

Data Encryption Standard

הצפנה סימטרית המבוצעת באסמבלר 8086

שם המתכנת: אייל גודוביץ'  
תעודת זהות: 315116707  
מורה מלווה: אורית קופרמן, יואב לוי  
כיתה: י6  
בית ספר: כפר הנוער מאיר-שפיה

**תוכן עניינים**

[מבוא 3](#_Toc419233321)

[נושא העבודה 4](#_Toc419233322)

[מהי הצפנה ? 5](#_Toc419233323)

[מהי הצפנה סימטרית ? 6](#_Toc419233324)

[סטנדרנט הצפנת המידע – די.אי.אס 7](#_Toc419233325)

[תיאור הצופן 7](#_Toc419233326)

[אופן הפעולה 7](#_Toc419233327)

[אופן ההפעלה 8](#_Toc419233328)

[אופן ההפעלה - המשך 9](#_Toc419233329)

[אופן ההפעלה - המשך 10](#_Toc419233330)

[אופן ההפעלה - המשך 11](#_Toc419233331)

[גרסאות המערכת 12](#_Toc419233332)

[תיעוד והסבר הפתרון 13](#_Toc419233333)

[תרשימי זרימה 14](#_Toc419233334)

[תרשים הזרימה עבור התוכנית הכללית: 14](#_Toc419233335)

[תרשים הזרימה עבור פרצדורת הרחבת המפתח 15](#_Toc419233336)

[רשימת הפעולות 16](#_Toc419233337)

[רשימת הפעולות - המשך 17](#_Toc419233338)

[רשימת הפעולות - המשך 18](#_Toc419233339)

[קוד התוכנית 19](#_Toc419233340)

[דוגמאות הרצה 20](#_Toc419233341)

[סיכום אישי 21](#_Toc419233342)

# מבוא

שם העבודה:

יישום סטנדרנט ההצפנה בשפת אסמבלר 8086

הקובץ **:**

בעבודה ישנם מספר קבצים, הקובץ הראשי נמצא בכתובת היחסית הבאה :

Codes\Des.ASM

קבצים נלווים:

כל הקבצים אשר בתיקיה "קודס" הם הכרחיים לחלוטין לקיום והרצת הפרוייקט בדוסבקס.  
להלן רשימת הקבצים:

Codes\Des.asm  
Codes\Encrypt.asm  
Codes\Key.asm  
Codes\Perm.asm  
Codes\Library\Base.asm  
Codes\Library\Console.asm  
Codes\Library\File.asm  
Codes\Library\String.asm

סביבת העבודה:  
טורבו אסמבלר

סביבת הפיתוח:

סאבליים טקסט 2, סאבליים טקסט הוא עורך טקסט המפותח על ידי אדם עצמאי לנוחות שאר המתכנתים בעולם, נחשב לאחד העורכים היותר נחשבים כיום.

סביבת ההרצה:  
סביבת ההרצה היא דוסבוקס, גרסה 0.74.  
למען נוחות המשתמש, צורפו לדוסבוקס עזרים אשר נכתבו על ידי, אשר מאפשרים לאדם ללא ידע להשתמש בתוכנה ללא התעמקות עמוקה ומחקר ארוך במדריך למשתמש.

# נושא העבודה

**­­­­**נושא העבודה הוא יישום ההצפנה די.אי.אס באמצעות שפת אסמבלי 80386.  
הרעיון הכללי בתחילת הדרך היה ליצור תוכנה פשוטה, עם ממשק מפואר יחסית ונוח לשימוש, המאפשר למשתמש להכניס מחרוזת (אל תוך קובץ), להכניס מפתח הצפנה שקל לזכור ( 8 תווים בלבד ! ), ולאפשר לו להצפין את אותו הטקסט בקלות ללא דאגה וחיפוש כלים באינטרנט.

בנוסף, כמובן למשתמש יש את האפשרות לפענח את הטקסט אשר הצפין, לדוגמא, במידה ואני אצפין הודעה שארצה לשלוח לחבר בלי שאף אדם אחר יבין, אסכם איתו מראש על מפתח ההצפנה, ולאחר מכן אשלח לו בדרך כל שהיא את הטקסט שהצפנתי באמצעות מפתח ההצפנה, אותו חבר יוכל לאחר מכן לפענח את אותו טקסט מוצפן באמצעות המפתח, ללא שכל אדם אחר יוכל להבין מה כתוב בטקסט המוצפן ללא המפתח הדרוש.

