פרויקט מסכם באסמבלי - הצפנה ופענוח בצופן הזזה

על ידי : אמיר וולברג

מוגש ל :אורי לוי

3.6.2018



***תוכן עניינים -***

עמוד 1 : דף שער

עמוד 2 : תוכן עניינים

עמודים 3-4 : מדריך הפעלה והסבר בסיסי לדרך העבודה של התוכנה

עמודים 5-6 : רשימת פרוצדורת והסבר למה שהן עושות

עמודים 7-8 : רשימת משתנים והסבר לתפקידם

עמוד 9 : תרשים זרימה

עמודים 10-11 : מסכים בפרויקט

**מדריך הפעלה :**

לאחר הפעלת התוכנה ישנן 2 אפשרויות למשתמש והן :

א) לאחר שמכניסים את התו "1" התוכנה תבקש להכניס הודעה עד 254 תווים , לאחר מכן היא תבקש להכניס סיסמא עד 254 תווים , ואז התוכנה מחברת את כל תווי הסיסמא ומורידה מהם 26 עד שערך הסיסמא קטן מ26 , כשזה קורה מוסיפה התוכנה את ערך הסיסמא לכל אחד מן התווים בהודעה ומדפיסה את מה שהיא מקבלת.

לסיום מבקשת התוכנה את הסיסמא אם ניתנת הסיסמא הנכונה התוכנה מורידה את הערך מכל תווי ההודעה ומדפיסה אותה אם לא ניתנת הסיסמא הנכונה התוכנה לא מחזירה דבר.

ב) לאחר שמכניסים את התו "2" מקבלים אפשרות לפענח הודעה המוצפנת בצופן הזזה ללא ידיעת הסיסמא , המשתמש מכניס הודעה והתוכנה עושה את שלושת הדברים הבאים :

1. היא מחפשת את התו שמופיע הכי הרבה ומשווה אותו לE האות שמופיעה הכי הרבה בשפה האנגלית ואז היא מוצאת את ההפרש בינו לבין E ומורידה לכל התווים את ההפרש הזה ומדפיסה לכם את ההודעה - בחלק זה יש עדיפות לאות שמופיעה הכי הרבה פעמים האחרונה בסדר האלפבת מכיוון שהאות שמופיעה בפעם השנייה הכי הרבה פעמים היא A שמגיעה בסדר לפני E.

התוכנה שואלת אם אתה רוצה לנסות דרך פענוח שונה אם כן 2 קורה אם לא החלק של הפענוח מסתיים .

1. לאחר מכן היא מחפשת את התו שמופיע הכי הרבה ומשווה אותו לA האות שמופיעה הכי הרבה אחרי E בשפה האנגלית ואז היא מוצאת את ההפרש בינו לבין A ומורידה לכל התווים את ההפרש הזה ומדפיסה לכם את ההודעה - בחלק זה יש עדיפות לאות שמופיעה הכי הרבה פעמים הראשונה בסדר האלפבת מכיוון שהאות A היא האות הראשונה באלפבת האנגלי.

התוכנה שואלת אם אתה רוצה לנסות דרך פענוח נוספת אם כן 3 קורה אם לא החלק של הפענוח מסתיים.

1. יש 26 אותיות באלפבת האנגלי , החלק הזה של התוכנה מוריד את הערכים של התוכנה 26 פעמים וכל פעם מראה לכם את התוצאה ושואל אם אתה מרוצה מהפענוח או אם אתה רוצה לנסות שוב . דבר זה קורה רק כאשר אתה מאשר שאף אחת מהדרכים האחרות לא עבדו (בדרך כלל יקרה במשפטים קצרים מאוד בהם E או A הן לא האותיות המופיעות הכי הרבה פעמים).

לסיום התוכנית תשאל אם אתם רוצים לפענח הכל מחדש , לסיים את התוכנית או לחזור למסך פתיחה.



