ספר הפרויקט

מגיש: עומר דגרי

מנחה: ניר דוויק

**DES Encryption & Decryption**

**&**

**3DES2 Encryption & Decryption**

Contents

[מדריך למשתמש 3](#_Toc68304355)

[Stage 1 3](#_Toc68304356)

[Stage 2 3](#_Toc68304357)

[תרשים זרימה של הפרויקט 5](#_Toc68304358)

[רשימת הפרוצדורות 6](#_Toc68304359)

[permutation 6](#_Toc68304360)

[printstring 6](#_Toc68304361)

[readstring 6](#_Toc68304362)

[shift\_keys 6](#_Toc68304363)

[shift\_keys\_2 6](#_Toc68304364)

[connect\_arr 6](#_Toc68304365)

[connect\_arr\_run4last 7](#_Toc68304366)

[copy\_arr 7](#_Toc68304367)

[xor\_arr 7](#_Toc68304368)

[S\_Box\_1 S\_Box\_2 S\_Box\_3 S\_Box\_4 S\_Box\_5 S\_Box\_6 S\_Box\_7 S\_Box\_8 7](#_Toc68304369)

[S\_Box1to8 7](#_Toc68304370)

[Final\_Stage 7](#_Toc68304371)

[hex\_to\_ascii 8](#_Toc68304372)

[DES\_Encryption 8](#_Toc68304373)

[ascii\_to\_hex 8](#_Toc68304374)

[reversed\_permutation 8](#_Toc68304375)

[DES\_Decryption 8](#_Toc68304376)

[clean\_data 9](#_Toc68304377)

[DES3\_Encryption 9](#_Toc68304378)

[DES3\_Dcryption 9](#_Toc68304379)

[רשימת מקורות חיצוניים 10](#_Toc68304380)

מדריך למשתמש

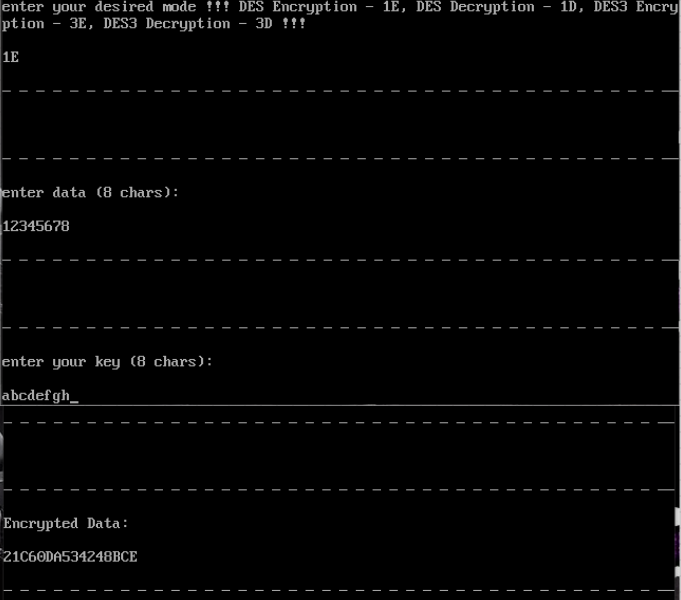
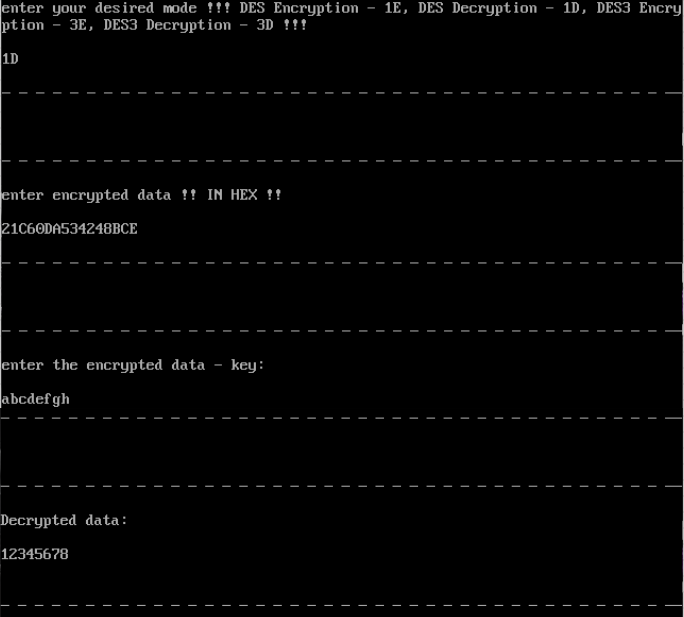
## Stage 1

