא אחת שתאפשר לכם לגשת לאתר ולהתחיל בפעילות כנגד התארגנות זו. הסיסמא שלך היא (ללא רווחים):

NPLKH4Z4BNC8DWD7

משימתכם היא למצוא את פרטי ההתחברות של כל המשתמשים במערכת ואת זהויותיהם, במידה וקיימות. על מנת להתחיל, מומלץ להציץ בקוד המקור של האתר. ניתן לעשות זאת באמצעות ה Developer Console הקיים בדפדפנים השונים (F12 בדרך כלל). כאשר אתם נתקלים בקובץ הרצה (.exe) או בקובץ קוד מקור, חקרו אותו והבינו מהו הקלט שהתכנית מצפה לה, ואיזה קלט יכול לשרת את מטרתכם. במידה ואתם נתקלים בתכנית בעלת כמה שלבים, עליכם לעבור את כל השלבים על מנת להצליח.

עליכם לתאר **במפורט** את הדרך שבה פעלתם על מנת להשלים את המשימה.

במידה ואתם נתקלים בפונקציה rand\_32 אין צורך להתעמק בה, היא מחזירה מספר רנדומלי בהינתן seed המועבר אליה, זוהי פונקצייה בה משתמשת הקבוצה לייצור מספרים בצורה רנדומית.

שימו לב כי אין צורך בהכרות מוקדמת עם חוקי המשחק על מנת להשלים את התרגיל. אנו נשלים את החלקים הרלוונטיים תוך כדי ההתקדמות בתרגילי הבית 😊. בתרגיל זה נלמד מה ניתן לעשות עם המשאבים המחולקים לשחקנים לאחר כל הטלה של הקוביות. במשחק חמישה סוגי משאבים, משאבים אלו משמשים לבנייה של דרכים, יישובים וערים, ורכישה של קלפי פיתוח. לפניכם קלפי המשאבים ומחירי הבניה:



BUILD COSTS				
Road				
Settlement				
City				
Development				

## הוראות הגשה

עליכם הגיש קובץ zip המכיל בתוכו בתיקייה הראשית את הקבצים הבאים:

- קובץ id.txt – על קובץ זה להכיל את מספר תעודת הזהות של הסטודנט שגרסתו נבחרה.
- dry.pdf - המכיל את הפתרונות וההסברים שלכם לחלקים ב' וג'.
- partb.opt.s - הקוד המתוקן עבור partb.opt.s (חלק ב').
- partb.nopt.s - הקוד המתוקן עבור partb.nopt.s (חלק ב').
- כל קובץ רלוונטי אחר הדרוש על מנת להשלמת חלק ג'.
- אתם יכולים להגיש כל קובץ נוסף כרצונכם בתוך תיקייה בשם extras (אם אין לכם קבצים נוספים, הוסיפו תיקייה ריקה בשם זה).

### שמות קבצים בחלק ג':

- קובץ input עבור קובץ הרצה file.exe או file.S יקרא באותו השם עם סיומת txt כלומר file.txt.
- קובץ המכיל ארגומנטים עבור שורת הפקודה של קובץ הרצה בשם file.exe (לא כולל redirection) יקראו באותו השם עם סיומת args, כלומר file.args.
- שמות הקבצים האחרים אותם תגישו יהיו זהים לאלו שתדרשו במהלך התרגיל עצמו.

### שומעים חופשיים

שומעים חופשיים בקורס אשר אין להם גישה לתרגיל מוזמנים לפנות אל אלעד במייל, ולקבל עותק.

**בהצלחה!**