תרגיל סיכום python – המרד הגדול!

עם הנסיגה החפוזה של קסטיוס גאלוס מהמצור על ירושלים ואיבוד החיילים שלו במארבים בנסיגה, הבינה המנהיגות בירושלים שהתגובה הרומאית תגיע ועליהם להיערך לכך.

המנהיגות כללה את חנן בן חנן, יהושוע בן גמלא, אלעזר בין חנניה, רבן שמעון בן גמליאל ויוסף בן מתתיהו.

ממשלת המרד ביצעה מיפוי של הארץ. היא חילקה את הארץ למחוזות ומינתה מפקד לכל אזור, כמו יוסף בן שמעון - מפקד יריחו, יוחנן האיסיי – מפקד יפו, לוד, טמאוס ניקופוליס ומחוז תמנה, יוסף בן מתתיהו כמפקד הגליל והגולן ועוד. מייד עלתה שאלת התיאום והעברת ההודעות בין המפקדות השונות.

רבן שמעון בן גמליאל הציע להשתמש ב-[Scytale](https://en.wikipedia.org/wiki/Scytale), אך יוסף בן מתתיהו לגלג עליו "אפילו אתה כבר זקן מידי בשביל להשתמש ב-Scytale. כשהרומאים השתלטו על האימפריה היוונית, הם מצאו את כל הגלילים הקיימים ויהיה לנו מאד קשה למצוא גליל שנצליח להעביר לכל המחוזות ושיאנו נמצא בידי הרומאים"

רבן שמעון בן גמליאל, נפגע והחליט לא לקחת חלק נוסף בדיוני התקשורת והחליט להתרכז בהובלת הסנהדרין שהוא היה נשיאה.

חנן בן חנן הציע להשתמש [בצופן קיסר](https://en.wikipedia.org/wiki/Caesar_cipher), אך הצעתו נפסלה מייד בשל העובדה שהצופן היה בשימוש ע"י הרומאים, הוא הרי אפילו נקרא על שם הקיסר יוליוס אשר השתמש בצופן זה עם מפתח 3.

יוסף בן מתתיהו שהיה לו כושר התבטאות ושכנוע נדיר אמר "אולי נשתמש בצופן שחלוף" ומיד השתררה דממה בחדר וכל העניים היו נשואות אליו.

וכאן נכנס תפקידכם בתור צוות הפיתוח של הנהגת המרד הגדול.

בעולם המחשבים כאשר אנו מעוניינים לנהל דיאלוג ומבלי שאיש יוכל לדעת את תוכנו אנו משתמשים בהצפנה.

עליכם לפתח תוכנה אשר יודעת הן להצפין והן לפענח הודעות:

* לתוכנה יהיו שתי אפשרויות (ע"י העברת פרמטר לתוכנה ב sys.argv).
  + encrypt - הצפנה
    - התוכנה תבקש מהמשתמש להכניס הודעה
    - על התוכנה להצפין את ההודעה ולשמור אותה בקובץ בשם encrypted\_msg.txt בספרייה שממנה התוכנה רצה
  + decrypt - פיענוח
    - התוכנה תפענח את הקובץ המוצפן (encrypted\_msg.txt) ותדפיס את תוכנו למסך.

אם יועבר לתוכנה פרמטר encrypt – עליה לבצע הצפנה של הודעה ולשמור אותה לקובץ.

אם יועבר לתוכנה פרמטר decrypt – עליה לבצע פיענוח של הודעה מהקובץ ולהציגה למשתמש.

**הבהרה:** לשם הפשטות, כדי לא להסתבך בשלב זה עם תווים שהם לא ascii, נשתמש רק באותיות אנגליות.

**הצפנה** – כל תו יוחלף במספר (לפי הטבלה) ובין כל שני תווים יפריד פסיק (הניחו שאין תווים שלא מופיעים בטבלה).

\*ראו בסוף המטלה דוגמאות לבדיקה.