**לאחר ההרצה המשתמש מתבקש להכניס את הmode שהוא רוצה להיות בו.**

**enter your desired mode !!! DES Encryption - 1E, DES Decryption - 1D, DES3 Encryption - 3E, DES3 Decryption - 3D !!!**

## Stage 2

**לאחר שהמשתמש הכניס את הmode הרצוי הוא יתבקש בהתאם לmode שבחר להכניס את הנתונים שצריך, לאחר שהוא יכניס את הנתונים הוא יקבל את המידע המוצפן או המפוענח תלוי בmode שבחר.**

** **

Mode 1D

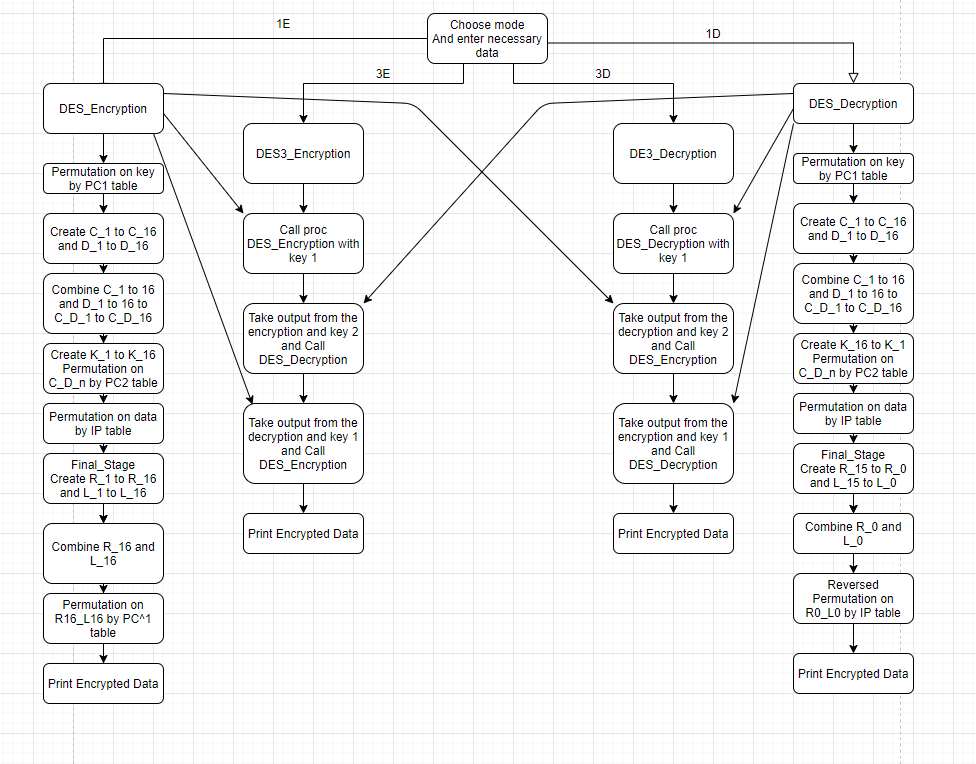
Mode 1E

** **

Mode 3E

Mode 3D

# תרשים זרימה של הפרויקט

****

# רשימת הפרוצדורות

## permutation

offset של טבלה לפרמוטציה וoffset של מה שעושים עליו פרמוטציה וoffset של הפלט ועל כמה ביטים מבצעים את הפרמוטציה.

הפרוצדורה לוקחת את הערך הראשון מהטבלה שהוא מייצג מיקום של ביט מסוים ואז הולכת לביט המסוים בoffset שעליו עושים פרמוטציה ומעתיקה אותו למיקום של הביט הראשון בoffset החדש ואז לוקחת את הערך השני הולכת לביט ומכניסה אותה למיקום של הביט השני וכך הלאה.

## printstring

מקבלת offset של משהו ומדפיסה מהoffset הזה עד שמגיע ל’$’.

## readstring

מקבלת offset של מקום לאחסן קלט ומכניסה את הקלט למקום זה (במערך צריך להיות 2 בתים ריקים בהתחלה, הראשון אומר כמה בתים ניתן לקלוט והשני אומר כמה נקלטו, את הראשון צריך לקבוע מראש).

## shift\_keys

מקבלת offset של 2 דברים, אחד שהיא עושה לו שיפט מעגלי ואחד שהיא תשמור אליו את התוצאה.

## shift\_keys\_2

מקבלת offset של 2 דברים, אחד שהיא עושה לו שני שיפטים מעגליים ואחד שהיא תשמור אליו את התוצאה, פרוצדורה זו קוראת פעמיים ל[shift\_keys](#_shift_keys).

## connect\_arr

מקבלת offset של שני מערכים ואת אורכם וoffset של מערך ריק בגודל פי 2 משני המערכים האחרים ומחברת את שני המערכים לתוך המערך היחיד הגדול פי 2.

