

תרגיל בית 4

1. (50%) בשאלת זאת תමמשו צופן לטקסט הכתוב באותיות לטיניות

א. נגיד רעלת חיבור (שנסמן אותה +) על האותיות 'z','c','b','a' באוף הבא. לכל אות מותאם ערך מסוים: 'a' מקבלת ערך 0 , 'b' מקבלת את הערך 1, וכן הלאה עד 'z' שמקבלת ערך 25. כדי לחבר שתי אותיות מוחברים את הערכיהם המספריים שלhan ואת התוצאה מתרגמים לאות המתאימה. אם התוצאה גדולה מ 25 לוקחים את השארית מ 26. למשל, כדי לחבר 'f' ו 'x' מחשבים $23+5=28$, השארית מ 26 היא 2 וכן התוצאה היא האות 'c'. דוגמאות נוספות: 'e'='g', 'b'='d', 'y'='a', 'b'+'c'='d', 'a'+'a'='a'. כתבו פונקציה add_letters במקבלת שתי מחרוזות. אם שתי המחרוזות באורך 1 ומיצגות אותיות לטיניות הפונקציה תחזיר את הסכום של האותיות לפי הגדרה הנ"ל. אם לא – יוחזר None. התוצאה תמיד תהיה אות לטינית קטנה, גם אם אחד הפרמטרים או שניהם מייצגים אותיות לטיניות גדולות.

דוגמאות:

```
('b','a') add_letters ('b',  
(('F','x') add_letters ('c',  
(('Y','e') add_letters ('G',  
,None add_letters ('a', 'bcd')  
,None add_letters ('%', ''))
```

ב. כתבו פונקציה add_strings שמקבלת שתי מחרוזות המורכבות Maoiotot לטיניות באורךם כלשם ומחזירה מחרוזת שבה כלתו הוא סכום התווים המתאיםים במחרוזות הקלט. אורקל הפליט כאורך המחרוזת הקצרה מבין השתיים.
למשל ('input','output') תחזיר whijc כיוון 'h'='u'+'n', 'w'='o'+'i' וכן הלאה. אם מחרוזות הקלט לא מורכבות אך ורק Maoiotot לטיניות הפונקציה תחזיר None. יש להשתמש בפונקציה add_letters מסעיף א'.

ג. צופן ויג'ניר (Vigenere) הוא צופן עתיק מהמאה ה 16 להצפנת טקסט הכתוב באותיות לטיניות. כדי להצפין טקסט כלשהו s בוחרים מפתח סודי k (בדרכן כל מלה שקל לזכור), בונים מחרוזת t ע"י שכפול של k מספר פעמים עד שהאורך של t הוא לפחות באורך של s ואז מוחברים את s ו t באמצעות הפונקציה add_strings. התוצאה היא הטקסט המוצפן.
למשל, אם אנחנו רוצים להצפין את הטקסט 'attackatsixoclock' בסיס='input' מפתח='k', אז המחרוזת t תהיה 'inputinputinputinput' ותוצאת ההצפנה תהיה 'igiuvsnsimbfbfrfhkx'. יש לכתוב פונקציה vigenere_encrypt שמקבלת מחרוזת s ומפתח k ומחזירה את תוצאת ההצפנה של s באמצעות המפתח k. אם k לא מרכיב Maoiotot לטיניות בלבד, אז יוחזר None. אם s לא מרכיב Maoiotot לטיניות בלבד, אז הפונקציה תתעלם מכל התווים שאינם Maoiotot לטיניות (הפונקציה תתעלם גם מרוחוקים). הפונקציה vigenere_encrypt תשתמש בפונקציה add_strings.

למשל, ('Attack at Six (6) o'clock', 'input') תצפין את המחרוזת 'AttackatSixoclock' ותחזור את המחרוזת 'AttackatSixoclock' (שים לב שהפונקציה add_letters הופכת אותיות גדולות לקטנות)
ד. יש לכתוב פונקציה vigenere_decrypt שמקבלת מחרוזת w ומפתח k ומחזירה את תוצאת הפיענוח של w באמצעות המפתח k. אם k לא מרכיב Maoiotot לטיניות בלבד, אז יוחזר None.

למשל, ('igiuvsnsimbfbfrfhkx', 'input') vigenere_decrypt תחזיר את המחרוזת 'attackatsixoclock' (שים לב שהתוצאה תמיד באותיות קטנות ובלי רווחים).
ה. יש לכתוב תוכנית vigenere.py שעושה את הפעולות הבאות, לאחר שהמשתמש הຕבקש לבחור בין s ל d :

i. אם המשתמש הקיים s (קיצור של encrypt), אז התוכנית תבקש ממנו מפתח הצפנה ושם קובץ. התוכנית תצפין באמצעות הפונקציה vigenere_encrypt את תוכן הקובץ. התוצאה

- תודפס לקובץ בשם דומה לקובץ המקורי, אבל עם הסיומת .vig. למשל, אם שם הקובץ המקורי הוא pooh.txt אז תוצאת הצפנה תישמר לקובץ vig.pooh.txt. התוכנית תצפן רק אותיות אנגליות ותתעלם מכל תווים שאינם אות אנגלית.
- ii. אם המשתמש הקיש d (קיצור של decrypt) אז התוכנית תבקש ממנו מפתח הצפנה ושם קובץ ותפענה את הטקסט שנמצא בתוך הקובץ באמצעות הפונקציה vigenere_decrypt.
- iii. אם המשתמש הקיש כל דבר אחר, אז התוכנית לא תעשה כלום ותפסיק את פעולתה התוכנית תתריע במקרה שקובץ כלשהו שהוא אמור לקרוא ממנו לא נמצא. כדי שהתוכנית לא טיפול במקרה שקובץ לא נמצא יש להשתמש בטיפול בחירגות:

try:

```
f = open(filename,'r')
s = f.read()
f.close()
except IOError:
    print("File not accessible")
```

לצורך בדיקה עצמית מצורפים כמו קבצים מוצפנים. המפתחות לפיענוח הקבצים הם:

מפתח	קובץ
robbers	alibaba.vig
childhood	catcher.vig
tragedy	hamlet.vig
character	poohbear.vig

נסו לפענוח את הקבצים באמצעות התוכנית שאתם כתובים. ודאו שגםם מקבלים טקסט באנגלית (באותיות קטנות ולא רווחים)