לאחר שהתחלתי לחקור בנושא ההצפנות, ניגשתי להצפנות הפשוטות ביותר והקדומות ביותר, והבולטת מהן הייתה די.אי.אס ( סטנדרנט הצפנת המידע ), אשר מאפשרת לאדם להצפין כל דבר, באופן יעיל ומהיר, בצורה שבאותם זמנים נחשבה בלתי אפשרית לפיענוח ללא המפתח הנכון, מכיוון שיש 2 בחזקת 55 אפשרויות למפתחות.  
אפילו היום, המחשבים הכי חזקים יצטרכו לעבוד במשך זמן רב על מנת לפענח הודעה קטנה, וזאת גם במידה וידוע לנו לפחות קצת מידע בנוגע לתוכן ההודעה.

אחת הסיבות היותר משפיעות שגרמו לי לבחור בהצפנה הזו ולא הצפנה אחרת, היא שהיא קשה מאד לביצוע בשפת אסמבלר 8086, מכיוון שההצפנה מבוצעת על בלוקים של מידע בגודל 64 סיביות, והרגיסטרים שלנו מגיעים אך ורק עד 16 סיביות ( מילה ), לכן, למען ההיגיון והפשטות, עברתי לשפת אסמבלר 80386, המאפשרת שימוש ברגיסטרים מוארכים, בגודל 32 סיביות ( מילה כפולה ).

למרות המעבר, הפיתוח מסובך, ודורש המון השקעה.

## מהי הצפנה ?

הצפנה היא דרך להסתרת המשמעות של מסר קריא באמצעות פונקציה שמקבלת כפרמטר מפתח הצפנה והופכת את המסר לרצף של סימנים המכונה צופן ואינו מובן לאיש.  
שחזור הצופן למצבו הקריא באמצעות פונקציה הופכית מתאימה עם מפתח הפענוח, קרוי פענוח.  
שיטות הסתרת מידע שאינן עושות שימוש במפתח הצפנה קרויות סטגנוגרפיה.  
המונח צופן מתייחס לאלגוריתם הצפנה, כאשר קלט האלגוריתם נקרא טקסט קריא או גלוי, ואילו פלט האלגוריתם נקרא טקסט מוצפן או כתב סתר, בשפה העברית משמשת המילה צופן גם כשם עצם לכתב סתר או קוד.

הצפנות מודרניות מטפלות בשלושה נושאים עיקריים כיום:

**סודיות –**

סודיות כיום מושגת על ידי הצפנה שנעשית על ידי השולח באמצעות מפתח הצפנה סודי ובמסגרתה המסר הגלוי מועבר למצב מוצפן ופענוח שנעשה על ידי היעד חוזר להיות גלוי.  
לעיתים קרובות המפתח הצפנה זהה למפתח הפענוח, אך לעיתים שונה.  
בשני השלבים שנאמרו לעיל ( להלן הצפנה ופיענוח ), משתמשים השולח והמקבל באלגוריתמים קריפטוגרפיים ידועים למען הסודיות, אך מפתח ההצפנה סודי ולא גלוי.

**אימות -**במערכת קריפטוגרפית שלמה סודיות אינה מספיקה, יש צורך באימות זהות נוסף שנועד למנוע התחזות ולספק את הצופן אך ורק ליעד האמיתי ולספק דרך לדעת מיהו המקור של המידע שהתקבל, הדבר דומה לאדם הממלא חתימה על גבי מחאה.

**הבטחת שלמות –**

תפקיד ההצפנה להבטיח שהמידע אותנטי, כלומר לא נעשה בו שינוי זדוני כלשהוא על ידי צד שלישי, האפקט הרצוי נוצר על פי כך שכל שינוי (אפילו שינוי אות אחת), יתגלה מיד על ידי המשתתפים בשיחה, מה שיגרום למערכת לזהות את המסתנן, ולהתריע למשתמשים לגבי הפריצה ולגבי ההודעה הפגומה.

## מהי הצפנה סימטרית ?

הצפנה סימטרית היא סכמת הצפנה שבה משתמשים במפתח הצפנה סודי יחיד גם להצפנה וגם לפיענוח.

ניתן להמחיש צופן סימטרי באופן הבא:  
האלפבית העברי כולל 22 אותיות ( לא כולל סופיות ): אבגדהוזחטיכלמנסעפצקרשת.

e=34125אם נבחר מפתח שהוא פרמוטציה באורך 5 אותיות מעל האלפבית, ההצפנה תתבצע על ידי חלוקת המסר לקבוצות של חמש אותיות והפעלת התמורה על כל קבוצה באופן מחזורי, למשל:  
נגיד והמפתח שלנו הוא , דהיינו האות הראשונה בכל חמישייה תוחלף באות השלישית הבאה אחריה בסדר האלפביתי, האות השניה מוחלפת באות הרביעית, האות השלישית מוחלפת באות הראשונה הבאה אחריה, וכן הלאה.  
אפשר להציג את המפתח כטבלת תמורה עם חמישה היסטים שונים, בשורה הראשונה, האלפבית העברי ובשורות הבאות ההיסטים של האלפבית במרחק שנקבע לפי המפתח, להלן:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| מפתח | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח | ז | ו | ה | ד | ג | ב | א |
| 3 (ג) | ג | ב | א | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח | ז | ו | ה | ד |
| 4 (ד) | ד | ג | ב | א | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח | ז | ו | ה |
| 1 (א) | א | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח | ז | ו | ה | ד | ג | ב |
| 2 (ב) | ב | א | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח | ז | ו | ה | ד | ג |
| 5 (ה) | ה | ד | ג | ב | א | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח | ז | ו |

