משחקי ריגול

רקע

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, מפתח ההצפנה שבו השתמשו ידוע. בשאלות 2 ו-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.

חלק ראשון

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])
```

<u>חלק שני</u>

מסר מוצפן:

YVxcGVRATVhWXxlOXFhVGUZAWEtBFFZXFWBMXEZQWEAVWVZLW11XXg==

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))]))
```

<u>חלק שלישי</u>

מסר מוצפן:

euTtSa:0 kty1h a0 nlradstara atlot 5wtic

מפתח הצפנה:

המפתח עצמו לא ידוע, **אולם ידוע שהאויב משתמש במחרוזת באורך 3 תווים המכילה אותיות אנגליות (גדולות/קטנות)***

כמו-כן, ידוע שהמסר הגלוי **מתחיל באותה מילה** כמו המסר הגלוי בחלק ב'.

אלגוריתם הצפנה:

```
import random
def encrypt3(message, key):
    random.seed(key)
    l = range(len(message))
    random.shuffle(l)
    return "".join([message[x] for x in l])
```

* היעזרו בפונקציה itertools.permutations

קרדיט: ליאור גרנשטיין

עריכה: ברק גונן