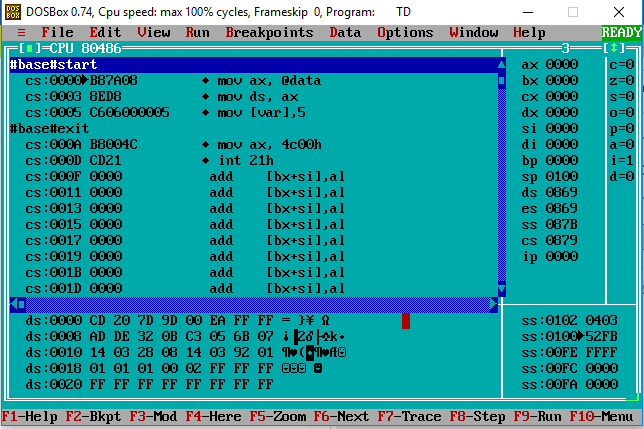
***רשימת פרוצדורות -***

|  |  |
| --- | --- |
| **שם הפרוצדורה** | **מה הפרוצדורה עושה** |
| ***printchar\_space*** | מקבל תו בdl מדפיס אותו ואז רווח |
| ***tryagainproc*** | מדפיס מחרוזת tryagain |
| ***decaproc*** | מדפיס מחרוזת deca |
| ***gotomainmenu*** | מדפיס מחרוזת mainmenu |
| ***encgotomainmenu*** | מדפיס מחרוזת encmainmenu |
| ***baddec*** | מדפיס מחרוזת wrongdec |
| ***openmsg*** | מדפיס מחרוזת open |
| ***printstar*** | מדפיס מחרוזת stars |
| ***message*** | מדפיס מחרוזת msgmsg ומקבל מחרוזת get\_msgencrypt |
| ***decmessage*** | מדפיס מחרוזת decmsg ומקבל מחרוזת get\_decmsg |
| ***decryptpass*** | מדפיס מחרוזת passconfirm ומקבל מחרוזת confirmpass |
| ***printline*** | מדפיס מחרוזת line |
| ***password*** | מדפיס מחרוזת msgpass ומקבל מחרוזת get\_msgpass |
| ***printchar*** | מקבל תו בdl ומדפיס אותו |
| ***print\_newline*** | יורד שורה |
| ***get\_char*** | מקבל תו מהמשתמש ושם אותו בal |
| ***convert\_key\_to\_number*** | משתמש בסיסמא שניתנה על ידי המשתמש , מחבר את כל התווים שלה ושם את התוצאה בax לאחר מכן מוריד 26 מax שוב ושוב עד שהערך בax נמוך מ26 |
| ***encrypting*** | מוסיף לכל אחד מהתווים בהודעה את הערך שבax ואז מדפיס את ההודעה שהתקבלה |
| ***Decryptingwithpass*** | מבקש להקליד את הסיסמא , בודק אם היא נכונה , אם כן הוא מוריד את הערך שבax מכל אחד מהתווים שבהודעה ומדפיס את ההודעה שהתקבלה (שהיא בעצם ההודעה שהוכנסה בהתחלה) אם לא הוא קופץ לחלק הבא בתוכנית |