כמובן שצופן כזה אינו ראוי לשימוש כיום, מכיוון שמספר המפתחות האיפשריים מאד מוגבל ומלבד זאת בצופן כזה ניתן לפענח באמצעות ניתוח תדירויות, הצופן אשר הוצג הוא צופן עתיק יומין בשם צופן ויז'נר, צופן זה מדגים בצורה מעולה את סימטריות הצופן, ניתן לראות כי תהליך הפענוח קל בידיעת מפתח ההצפנה בלבד.

סטנדרנט הצפנת המידע – די.אי.אסדי.אי.אס הוא תקן הצפנת נתונים שפותח בשנת 1975 על ידי אי.בי.אמ בשיתוף פעולה עם הסוכנות לביטחון לאומי ( אנ.אס.אי ).  
האלגוריתם התקבל בשנת 1976 כחלק מדרישת תקן עבור הממשל האמריקאי להצפנת נתונים בעולם האזרחי והצופן שימש בתפקיד זה עד נובמבר 2001, אז הוחלף בתקן החדש ( איי.אי.אס ), שהוא בטוח יותר ומהיר יותר מהקודם לו.  
למרות זאת, די.אי.אס נמצא עדיין בשמוש נרחב בעיקר בתחום הבנקאות.

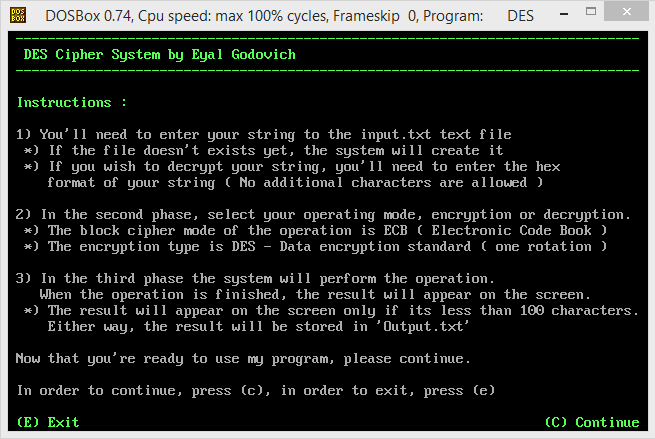
## תיאור הצופן

די.אי.אס הוא צופן בלוקים סימטרי איטרטיבי.  
הפונקצייה הפנימית של האלגוריתם מתבצעת בשישה עשר סבבים על בלוק מידע בגודל 64 סיביות ( 8 בייטים, 8 אותיות ), בעזרת מפתח סודי בגודל 64 סיביות ( שמתוכם רק 56 סיביות בשימוש ) ומפיקה פלט בגודל זהה ( קלט בגודל 64 סיביות יגרום לפלט בגודל 64 סיביות ).  
צופן די.אי.אס מבוסס על רעיון שנקרא צופן מרוכב שהוא שילוב של החלפה ותמורה ליצירת פונקציה חזקה, במבנה הנקרא רשת פייסטל, הרעיון של פייסטל הוא המקור להשראה לאלגוריתם של די.אי.אס.  
רשת פייסטל נועדה לבנות את הצופן באופן כזה שהפונקציה הפנימית תהיה פרמוטציה הפיכה, כך ניתן יהיה להשתמש באותה פונקציית הצפנה גם לפיענוח בהינתן המפתח בסדר הפוך.

## אופן הפעולה

תחילה מחלקים מספר זוגי של סיביות של בלוק טקסט קריא למספר זוגי של בלוק צופן באופן הבא: תחילה מחלקי םכל בלוק לשני חלקים, צד ימין וצד שמאל, בכל סבב מצפינים צד אחד בנפרד ושוזרים, כלומר צד ימין וצד שמאל מחליפים מקומות.  
פונקציית ההצפנה הפנימית מבוצעת בכלל סבב רק על מחצית הבלוק לסירוגין, פלט צד ימין הופך לקלט צד שמאל וחוזר חלילה. החיסכון הוא שפענוח מתבצע באותה פונקציה אך עם פונקציית מפתח הפוכה.

