צופן טרנספוזיציה (transposition)

צופן טרנספוזיציה הינו צופן בו בזמן ההצפנה אנו משנים את מיקומן של האותיות. הצופן הוא וותיק מאד ודוגמה שלו הינה הצפנת skytale.

אחד המימושים הנפוצים בהצפנה זו הינו בעזרת מטריצה. מפתח ההצפנה הינו מספר העמודות במטריצה, כאשר מספר השורות נקבע בהתאם לאורך הטקסט המוצפן. ההודעה תכתב החל מהשורה הראשונה, כאשר בכל תא תיכתב אות אחת. הצופן ייכתב על פי העמודות, כאשר מתחילים מהעמודה הראשונה.

לדוגמה אם נרצה להצפין את הטקסט הבא בעזרת מפתח 8:

I WAS DISCOVERED SAVE YOURSELF

נכתוב אותו במטריצה בעלת 8 עמודות:

| I |  | W | A | S |  | D | I |
| --- | --- | --- | --- | --- | --- | --- | --- |
| S | C | O | V | E | R | E | D |
|  | S | A | V | E |  | Y | O |
| U | R | S | E | L | F |  |  |

נקבל את הצופן:

IS U CSRWOASAVVESEEL R FDEY IDO

שימו לב שיש לנו בעיה בסיום הטקסט, כאשר אורך הטקסט אינו מתחלק במפתח ללא שארית. נסמן את התווים הללו ברווח, כאשר ניתן לוותר על התו האחרון.

* נקודה למחשבה – חישבו כיצד בעיית התווים בסוף ההודעה יכולה לשרת את התוקף אשר מעוניין לפרוץ את ההודעה. ואכן כדי להתגבר על כך, הצפנות רבות כלל לא מכניסות את התווים הריקים לצופן.

במקרים רבים נהוג לסמן את סוף הטקסט בסימן '|' (pipe).

כעת ננסה לפענח. כאמור מפתח ההצפנה הוא 8 והוא ידוע לשני הצדדים. נחלק את אורך הטקסט (31) במפתח ונעגל כלפי מעלה.

31 / 8 = 3.875 🡪 4

נבנה מטריצה עם 4 עמודות ונכתוב לתוכה את הצופן:

| I | S |  | U |
| --- | --- | --- | --- |
|  | C | S | R |
| W | O | A | S |
| A | V | V | E |
| S | E | E | L |
|  | R |  | F |
| D | E | Y |  |
| I | D | O |  |

נפענח את הצופן לפי העמודות:

I WAS DISCOVERED SAVE YOURSELF

ועכשיו למשימה שלכם.

1. נסו להצפין את ההודעה שבדוגמה עם מפתח 25.
   1. האם לדעתכם הצופן קל או קשה לפיצוח?
   2. בד"כ נהוג לא להשתמש במפתח הגדול ממחצית אורך הטקסט.
2. כתבו קוד ב-python אשר מקבל מהמשתמש את ההודעה להצפנה ואת המפתח (על המפתח להיות בגודל מתאים – על פי מה שלמדנו בסעיף הקודם). על התוכנית להדפיס את ההודעה המוצפנת.
3. כתבו קוד ב-python אשר מקבל מהמשתמש את ההודעה המוצפנת ואת המפתח. על התוכנית להדפיס את ההודעה המפוענחת.
4. מזגו את שתי התוכניות לתוכנית אחת המקבלת ב-sys.argv את מוד הריצה:
   1. Encrypt – להצפנה.
   2. Decrypt לפיענוח.
5. פענחו את ההודעה הבאה בעזרת מפתח 10:
   1. מקודד ללא רווחים במקום תווים בסוף ההודעה

'hccnShx5ehtsoteG9Cdat.m/AQvpirpg/dXqAdtisod/7tov?n:oo1oUUuug/gcCEoPTs/lu6EAyBpdemQZMK0=o.e26WY/s'

* 1. מקודד עם רווחים במקום תווים בסוף ההודעה

'hccnShx5ehtsoteG9Cdat.m/AQvpirpg/dXqAdtisod/7tov?n:oo1oUUuug/gcCEoPTs /lu6EAyBp demQZMK0= o.e26WY/s '