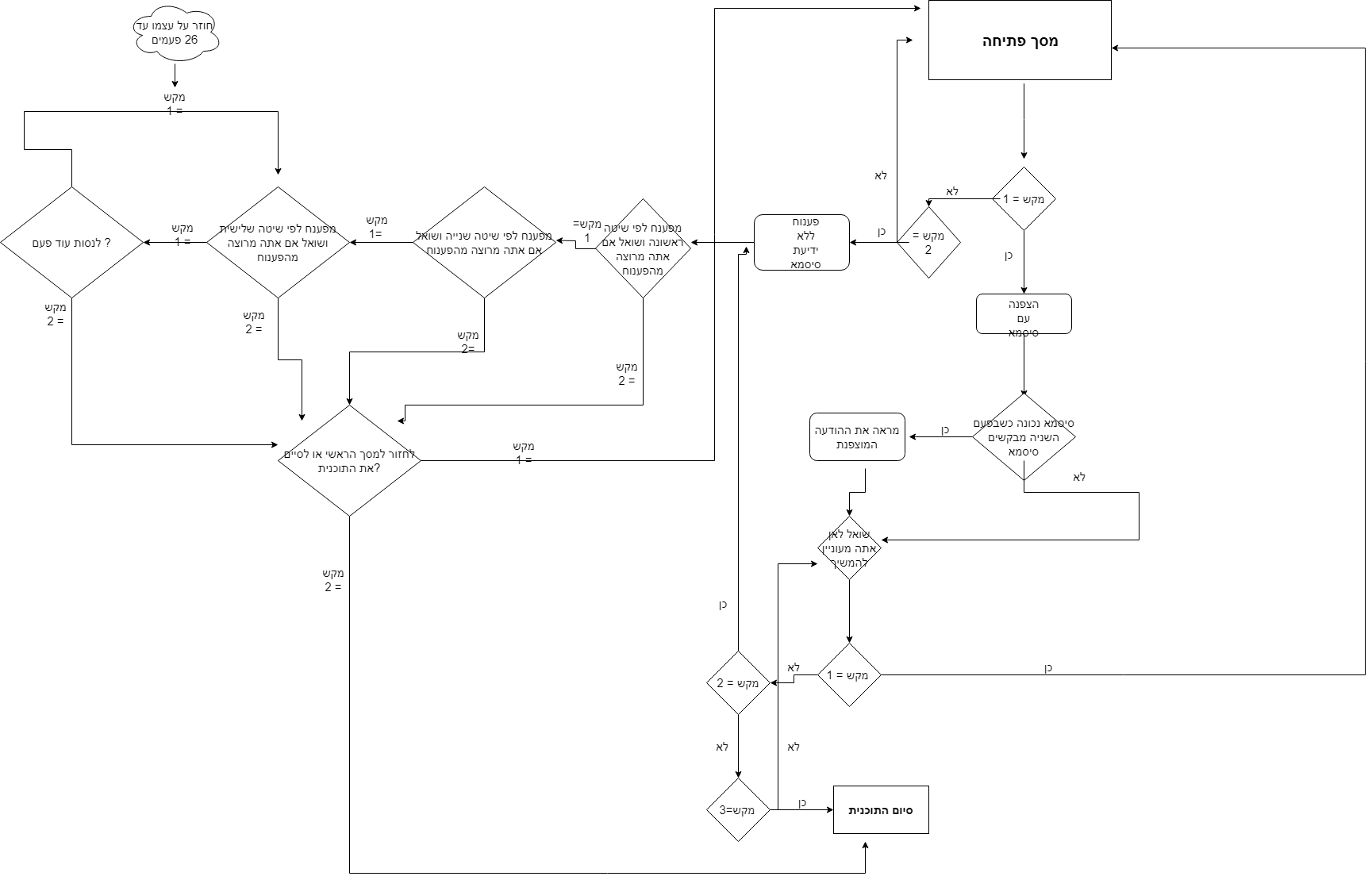
|  |  |
| --- | --- |
| ***inputenc*** | קורא לפרוצדורות שמקבלות את ההודעה והסיסמא בחלק של ההצפנה |
| ***project*** | קורא לכל הפרוצדורות הראשיות , יוצר את גוף הפרויקט ומבצע את כל המעברים בין החלקים השונים בפרויקט ואת כל הקפיצות |
| ***brute\_decryption*** | מוריד מכל אות בהודעה את הערך 1 שוב ושוב 26 פעמים ומדפיס אותה לאחר כל פעם ולאחר מכן שואל אם אתה רוצה להוריד שוב את הערך |
| ***decrypting*** | מוצא את המספר שמופיע הכי הרבה פעמים ושם את ההפרש בינו לבין e בbx  לאחר מכן מוריד bx מכל אחת מהאותיות בהודעה ומדפיס את מה שהוא מקבל  אחר כך שואל אם אתה רוצה לנסות שוב ומבצע את כל זה שוב פעם אבל עם a ולא e ולבסוף שואל אם אתה רוצה לנסות שוב ואם כן קורא ל brute\_decryption |
|  |  |