# אופן ההפעלה

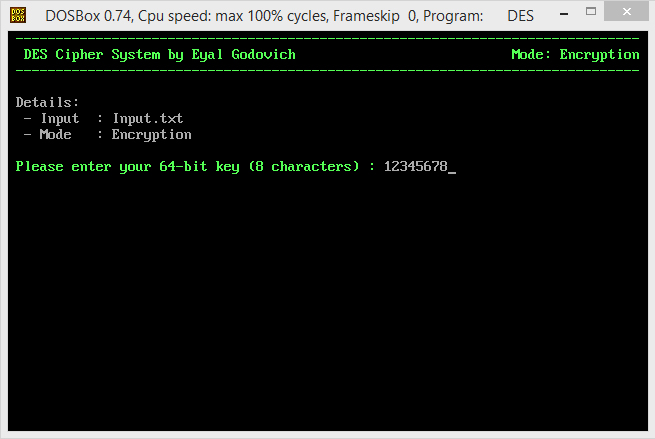


תחילה, כאשר מגיעים אל עמוד הפתיחה ( כפי שניתן לראות בתמונה למעלה ), יש לקרוא את ההוראות, עבור אנשים אשר מתקשים בשפה האנגלית, להלן תרגום:  
1) עלייך להכניס את הטקסט שלך אל הקובץ!  
 \* במידה והקובץ אינו קיים עדיין, המערכת תיצור איתו במהלך הריצה.  
 \* במידה ואתה רוצה לפענח את המחרוזת שלך, אתה תדרש להכניס את הצופן בבסיס 16.  
2) בשלב השני תדרש לבחור את צורת הפעולה, הצפנה או פיענוח.  
 \* צורת ההצפנה היא אי.סי.בי ( אלקטרוניק קוד בוק ).  
 \* סוג ההצפנה הוא די.אי.אס ( סטדנרט הצפנת המידע ).  
3) בשלב השלישי המערכת תבצע את ההצפנה!  
 \* המערכת תשמור את התוצאה המפוענחת\מוצפנת בקובץ הפלט ( אאוטפוט )  
לאחר שההוראות ברורות, יש ללחוץ על הכפתור "סי" במקלדת על מנת להמשיך או על הכפתור "אי" על מנת לצאת מהתוכנית.

## C:\Users\Eyal\Desktop\Untitled-2.jpgאופן **ההפעלה - המשך**

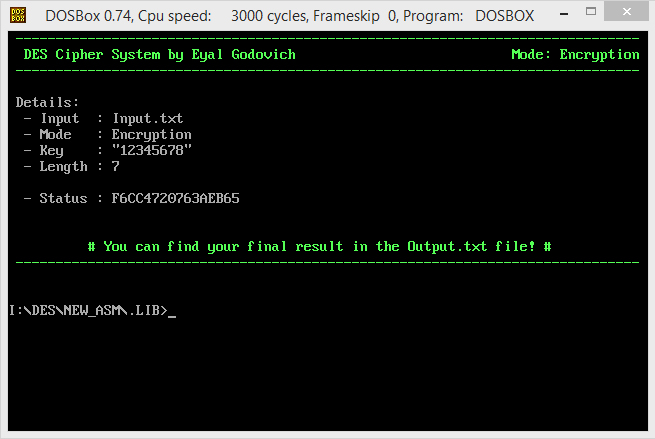
במידה והמשתמש בחר להמשיך ולא לצאת מן התוכנית, יופיע בפניו העמוד הבא ( התמונה מעל ).  
בשלב זה המשתמש יצטרך לבחור באיזו פעולה הוא מעוניין לבצע, הצפנה או פיענוח.  
על מנת לבחור בהצפנה יש ללחוץ בחלק העליון של המקלדת על הכפתור "1", ובמידה והמשתמש רוצה לבחור בפיענוח יש ללחוץ בחלק העליון של המקלדת בכפתור "2".  
  
במידה והמשתמש לא הכניס קלט אל תוך הקובץ, תופיע הודעת שגיאה והמשתמש לא יוכל להמשיך.  
תופיע הודעת שגיאה כמובן גם עבור קלט לא תקין או קלט גדול מדי ( מגבלות הזיכרון של התוכנה ).

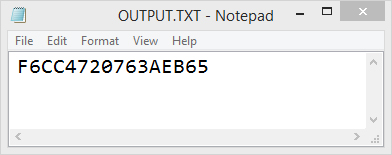
## אופן ההפעלה - המשך



לצורך הדגמה זו, אבחר באפשרות ההצפנה ( "1" במקלדת ).  
לאחר שבחרנו אפשרות, נועבר לדף הבא ( כפי שניתן לראות למעלה ).  
שם נתבקש להכניס את מפתח ההצפנה ו\או הפיענוח שלנו, שהוא מפתח בעל 64 סיביות כפי שנאמר בהסבר, או 8 בייטים, להלן 8 אותיות, לצורך ההדגמה בחרתי ב"12345678".  
  
