תרגיל בית מספר 2

|  |  |
| --- | --- |
| **חומר הלימוד לתרגיל:** מחרוזות ומצביעים | |
| **מספר שאלות: 1** | **משקל התרגיל:** 5% |
| **סמסטר:** 2024א | **מועד אחרון להגשה:** |

הצפנה היא טכניקה המשמשת להעברת מידע רגיש בצורה מאובטחת. מפתח הצפנה הוא פיסת נתונים המשמשת להפיכת טקסט רגיל לטקסט מוצפן.

צופן ויז'נר הוא שיטה להצפנת נתונים בעזרת מפתח נתון. צופן זה הוא צופן החלפה, המחליף כל אות במסר באות אחרת על פי אינדקס שונה במפתח. השימוש במפתח נעשה באופן מחזורי. המפתח מתקבל כרצף אותיות אך מתייחסים אליהן כמספרים. האות a מקבילה למספר 0, b ל-1 וכן הלאה.

לדוגמה:

עבור המסר "we love c course" ומפתח ההצפנה "atlm", נבצע לכל אות במסר 0,19,11,12 הזזות באופן מחזורי.

עבור האות הראשונה w נבצע 0 הזזות והיא תישאר w,

עבור האות השניה e נבצע 19 הזזות והיא תהפוך לx,

עבור האות השלישית l נבצע 11 הזזות והיא תהפוך לw,

עבור האות הרביעית o נבצע 12 הזזות והיא תהפוך לa,

עבור האות החמישית v נבצע 0 הזזות והיא תישאר v וכו'

כל תו שאינו אות נותר ללא שינוי.



כתבו קובץ בשם Ex2.c ובתוכו ממשו את הפונקציות הבאות:

void encode(char str[], char key[], char e[], char\* terms[])

הפונקציה תקבל כפרמטרים מחרוזת המכילה טקסט, מחרוזת המייצגת מפתח הצפנה, מחרוזת e ומערך מצביעים.

הפונקציה תצפין את הטקסט ותציב את הטקסט המוצפן במחרוזת e.

בנוסף, הפונקציה תעדכן את מערך המצביעים terms כך שכל תא i במערך יכיל מצביע למילה הi בטקסט המוצפן.

לדוגמה:

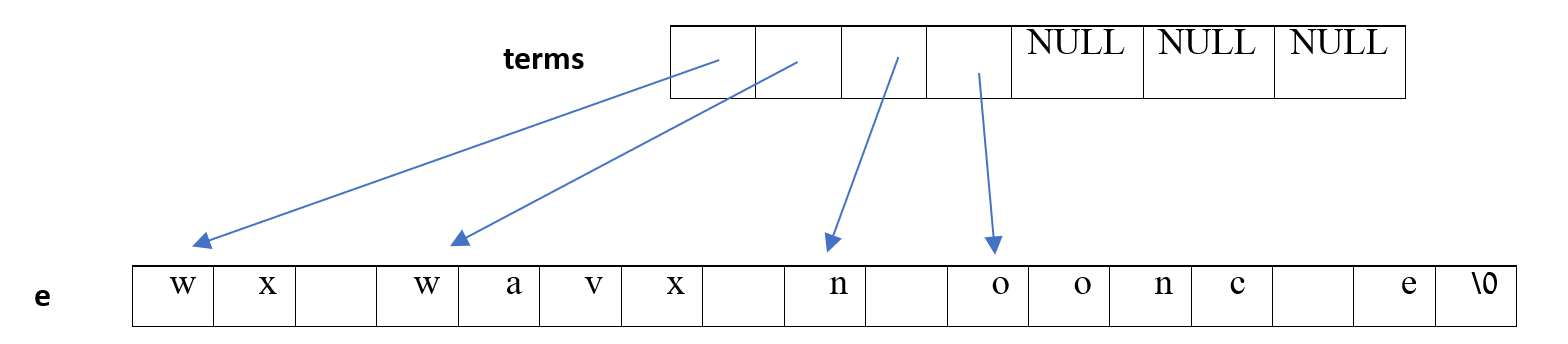
אם הפונקציה קיבלה את הפרמטרים:

str = "we love c course"

key = “atlm”

אז בסיום הפונקציה, המחרוזת e תהיה שווה ל "wx wavx n oonce"

וכך יראו יחד המחרוזת e והמערך terms:



כלומר, תא מספר 0 במערך terms מצביע לתא מספר 0 במחרוזת e

תא מספר 1 במערך terms מצביע לתא מספר 3 במחרוזת e

תא מספר 2 במערך terms מצביע לתא מספר 8 במחרוזת e

תא מספר 3 במערך terms מצביע לתא מספר 10 במחרוזת e

אפשר להניח שבמחרוזת e ובמערך terms יש מספיק מקום.

הפונקציה עשויה לקבל טקסט המכיל אותיות קטנות, גדולות ותווים שונים. לאותיות גדולות נתייחס כאותיות קטנות, לדוגמה: A עם 2 הזזות יהפוך לc. תווים שאינם אותיות יישארו ללא שינוי.

void getIthElement(char e[], char\* terms[], int i, char out[])

הפונקציה תקבל מחרוזת e שמייצגת טקסט, מערך terms של מצביעים לchar ואינדקס i. פונקציה תציב במחרוזת out את המילה הi במחרוזת e.

לדוגמה:

אם " e ="wx wavx n oonce ו-i=1, הפונקציה תציב בout את המחרוזת "wavx". אם i = 2, הפונקציה תציב בout את המחרוזת "n". אם i מכיל אינדקס של מרכיב שלא קיים (למשל i=10 בדוגמה) הפונקציה תציב בתוך out את המחרוזת הריקה "".

הערות והנחיות

1. הגדירו בראש הקובץ שני קבועים

#deine MAX\_TERMS 20

#deine MAX\_STR 200

הקבועים יגדירו את הגדלים המקסימלים של מערך המצביעים והמחרוזות.

קלט המשתמש חייב להתאים לגדלים. התכנית לא נדרשת להתמודד עם מצב של קלט שאינו מתאים לגדלים אלו.

1. מותר להוסיף פונקציות נוספות, בנוסף לפונקציות שמוגדרות בתרגיל.
2. כתבו טסטים שונים לבדיקת נכונות ריצת התכנית.
3. תוכלו להיעזר באתר הבא לבדיקת נכונות הקידוד שלכם: <https://www.cs.du.edu/~snarayan/crypt/vigenere.html>

**הנחיות הגשה**

1. עליכם להגיש תיקיה מכווצת לzip עם הקובץ Ex2.c
2. אין לשנות את חתימות הפונקציות.
3. אין להגיש בזוגות.
4. שימו לב להנחיות הגשת התרגילים שמפורסמות באתר הקורס.
5. הגישו את המטלה במערכת המטלות עד לתאריך   בשעה 23:59.

בהצלחה!