## connect\_arr\_run4last

מקבלת offset של שני מערכים ואת אורכם וoffset של מערך ריק בגודל פי 2 משני המערכים האחרים פחות בית (לדוגמה 2 מערכים של 4 אז זה יהיה מערך של 7) ומחברת את שני המערכים לתוך המערך היחיד, אך דורסת בבית האחרון בכל מערך את ה4 ביטים האחרונים מאחר ולא הייתי צריך אותם (ולכן פי 2 פחות בית).

## copy\_arr

מקבלת offset של שני מערכים ואת אורכם ומעתיקה את המערך הראשון לשני.

## xor\_arr

מקבלת offset של שני מערכים ואת אורכם ועושה ביניהם xor.

## S\_Box\_1 S\_Box\_2 S\_Box\_3 S\_Box\_4 S\_Box\_5 S\_Box\_6 S\_Box\_7 S\_Box\_8

כל הפרוצדורות האלו מקבלות offset של שני מערכים וכל אחת לוקחת את ה6 ביטים שהיא צריכה לקחת במערך הראשון ולפי כל s-box הופכות את ה6 ביטים ל4 ביטים ומעתיקות את ה4 ביטים האלו למערך השני.

## S\_Box1to8

מקבלת offset של שני מערכים וקוראת לS\_Box\_1 עד לS\_Box\_8.

## Final\_Stage

מקבלת offset של 9 מערכים ומבצעת את הexpansion ואז את הxor ואז את הs\_boxes ואז permutation ואז עוד xor ובסוף מקבלים את R\_1 עד R\_16 ואת L\_1 עד L\_16.

## hex\_to\_ascii

מקבלת offset של מערך ואורכו ומדפיסה את הערך עצמו שיש בזיכרון ולא את הערך האסקי של הערך שבזכרון, לדומה יש בזכרון 31 היא תדפיס 31 ולא את הספרה 1.

## DES\_Encryption

לאחר שקוראים לפרוצדורה היא תדאג לקבל קלט לבד (אלא אם זה דרך des3, ואז הקלט כבר קיים).

הפרוצדורה מבצעת את כל תהליך ההצפנה של DES בעזרת כל הפרוצדורות שהיו עד עכשיו ומדפיסה את התוצאה.

## ascii\_to\_hex

מקבלת offset של שני מערכים ואת האורך של המערך פלט, לוקחת מהמערך הראשון את הערכים שיש (אמורים להיות באסקי, בשלב של פענוח קולטים את הטקסט שצריך לפענח בהקסהדצימלי ואז זה הופך להיות אסקי בזיכרון אז צריך להמיר את זה להקסהדצימלי בזיכרון) וממירה אותם להקסהדצימלי ושומרת במערך השני.

## reversed\_permutation

מקבלת offset של שני מערכים וoffset של טבלת פרמוצטיה ואת כמות הביטים שיש, והופכת את התהליך שהפרוצדורה [permutation](#_permutation) עושה.

## DES\_Decryption

לאחר שקוראים לפרוצדורה היא תדאג לקבל קלט לבד (אלא אם זה דרך des3, ואז הקלט כבר קיים).

הפרוצדורה מבצעת את כל תהליך הפענוח של DES בעזרת כל הפרוצדורות שהיו עד עכשיו ומדפיסה את התוצאה.

## clean\_data

מנקה את כל המידע שצריך להשתמש בו שוב, רק בmode 3D ו3E, מאחר ורק בהם מצפינים ומפענחים כמה פעמים.

## DES3\_Encryption

לאחר שקוראים לפרוצדורה היא תדאג לקבל קלט לבד.  
הפרוצדורה מבצעת את כל תהליך ההצפנה של 3DES2 בעזרת [DES\_Encryption](#_DES_Encryption) ו- [DES\_Decryption](#_DES_Decryption) ו[clean\_data](#_clean_data).

## DES3\_Dcryption

לאחר שקוראים לפרוצדורה היא תדאג לקבל קלט לבד.  
הפרוצדורה מבצעת את כל תהליך הפענוח של 3DES2 בעזרת [DES\_Encryption](#_DES_Encryption) ו- [DES\_Decryption](#_DES_Decryption) ו[clean\_data](#_clean_data).

# רשימת מקורות חיצוניים

Source 1: <https://he.wikipedia.org/wiki/3DES>  
Source 2: <https://paginas.fe.up.pt/~ei10109/ca/des.html>  
Source 3: http://xor.pw/#  
Source 4: <https://he.wikipedia.org/wiki/DES>  
Source 5: <https://pdfcoffee.com/des-example-encryption-decryption-pdf-free.html>  
Source 6: http://des.online-domain-tools.com/