לאחר שבחרנו את מפתח ההצפנה וכתבנו אותו, יש ללחוץ אנטר להמשך.  
במידה והמפתח הנקלט אינו תקין, תופיע הודעת שגיאה.

## אופן ההפעלה - המשך

****

לאחר שהכנסנו את המפתח הנבחר שלנו ("12345678"), המערכת תמשיך ותצפין את הטקסט אשר התקבל בקובץ, באמצעות מפתח ההצפנה.  
  
לאחר שהתהליך יסתיים ( במהירות, אפילו עבור הקלטים הגדולים ביותר ), תופיע התוצאה על המסך ( או לפחות 62 אותיות מהתוצאה הסופית ), אך במידה ותרצו להעתיק ו\או לראות את התוצאה בשלמותה, תוכלו לפתוח את הקובץ "אאוטפוט" בתיקיה הראשית ולמצוא שם את הפלט של התוכנית.

# גרסאות המערכת

בגרסה העדכנית יש מספר אפשרויות פעולה מוגבל.

בגרסה הנוכחית יש שתי אפשרויות: פיענוח והצפנה של טקסט בהינתן מפתח הצפנה סודי.

בגרסאות הבאות חשבתי לכלול אפשרות לפיצוח צופן נתון ללא מפתח ההצנה הסודי בהינתן חלק מן הטקסט המקורי, זאת אומרת, במידה ואצפין את הטקסט "שמי ואייל ואני בן 16", ואכניס למערכת את הטקסט המוצפן ואת הטקסט "16" ( שתי התווים האחרונים של המחרוזת ), אקבל בחזרה את מפתח ההצפנה בו השתמשתי ( כמובן יכול להיות שהמפתח אינו זהה אך עובד גם כן, מכיוון שזה מבוסס על הביטים המוגדרים ולא על האם זה "1" או "2").

בגרסאות הבאות בנוסף חשבתי לכלול מערכת המאפשרת לבחור גם אפשרות הצפנה אחרת, זאת אומרת לא רק לכלול במערכת את די.אי.אס, אלא גם לנסות ולכתוב באסמבלר יישום של האיי.אי.אס, הממשיך של די.אי.אס בתקן הנוכחי.  
כמובן שזה דבר מאתגר ולא פשוט כלל, בגלל הגבלות השפה והאימולטור, אך עם קצת רצון וקצת יכולת זה אפשרי, ויוסיף המון לתוכנה.  
  
ואם אכן אצליח, אוכל לכתוב גם חלק המנסה לפצח גם צופן המוצפן באיי.אי.אס.  
אך לפני שנקפוץ למים העמוקים וננסה לכתוב הצפנות אחרות, ננסה לפתח את ההצפנה הנוכחית במצבים שונים וחוזקים שונים (טריפל די.אי.אס לדוגמא).

על מנת לחזק את ההצפנה הזו ( די.אי.אס ), ניתן להוסיף מצב הצפנה שונה מהנוכחי ( אי.סי.בי ), ולהשתמש לדוגמא בסי.בי.סי ( כאשר מצפינים כל בלוק מידע בבלוק מידע המוצפן הקודם לו ).

# תיעוד והסבר הפתרון

התוכנית בנויה משמונה קבצים ( נכון לזמן כתיבת תיק הפרוייקט ).  
ישנו הקובץ הראשי (דיאיאס.אסמ), עוד שלושה קבצי תוכנית נלווים, ועוד ספריות עזר שונות.

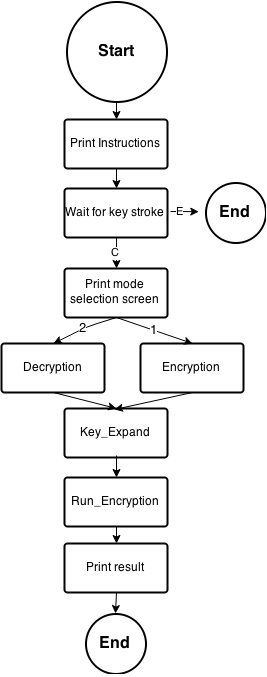
הקובץ הראשי הוא הקובץ שדואג לכל ההתנהלות על המסך והממשק, תחילה מדפיס את ההוראות, מחכה לקלט מהמשתמש ( המשך או יציאה ), לאחר שהמשתמש הכניס את הטקסט שלו לקובץ ואת המפתח הסודי לתוכנה, הקובץ הראשי יקרא למאקרו אשר מבצע את פרוצדורת הרחבת המפתחות.  
לאחר מכן, כאשר פרוצדורת הרחבת המפתחות הסתיימה ויש בידינו את 32 המפתחות, הקובץ הראשי יקרא לקובץ אינקריפט, ויפעיל את המאקרו אשר מבצע את ההצפנה או את הפיענוח.  
לאחר הסיום של הפיענוח או ההצפנה, התוצאה תוצג.