טבלת ההצפנה:

| A | 56 | J | 45 | S | 64 | b | 13 | k | 32 | T | 91 | .(נקודה) | 100 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| B | 57 | K | 46 | T | 65 | c | 14 | l | 33 | U | 92 | ‘(גרש) | 101 |
| C | 58 | L | 47 | U | 66 | d | 15 | m | 34 | V | 93 | ! | 102 |
| D | 59 | M | 48 | V | 67 | e | 16 | n | 35 | W | 94 | - | 103 |
| E | 40 | N | 49 | W | 68 | f | 17 | o | 36 | X | 95 |  |  |
| F | 41 | O | 60 | X | 69 | g | 18 | p | 37 | Y | 96 |  |  |
| G | 42 | P | 61 | Y | 10 | h | 19 | q | 38 | Z | 97 |  |  |
| H | 43 | Q | 62 | Z | 11 | i | 30 | r | 39 | רווח | 98 |  |  |
| I | 44 | R | 63 | a | 12 | j | 31 | s | 90 | ,(פסיק) | 99 |  |  |

על התכנה שלכם לדעת להתמודד עם הודעה ריקה (במקרה זה ההודעה המוצפנת גם תהיה ריקה) – לא None.

מי יודע, אולי, אילו הייתם חיים לפני 1954 שנים, תוצאת המרד הייתה שונה.

בעיית המפתחות המשיכה להיות המכשול הגדול בתקשורת מוצפנת לאורך דורות רבים, וכ-1900 שנים לאחר הכרעת המרד הגיע פרופסור עדי שמיר שיחד עם חבריו למחקר גילה את אלגוריתם ה [RSA](https://en.wikipedia.org/wiki/RSA_(cryptosystem)).

להלן מספר דוגמאות להודעות שיעזרו לכם לבדוק את התוכנה (ההודעה וההודעה המוצפנת), אך עליכם כמובן לבדוק אותה בצורה כללית יותר:

**הודעה ראשונה:**

I did not return the money we took from the convoy to Agripas. I used it to fortify the walls of Tarichaea. 'Yosef Ben Matityahu'

**הצפנה ראשונה:**

44,98,15,30,15,98,35,36,91,98,39,16,91,92,39,35,98,91,19,16,98,34,36,35,16,96,98,94,16,98,91,36,36,32,98,17,39,36,34,98,91,19,16,98,14,36,35,93,36,96,98,91,36,98,56,18,39,30,37,12,90,100,98,44,98,92,90,16,15,98,30,91,98,91,36,98,17,36,39,91,30,17,96,98,91,19,16,98,94,12,33,33,90,98,36,17,98,65,12,39,30,14,19,12,16,12,100,98,101,10,36,90,16,17,98,57,16,35,98,48,12,91,30,91,96,12,19,92,101

**הודעה שניה:**

Vespasian army landed in Caesarea. The Oracle has promised him 'all your wishes, may it be the greatest dream, will come true'.

**הצפנה שניה:**

67,16,90,37,12,90,30,12,35,98,12,39,34,96,98,33,12,35,15,16,15,98,30,35,98,58,12,16,90,12,39,16,12,100,98,65,19,16,98,60,39,12,14,33,16,98,19,12,90,98,37,39,36,34,30,90,16,15,98,19,30,34,98,101,12,33,33,98,96,36,92,39,98,94,30,90,19,16,90,99,98,34,12,96,98,30,91,98,13,16,98,91,19,16,98,18,39,16,12,91,16,90,91,98,15,39,16,12,34,99,98,94,30,33,33,98,14,36,34,16,98,91,39,92,16,101,100

**הודעה שלישית:**

The Galilee has fallen. I am the only survivor. From now on my name shall be Josephus Flavius!

**הצפנה שלישית:**

65,19,16,98,42,12,33,30,33,16,16,98,19,12,90,98,17,12,33,33,16,35,100,98,44,98,12,34,98,91,19,16,98,36,35,33,96,98,90,92,39,93,30,93,36,39,100,98,41,39,36,34,98,35,36,94,98,36,35,98,34,96,98,35,12,34,16,98,90,19,12,33,33,98,13,16,98,45,36,90,16,37,19,92,90,98,41,33,12,93,30,92,90,102

**הודעה רביעית:**

Rabbi Yohanan Ben Zakkai has escaped in a Coffin and re-established the Sanedrin in Yavne.

**הצפנה רביעית:**

63,12,13,13,30,98,10,36,19,12,35,12,35,98,57,16,35,98,11,12,32,32,12,30,98,19,12,90,98,16,90,14,12,37,16,15,98,30,35,98,12,98,58,36,17,17,30,35,98,12,35,15,98,39,16,103,16,90,91,12,13,33,30,90,19,16,15,98,91,19,16,98,64,12,35,16,15,39,30,35,98,30,35,98,10,12,93,35,16,100