**רשימת משתנים -**

|  |  |
| --- | --- |
| **משתנה** | **מטרת המשתנה** |
| ***msgpass*** | מבקש להכניס סיסמא המיועדת להצפנה |
| ***get\_msgpass*** | מקבל את הסיסמא המיועדת להצפנה |
| ***decmsg*** | מבקש להכניס הודעה המיועדת לפענוח |
| ***get\_decmsg*** | מקבל את ההודעה המיועדת לפענוח |
| ***line*** | מדפיס שורת הפרדה המיועדת לעיצוב הפרויקט |
| ***msgmsg*** | מבקש להכניס הודעה המיועדת להצפנה |
| ***get\_msgencrypt*** | מקבל את ההודעה המיועדת להצפנה |
| ***passconfirm*** | מבקש את הסיסמא המיועדת לפענוח ההודעה המוצפנת |
| ***confirmpass*** | מקבל את הסיסמא המיועדת לפענוח ההודעה המוצפנת |
| ***stars*** | מדפיס שורת כוכביות המיועדת לעיצוב הפרויקט |
| ***open*** | מבקש להכניס 1 בשביל להצפין ו2 בשביל לפענח |
| ***tryagain*** | שואל אם אתה מעוניין לנסות עוד פעם או לא |
| ***mainmenu*** | שואל אם אתה מעוניין לחזור למסך הפתיחה או לסיים את התוכנית |
| ***encmainmenu*** | שואל אם אתה מעוניין להמשיך עם פענוח , לחזור למסך הפתיחה או לסיים את התוכנית |
| ***deca*** | שואל אם אתה מרוצה מהפענוח ואם אתה רוצה לנסות שוב פעם |
| ***letter\_counter*** | מערך מונים הבודק מהי האות שמופיעה הכי הרבה פעמים בהודעה לפענוח |
|  |  |



תרשים זרימה :



*מלבן* - מסך פתיחה / סיום תוכנית

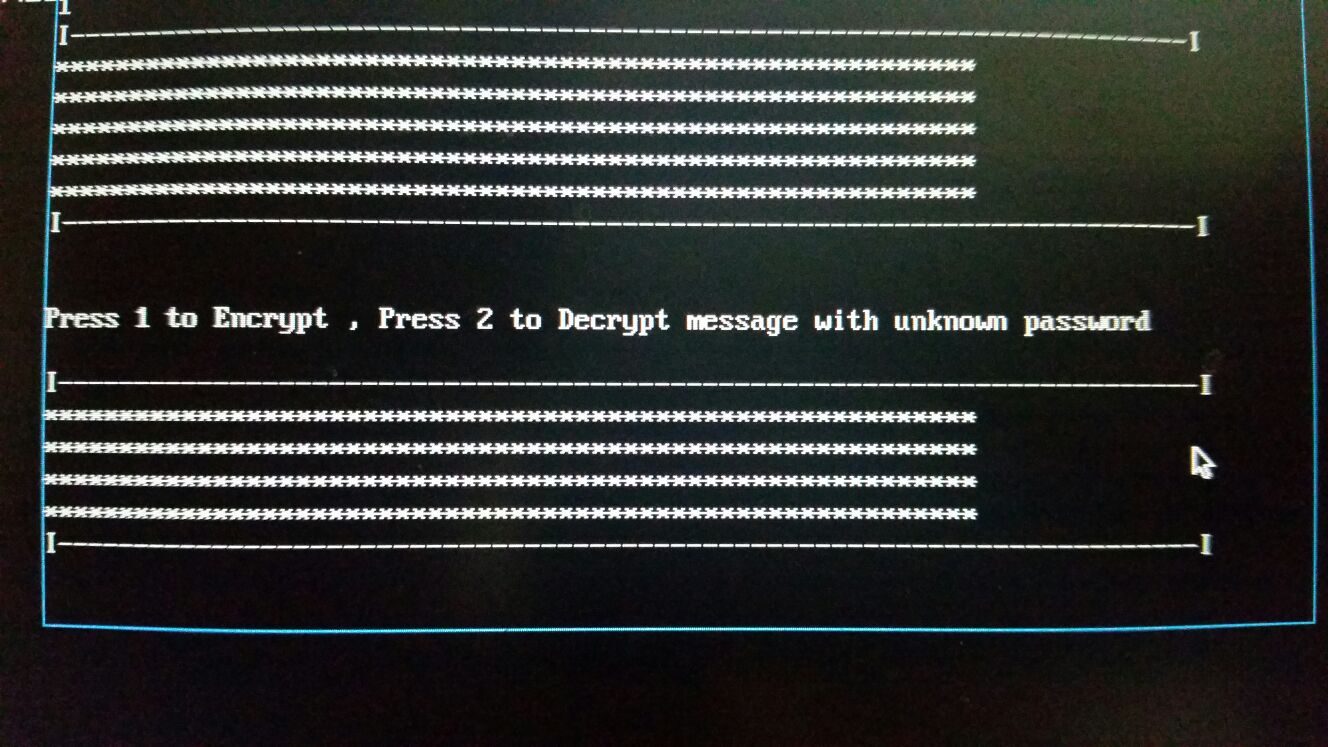
*מלבן מעוגל בקצוות* - חלק בפרויקט עם רק המשך אחד