|  |  |  |
| --- | --- | --- |
| הסבר | מטרה | שם |
| מטפלת בדברים הנוגעים לשימוש בסיסי במגוון דברים, כגון המחסנית, טעינת הספריות, ועוד. | דברי בסיס | Base.asm |
| מטפלת בדברים הנוגעים לקונסול, הכוונה להדפסת טקסטים, צבעים וכדומה. | ממשק המשתמש | Console.asm |
| נותנת אפשרות לטיפול קבצים קל ויעיל יותר באמצעות פרוצדורות עזר כגון פתיחת קובץ, כתיבה לקובץ ועוד | טיפול בקבצים | File.asm |
| מספקת אפשרות לדיבוג קל באמצעות הדפסת הערך של רגיסטרים. | דיבאגגינג | Debug.asm |
| פרוצדורות עזר לטיפול במחרוזות | מחרוזות | String.asm |

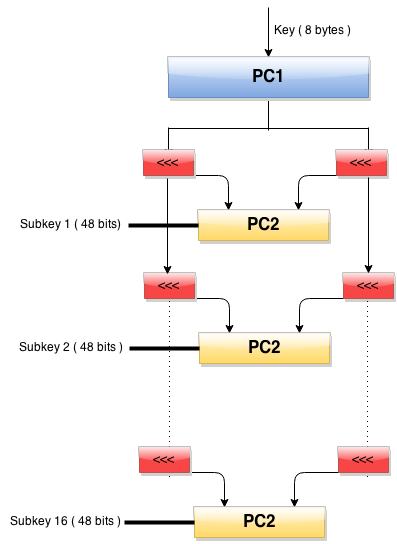
ישנם מספרי קבצי עזר והם:

תרשימי זרימה

## תרשים הזרימה עבור התוכנית הכללית:



## תרשים הזרימה עבור פרצדורת הרחבת המפתח



# רשימת הפעולות

|  |  |  |  |
| --- | --- | --- | --- |
| טענת יציאה | טענת כניסה | מטרת הפעולה | שם הפעולה |
| הפעולה דוחפת את כל האיברים שקיבלה אל תוך המחסנית | מקבלת רשימה של איברים | לדחוף מספר איברים למחסנית בפקודה אחת | Base\_PushRegisters |
| הפעולה תוציא מספר איברים מן המחסנית ותכניס אל האיברים שקיבלה ברשימה | מקבלת רשימה של האיברים אליהם היא תוציא מן המחסנית | להוציא מספר איברים מן המחסנית אל תוך מספר איברים נתונים | Base\_PopRegisters |
| הפעולה תטען את הקבצים באמצעות אינקלוד. | מקבלת רשימה של קבצים לטעינה | לטעון מספר קבצים אל תוך הקובץ הקורא לפעולה | Base\_Load |
| הפעולה מדפיסה את המחרוזת ולאחר מכן יורדת שורה | הפעולה מקבלת מחרוזת להדפסה | מדפיסה אל המסך את המחרוזת ולאחר מכן יורדת שורה | Console\_WriteLine |
| הפעולה מדפיסה את המחרוזת | הפעולה מקבלת מחרוזת להדפסה | מדפיסה את המחרוזת שקיבלה | Console\_Write |
| הפעולה אינה מחזירה דבר | הפעולה לא מקבלת פרמטרים | הפעולה יורדת שורה | Console\_NewLine |
| הפעולה מדפיסה את התו אל המסך | הפעולה מקבלת תו בודד | הפעולה מדפיסה תו בודד אל המסך | Console\_PrintChar |
| הפעולה מדפיסה את המחרוזת ולא מחזירה דבר | מיקום של מחרוזת בזיכרון | הפעולה תדפיס מחרוזת לפי המיקום שלה בזיכרון | Console\_PrintString |
| הפעולה מדפיסה את המספר בבסיס הרצוי על המסך | מקבלת מספר ובסיס | מקבלת מספר ובסיס, ומדפיסה אותו בבסיס הרצוי על המסך | Console\_PrintNumberByBase |
| הפעולה מדפיסה את התוכן של הבייט | מקבלת בייט בודד | מדפיסה ניבל אל המסך | Console\_PrintNibbble |
| לא מחזירה דבר | לא מקבלת דבר | מנקה את המסך | Console\_ClearScreen |
| לא מחזירה דבר | לא מקבלת דבר | מדפיסה את ההדר ( הכותרת העליונה של הממשק ) | Console\_PrintHeader |

