הצפנת קבצי פרוייקט

יש כאן מספר דוגמאות לקבצי טקסט לא מוצפנים (plaintext) וההצפנות שלהם.

הקבצים המוצפנים הם עם סיומת .e

קבצי הטקסט הם ללא סיומת. ניתן לצפות בהם גם ב- Windows וגם ב- Linux.

הקבצים הוצפנו בעזרת התוכנית שהקוד שלה נמצא בקובץ encode.c שגם הוא מצורף.

כדי לקמפל את התוכנית:

gcc encode.c -o encode

הקבצים המוצפנים נוצרו ע"י ביצוע הפקודות הבאות:

./encode ABCD < gettysburgAddress > gettysburgAddress.e

./encode 12345678 < movie\_quotes > movie\_qoutes.e

./encode A8 < lawyerJoke > lawyerJoke.e

./encode 6F < helloWorld > helloWorld.e

(הקובץ helloWorld הוא הקטן ביותר כאן ולכן הוא אולי הנוח ביותר לביצוע נסיונות).

התוכנית encode קוראת את הקלט שלה מה- standard input, מצפינה אותו בעזרת מפתח הניתן לה

כ- command line argument וכותבת את הטקסט המוצפן ל- standard output.

המפתח (שניתן כ- command line argument) הוא סדרה של ספרות הקסדצימליות (בסיס 16).

אם למשל המפתח הוא ABCD (כמו בדוגמא הראשונה הנ"ל) אז המפתח מורכב משני בתים:

הבית הראשון הוא 0xAB והבית השני הוא 0xCD (0x כאן משמעותו שהמספר כתוב בבסיס 16).

מספר הספרות (ההקסדצימליות) במפתח צריך להיות זוגי כדי שהמפתח יכיל מספר שלם של בתים (bytes).

(כי כל ספרה הקסדצימלית מתארת 4 סיביות וביחד 2 ספרות מתארות byte אחד).

טיפים:

בשיטת ההצפנה שאנו משתמשים בה (עושים xor עם המפתח) ניתן לפענח טקסט מוצפן בעזרת

שימוש באותו מפתח: אם מפעילים את אלגוריתם ההצפנה עם אותו מפתח על הטקסט המוצפן מקבלים

בחזרה את הטקסט הלא מוצפן.

לכן לדוגמא אם נבצע

./encode AB78 < helloWorld | ./encode AB78

אז הפלט יהיה הטקסט שנמצא בקובץ helloWorld. כאן נעשה שימוש ב- pipe: הפלט של פקודת ה- encode

הראשונה משמש כקלט של פקודת ה- encode השניה.

\*\*\*\*\*\*\*\*

ניתן לראות את התוכן של קבצים (גם כאלו שהם בינריים כלומר לא קבצי טקסט) בעזרת הפקודה

od (קיצור של octal dump). את התוכן ניתן לראות בפורמטים שונים ביניהם כמספרים אוקטליים או הקסדצימליים.

למשל כך ניתן לראות את התוכן של הקובץ helloWorld כאשר כל בית מוצג כשתי ספרות הקסדצימליות

ותווים הניתנים להדפסה מוצגים כתווי טקסט

od -cx --endian=big helloWorld

נסו ותראו מה רואים (בלי האופציה --endian=big תווי הטקסט והספרות ההקסדצימליות לא מופיעים באותו סדר -- תנסו ותראו למה הכוונה). כאשר הקובץ מכיל טקסט ניתן להבחין בפלט של od בקוד ה- ascii של התווים.

כדי לראות את טבלת ה- ascii המלאה אפשר לתת פקודה man ascii

נזכיר ש- man היא פקודה מאוד שימושית שמראה את ה- manual. אם תבצעו למשל את הפקודה

man od תקבלו תיאור מלא של הפקודה od שהוזכרה כאן.

\*\*\*\*\*\*\*\*\*

fortune היא פקודה נחמדה של Linux שבכל פעם שמבצעים אותה היא כותבת (ל- standard output)

קטע טקסט שנון. אפשר להשתמש בזה כדי לייצר קטעי טקסט שישמשו כטסטים לתוכנית שלכם.

הקובץ lawyerJoke שמופיע למעלה נוצר ע"י fortune.

הפעלה של fortune עם האופציה -l מייצרת טקסט ארוך יחסית (אם כי לא ממש ארוך).