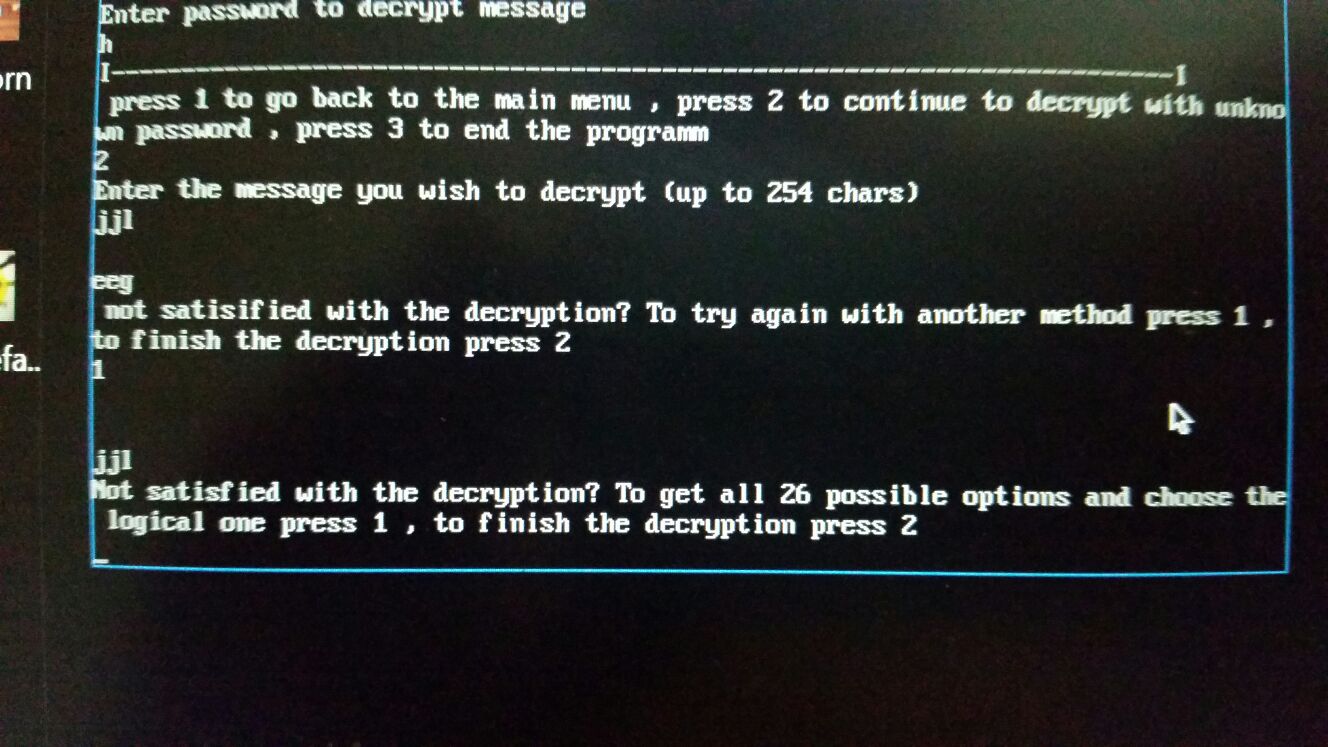
*ענן* - הסבר

*מעוין* - חלק בפרויקט עם 2 או יותר אפשרויות המשך

***מסכים בפרויקט :***

מסך פתיחה -



מסך פענוח - 

מסך הצפנה - 