## רשימת הפעולות - המשך

|  |  |  |  |
| --- | --- | --- | --- |
| טענת יציאה | טענת כניסה | מטרת הפעולה | שם הפעולה |
| הפעולה מדפיסה את התו בצבע הנתון אל המסך ואינה מחזירה דבר | מקבלת תו בודד ומספר צבע בהקסה | הפעולה מדפיסה תו בודד בצבע | Console\_PrintColoredChar |
| הפעולה מדפיסה את המחרוזת אל המסך בצבע הנתון | הפעולה מקבלת מחרוזת ומספר צבע | הפעולה מדפיסה מחרוזת בצבע | Console\_PrintColoredString |
| הפעולה אינה מחזירה דבר | הפעולה מקבלת פרמטר אחד האומר לה האם לקדם את הסמן או להחזיר באחד אחורה.  Inc / dec | הפעולה מזיזה את הסמן של העכבר בשלב אחד קדימה או שלב אחד אחורה | Console\_CursorBack |
| הפעולה תפתח את הקובץ עם ההרשאות שקיבלה, ותשמור את ה"ידית" אל תוך המשתנה. | הפעולה מקבלת שם של קובץ, את דרגת ההרשאות ואת המשתנה אליו ישמרו הפרטים של הקובץ | הפעולה פותחת קובץ נתון | File\_Open |
| הפעולה סוגרת את הקובץ | הפעולה מקבלת ידית של קובץ פתוח | הפעולה סוגרת קובץ על פי הידית שקיבלה | File\_Close |
| הפעולה יוצרת את הקובץ ומכניסה את הידית של הקובץ אל המשתנה | הפעולה מקבלת שם של קובץ ושם של משתנה | הפעולה יוצרת קובץ | File\_Create |
| הפעולה מזיזה את הסמן במספר המקומות שקיבלה | הפעולה מקבלת ידית של קובץ ובכמה מקומות יש להזיז את הסמן | הפעולה מזיזה את הסמן של הקובץ | File\_SetPointer |
| הפעולה כותבת אל הרגיסטר את הגודל של הקובץ בבתים | הפעולה מקבלת ידית של קובץ ורגיסטר יעד | הפעולה קוראת את הקובץ ומחזירה את הגודל שלו בבתים | File\_Size |

## רשימת הפעולות - המשך

|  |  |  |  |
| --- | --- | --- | --- |
| טענת יציאה | טענת כניסה | מטרת הפעולה | שם הפעולה |
| הפעולה מכניסה את התוכן אל תוך המשתנה | הפרוצדורה מקבלת ידית של קובץ ומשתנה לאחסון | פונקציה זו קוראת את כל התוכן של קובץ אל תוך משתנה | File\_Read\_All |
| הפעולה מכניסה את התוכן אל תוך המשתנה | הפעולה מקבלת ידית של קובץ, מספר הבייטים שצריכה לקרוא, ומשתנה לאחסון | פונקציה זו קוראת מספר בייטים נתון מתוך קובץ | File\_Read |
| במידה והקובץ לא קיים המשתנה יהיה שווה ל255 | מקבלת כתובת של קובץ ומשתנה | הפעולה בודקת האם קובץ קיים | File\_Exists |
| במידה והקובץ קלט קיים, היא תקפוץ אל הלייבל שקיבלה | מקבלת לייבל | בודקת האם קובץ הקלט שלנו קיים ובמידה כן קופצת אל לייבל מסויים | File\_CheckIfInputExists |
| מכניסה את גודל המחרוזת אל תוך הרגיסטר שקיבלה | רגיסטר לשמירת התוצאה ( כל גודל ) | לבדוק את גודל המחרוזת אשר נמצאת בזיכרון התוכנה | String\_GetSize |
| מכניסה את הקלט של המשתמש אל תוך המשתנה | מקבלת משתנה לקבלת המחרוזת ואורך מקסימלי | לקבל קלט מן המשתמש | String\_Scan |
| מחזירה תשובה באמצעות הרגיסטר די-איקס | תו בודד | מקבלת תו ואומרת האם זה בבסיס 16 | String\_IsHex |
| מחזירה את ערך האסקי של התו | מקבלת תו בודד | מקבלת תו ומחזירה את הערך אסקי שלו | String\_CharToASCII |
| מדפיסה את המחרוזת ולא מחזירה דבר | מקבלת מספר של אורך מקסימלי להדפסה | מדפיסה מחרוזת מהזכרון עם מקסימום של אורך נתון | String\_PrintUpTo |
| מוסיפה את התו אסקי כפי שהוא אל המחרוזת הסופית ולא מחזירה דבר | מקבלת תו | מוסיפה תו אל התוצאה הסופית | String\_AddHexToResult |

