

**עבודת 2:** **שאלה 1 (10 נקודות)**

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

WWODFS	YASEQM	JZKNIC	FSZWUW	JBNPLY	CFWXVB
DLVQMF	VBRULE	GYACDP	KTESYU	AMJLZV	IRLGNI
PEQITH	XONKHK	UNBJWX	LVIHPT	ZCFRSL	BJXAEZ
NQTVCJ	MHGPOA	TDDMJR	QXCBGN	HPHORD	RUUWKQ
SGMTXO	EIVZBF				

**a)** הוכחו כי התמורות המתאימות של צופן אניגמה הן:

$$\Delta_4 \Delta_1 = (\text{JNVU}) (\text{ZRYE}) (\text{GCXKSTMPI}) (\text{ALHOFWDQB}) ,$$

$$\Delta_5 \Delta_2 = (\text{HO}) (\text{XG}) (\text{DJETY}) (\text{MZIBL}) (\text{FVPRNW}) (\text{AQCSUK}) ,$$

$$\Delta_6 \Delta_3 = (\text{MOS}) (\text{CNK}) (\text{BXZW}) (\text{YGAP}) (\text{FLITJV}) (\text{QHDREU}) .$$

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

MWORVZ

חשבו את הטקסט המקורי.

תשפ"ו סמסטר א'

קריפטוגרפיה

ירמייהו מיילר

## **פתרונות**

### **שאלה 1**