**עקרונות אלגוריתם ההצפנה :**

**בוצע שימוש באלגוריתם הצפנה מסוג =**

# Rail Fence Cipher

**Encryption**

בצופן טרנספוזיציה, סדר האלפבית מסודר מחדש לקבלת טקסט הצופן.

בצופן גדר המעקה, הטקסט הפשוט נכתב כלפי מטה ובאלכסון על מסילות רצופות של גדר דמיונית.

כאשר אנו מגיעים למעקה התחתון, אנו חוצים כלפי מעלה ונעים באלכסון, לאחר שהגענו למעקה העליון, הכיוון משתנה שוב. כך נכתבים האלפבית של ההודעה באופן זיג-זג.

לאחר כתיבת כל האלפבית, השורות הבודדות משולבות לקבלת טקסט הצופן.

לדוגמה, אם ההודעה היא "GeeksforGeeks" ומספר המסילות = 3 אז הצופן מוכן

**Decryption**

**כפי שראינו קודם לכן, מספר העמודות בצופן גדרות הרכבת נשאר שווה לאורך הודעת הטקסט הפשוט. והמפתח מתאים למספר המסילות.**

**מכאן שניתן לבנות מטריצת מסילה בהתאם. לאחר שקיבלנו את המטריצה ​​נוכל להבין את הנקודות שבהן יש למקם טקסטים (באמצעות אותה דרך לנוע באלכסון למעלה ולמטה לחלופין).**

**לאחר מכן, אנו ממלאים את השורה של טקסט הצופן בצורה חכמה. לאחר מילויו אנו חוצים את המטריצה ​​באופן זיג-זג כדי להשיג את הטקסט המקורי.**

**יישום:**

**תן לצופן-טקסט = "GsGsekfrek eoe", ומפתח = 3**

**מספר עמודות במטריצה ​​= len (צופן טקסט) = 12**

**מספר שורות = מפתח = 3**

## **Brute force** **-** Caesar Cipher

<https://inventwithpython.com/hacking/chapter7.html>

נסיתי לעשות לבד את הקוד אך לא הצלחתי לכן השתמשתי בקוד הזה.

**אופן הפעלת התוכנה:**

**בתוכנה קיימים שתי אופציות לבחירה:**

1. **קריאה מהקובץ** = בחירה מה נרצה לעשות קבלת טקסט ומפתח או שרק טקסט ללא מפתח מקובץ לפי הסוג שנדרש , אחרי זה תהיה הודעה איפה להציג בקובץ או במסך את התוצאה.

2. **קליטה טקסט וקליטה מפתח או שרק טקסט ללא מפתח** = רושמים את הנתונים הנדרשים ו

**יש אופציה של :**

**list box**

**לוחצים ומופיע הפעולה הבא :**

**Button radio**

אשר יהיו אופציות להצפנה ועוד.....

לכל פעולה תידרש או טקסט ומפתח או שפשוט רק טקסט ללא מפתח תופיע חלונית של בחירה של כן ו לא , איפה להציג.

בוחרים באופציה הצגה במסך או הצגה בקובץ(שמירה תוצאה פלוס מפתח עבור הפעולות הבאות שנעשה).

תוצאה תוצג במסך האפור שקיים למטה.

כל פעם שנבחר באופציה נוכל לצאת או לעשות ריענון כדאי שיהיה מקום במסך עצמו.

בוצע טיפול בשגיאות של קלט!