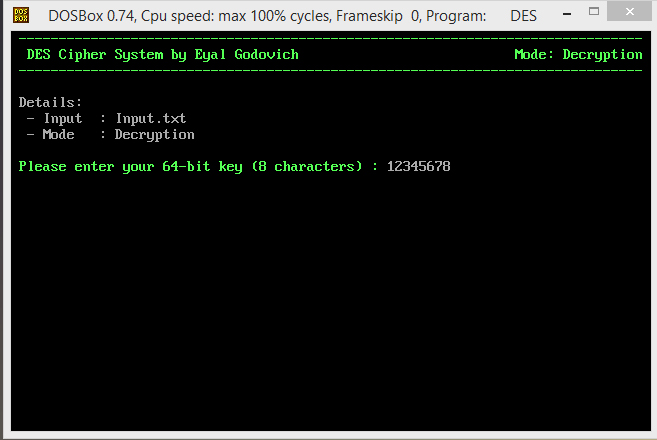
# קוד התוכנית

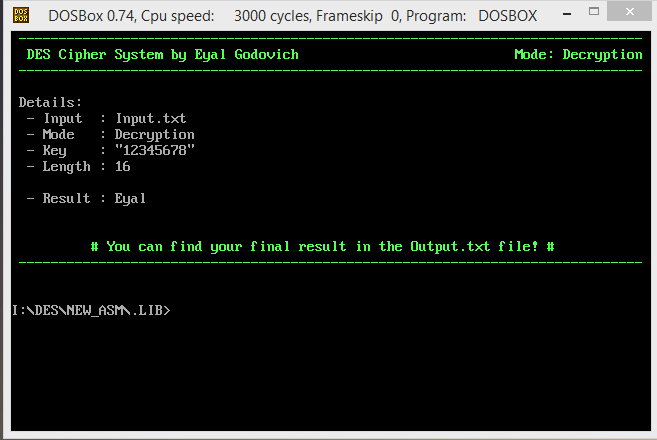
לצורך ההיגיון והנוחות, וכמובן שמירה על הסביבה, הקוד במלואו נמצא בגיטהאב.

[](https://github.com/EyalGodovich/DES)

<https://github.com/EyalGodovich/DES>

# דוגמאות הרצה





# סיכום אישי

אז זהו, לאחר שבועות ארוכים של כתיבת תיק פרוייקט ועוד יומיים של כתיבת הקוד עצמו, לאחר הרבה מאד שעות שהושקעו בפרוייקט הזה, אני גאה לומר שזה נגמר.  
אני מאוד מרוצה מהתוצר הסופי, בחרתי פרוייקט ברמה לא קלה, בתחום שלא התעסקתי בו בעבר ובשפה שלא הייתה לי איתה היכרות לפני הלימודים.

אחד האתגרים היותר גדולים בעבודה הזו, היה למידת השפה מכיוון שאסמבלי 8086 היא שפה מאד ישנה, וניתן להוכיח זאת עם עצם העובדה שאת רוב הלימודים שלי עשיתי ממדריך למשתמש של המוצר המקורי מ1996, 3 שנים לפני שנולדתי.

לאחר שהתגברנו על הקושי עם השפה, נשארנו עם בעיה אחת, כיצד עובדת בכלל ההצפנה הזו? ובכלל איך אפשר לעשות את זה באסמבלי?

השאלה הזו דרשה המון חקר, המון ניסיונות כושלים וחלקם מוצלחים ( אך הפתרון עבד בצורה איטית מדי ), אך לאחר המון זמן הצלחתי להשיג העתק של הקוד המקורי של אחד הפרוייקטים עם ספריות הצפנה היותר מורחבות שקיימות, ושם ראיתי פתרון מדהים לבעיה שהייתה לי, למדתי את הפתרון לעומק ויישמתי אותו בהצלחה באסמבלי.

לאחר שהתגברתי על כל הבעיות, סיימתי את הפרוייקט, ולאחר שיכולתי סוף סוף לנוח, נזכרתי שיש לי עוד תיעוד ותיק פרוייקט להכין, ולצערי זה לקח לי יותר זמן מהפרוייקט עצמו, אני מעדיף להביע את עצמי בקוד ולא בכתב, יותר קל עבורי.

אז לסיכום, ניתן לומר כי לא היה לי פרוייקט בית-ספרי אתגרי כמו שזה היה עבורי מעולם, ואני שמח שעשיתי את הפרוייקט הזה, הוא הרחיב את הידע שלי, זכיתי ללמוד לעומק שפה חדשה ולשפר את "יכולות הגוגל" שלי.