מבוא להצפנה: לתרגיל מס' 1.

1. שתי ההודעות הבאות הן הצפנה של אותו טקסט מקור, אחת על ידי צופן הזזה, השנייה על ידי צופן אפיני (לא בהכרח בסדר הזה). הסבירו את השלבים של הפתרון שלכם, ז"א את כל הבדיקות שעשיתם ולמה עשיתם אותן).

M1= hnermzkarmfhkrwfpvuzvneorxerr

M2= molyfsnbyfumnyrugizsiolxyalyy

   a. מצאו איזו הודעה הוצפנה על ידי צופן הזזה ומצאו את טקסט המקור (העזרו בתדירות האותיות).

   b. מצאו את המפתח ההצפנה ומפתח הפענוח של הצופן האפיני.

2. כמה צפנים אפיניים לא טריוויאליים ניתן להגדיר מעל $\mathbb{Z}_{32}$, $\mathbb{Z}_{48}$, $\mathbb{Z}_{103}$, $\mathbb{Z}_{144}$?

3. יהיו $N>1, \alpha \in \mathbb{Z}_N^*, \beta \in \mathbb{Z}_N$ המגדירים צופן אפיני $e(x)=\alpha x+\beta \bmod N$.

   a. מצאו תנאי הכרחי ומספיק על α,β כדי שלא ייתקיים x ב- $\mathbb{Z}_N$ שעבורו $e(x)\equiv x \bmod N$?

   b. תנו דוגמא אחד של N,α,β המקיים את התנאים האלה.

   c. תנו דוגמא אחד של N,α,β כך שיש בדיוק 4 איברים ש- $\mathbb{Z}_N$ המקיימים $e(x)\equiv x \bmod N$ . .

4. יהי $K=(\alpha,\beta)$ המפתח של צופן אפיני על N אותיות. אומרים כי המפתח "אינבולוטיבי" אם $e_K=d_K$ (פונקצית ההצפנה היא גם פונקצית הפענוח).

   a. הוכיחו כי K אינבולוטיבי אם ורק אם $a^2\equiv 1 \bmod N$ ו- $b(a+1)\equiv 0 \bmod N$.

   b. מצאו את כל המפתחות האינבולוטיביים עבור $N=26$.

5. אליס ובוב רוצים שהצופן שלהם יהיה יותר טוב והם מחליטים להפעיל שני צפנים אפיניים (על 26 אותיות) שונים אחד אחרי השני. האם הצופן שהם מקבלים יותר טוב מצופן אפיני פשוט? נמקו.

6. המטרה היא לפצח צופן אפיני בו השתמשו באלף בית של 37 אותיות. האלף בית כולל את הספרות 0 עד 9 שהן מיוצגות על ידי הערך שלהן ב- $\mathbb{Z}_{37}$ והאותיות A עד Z מוצגות על ידי המספרים 10 עד 35 והרווח מוצג על ידי 36 . פענחו את ההודעה $OH7F86BB46R3627O266BB9$ כשידוע כי היא מסתיימת בחתימה 007 (שימו לב להבדל בין הספרה 0 והאות O).

בהצלחה!