

עבודת 2:

שאלה 1 (10 נקודות)

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

WWODFS	YASEQM	JZKNIC	FSZWUW	JBPNLY	CFWXVB
DLVQMF	VBRULE	GYACDP	KTESYU	AMJLZV	IRLGNI
PEQITH	XONKHK	UNBJWX	LVIHPT	ZCFRSL	BJXAEZ
NQTV CJ	MHGPOA	TDDMJR	QXC BGN	HPHORD	RUUYKQ
SGMTXO	EIVZBF				

(א) הוכיחו כי התמורות המתאימות של צופן אניגמה הן:

$$\begin{aligned}\Delta_4\Delta_1 &= (\text{JNVU}) (\text{ZRYE}) (\text{GCXKSTMPI}) (\text{ALHOFWDQB}) , \\ \Delta_5\Delta_2 &= (\text{HO}) (\text{XG}) (\text{DJETY}) (\text{MZIBL}) (\text{FVPRNW}) (\text{AQCSUK}) , \\ \Delta_6\Delta_3 &= (\text{MOS}) (\text{CNK}) (\text{BXZW}) (\text{YGAP}) (\text{FLITJV}) (\text{QHDREU}) .\end{aligned}$$

(ב) נניח כי התמורות $\Delta_6\Delta_3, \Delta_5\Delta_2, \Delta_4\Delta_1$ הן בסדר ריבסקי. נתון הטקסט הבא שהוצפן ע"י צופן אניגמה:

MWORVZ

חשבו את הטקסט הגלוי.

תשפ"ו סמסטר א'

קריפטוגרפיה

ירמיהו מילר

פתרונות

שאלה 1