**תרגיל סייבר - הצפנה**

הנכם עובדים בארגון מודיעין אשר מטרתו היא לפענם מסרים מוצפנים הנשלחים בין הכוחות השונים של האויב.

אלגוריתם ההצפנה שבו משתמש האויב הוא פונקציה אשר מקבלת שני פרמטרים: הודעה גלויה (message), ומפתח הצפנה (key). הפונקציה מחזירה מסר מוצפן (cipher). על-מנת לפענח את המסר המוצפן, האויב משתמש באלגוריתם פענוח, אשר אינו ידוע לנו.

בשאלה 1 האלגוריתם הוא אלגוריתם הזזה, בשאלה 2, מפתח ההצפנה שבו השתמשו ידוע. בשאלה 3, מפתח ההצפנה אינו ידוע, אולם ידועים רמזים לגביו.

עליכם לפענח את המסרים המוצפנים בכל דרך שתבחרו. מומלץ תחילה לחקור את אלגוריתם ההצפנה, ובעזרתו לכתוב אלגוריתם פענוח.

**שאלה 1:**

כתבו תכנית מחשב שתעזור לכם לפענח את הצופן הבא:

WBQFMDHCUFODVMOQOSGOFQWDVSFOZGCYBCKBOGHVSGVWTHQWDVSFQOSGOFGQCRSCFQOSGOFGVWTHWGCBSCTHVSGWADZSGHOBRACGHKWRSZMYBCKBSBQFMDHWCBHSQVBWEISGWHWGOHMDSCTGIPGHWHIHWCBQWDVSFWBKVWQVSOQVZSHHSFWBHVSDZOWBHSLHWGFSDZOQSRPMOZSHHSFGCASTWLSRBIAPSFCTDCGWHWCBGRCKBHVSOZDVOPSHTCFSLOADZSKWHVOZSTHGVWTHCT3RKCIZRPSFSDZOQSRPMOSKCIZRPSQCASPOBRGCCBHVSASHVCRWGBOASROTHSFXIZWIGQOSGOFKVCIGSRWHWBVWGDFWJOHSQCFFSGDCBRSBQS

ההצפנה בוצעה ע"י צופן ההזזה כאשר הספרה 3 שמופיעה בטקסט לא עברה טרנספורמציה )רק האותיות

עברו(.

ניתן לקרוא את הטקסט המוצפן מהקובץ ciphertext.txt

**שאלה 2:**

מסר מוצפן: **Wkh#dwwdfn#zloo#vwduw#dw#vxqvhw**

מפתח הצפנה: 309

אלגוריתם הצפנה:

def encrypt1(message, key):

return "".join([chr(ord(x) + int(key[0])) for x in message])

**שאלה 3:**

מסר מוצפן:

c0xCVlFTFl5BGFVbXUtTF19ZXVISS0NFVxhCWBJaUxdAXVdTSw==

מפתח הצפנה: המפתח עצמו לא ידוע, אולם ידוע שהאויב משתמש במחרוזת באורך 4 תווים המכילה ספרות בלבד

אלגוריתם הצפנה:

import base64

def encrypt2(message,key):

return base64.encodestring("".join([chr(ord(message[i]) ^ ord(key[i % len(key)])) for i in xrange(len(message))]))