



3.4 הצופן שלי II

הצופן של סהר

סהר העתיק מהאינטרנט חידה עבור כיתתו, והתקבלה השורה הבאה:
“ינא המכ תב .”ותוא תוביכרמה תורפסה יתש תלפכממ םיילפכ אוה יליג”
 זו נראתה לו חידה בצופן, אבל הוא פענח אותה מהר.
 מקרה זה נתן לו רעיון להמציא צופן קשה יותר ולהתכתב באמצעותו עם חבריו.
 זה הצופן שהמציא:

שלב א: לכל אות, **סהר** התאים מספר כך:

כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
11	10	9	8	7	6	5	4	3	2	1

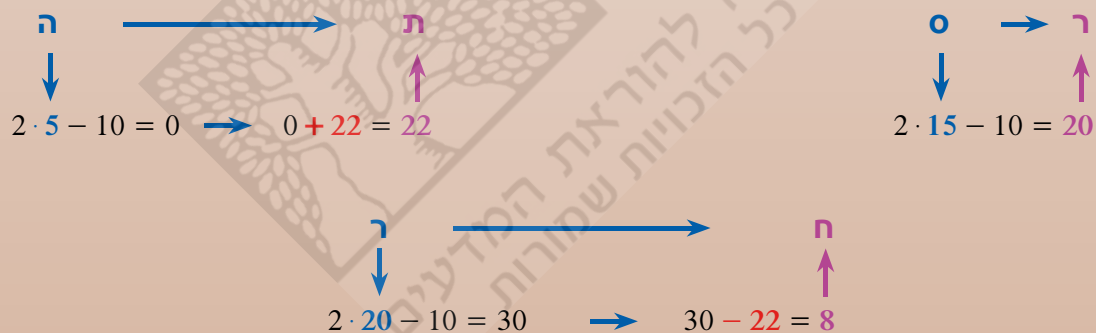
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל
22	21	20	19	18	17	16	15	14	13	12

שלב ב: הוא הציב כל מספר בביטוי $2x - 10$.

שלב ג: **סהר** החליף כל אות באות המתאימה לתוצאת ההצבה.

אם תוצאת ההצבה לא הייתה בטבלה, הוא הוסיף או החסיר 22,
 עד שהתקבלה תוצאה הנמצאת בטבלה.

דוגמה: ההצפנה של השם “**סהר**” היא: “**רתח**”, לפי החישוב הבא:



נצפין ונפענח טקסטים בשיטת ההצפנה של סהר ונחקור את השיטה הזו.

1. ההצפנה של השם “**סהר**” היא: “**רתח**”.
 נסו לפענח באמצעות הביטוי האלגברי את האותיות **רתח**.
 מהן האפשרויות שקיבלתם בנוסף ל**סהר**?
2. א. **הצפינו** שם של תלמיד או תלמידה מן הכיתה בשיטה של **סהר**.
 ב. **פענחנו** את השם שהצפין חברכם.
3. שם אביו של **סהר** הוא שם תנכי. שמו המוצפן הוא: **עית**. **פענחו** את שם האב.

חקירת שיטת ההצפנה של סהר

עבדו עם בן או בת זוג

4. א. האם יש אות שהצפנתה בשיטה זו נותנת אותה בעצמה? מהי?
האם יש אות נוספת כזו? נמקו.
- ב. אילו אותיות נותנות כתוצאת ההצבה מספר שנמצא בטבלה? הסבירו כיצד מצאתם.
- ג. אילו אותיות נותנות כתוצאת ההצבה מספר שיש להוסיף לו 22 כדי שיימצא בטבלה?
- ד. אילו אותיות נותנות כתוצאת ההצבה מספר שיש להפחית ממנו 22 כדי שיימצא בטבלה?
5. האם כל אות יכולה להופיע בהודעה שמוצפנת לפי שיטת ההצפנה של סהר?
אם לא, אילו אותיות לא יופיעו לעולם בהודעה המוצפנת לפי שיטה זו?
6. א. האם ההצפנה של כל אות היא יחידה? אם לא, כמה אותיות בצופן מתאימות לכל אות?
ב. האם הפענוח של כל אות הוא יחיד? אם לא, כמה אותיות מקוריות מתאימות לכל אות מוצפנת?



7. א. הכינו בגיליון אלקטרוני (Excel) טבלת התאמה שתעזור לכם להצפין ולפענח הודעה לפי הצופן של סהר.
השתמשו בנוסחה עבור עמודה C.

	A	B	C	D	E
1	אות מקורית	מספר מתאים לאות מקורית	מספר לאחר הצבה בביטוי $2x - 10$	הוספה או החסרה של 22	אות בצופן
2					
3					
4					

- ב. בדקו את תשובותיכם לשאלות הקודמות.
8. א. **הצפינו** הודעה קצרה (לא יותר מחמש מילים) לפי הצופן של **סהר**.
ב. **פענחו** את ההודעה שהצפין חברכם.



במלחמת העולם השנייה השתמשו הגרמנים והאיטלקים בעלי בריתם במכונות להצפנה ולפענוח של הודעות. משפחת המכונות הזו נקראת **אניגמה**. פירוש המילה ביוונית היא תעלומה או חידה. את ה**אניגמה** המציא מהנדס חשמל גרמני ששמו ארתור שרביוס (Arthur Scherbius) בשנת 1918. האניגמה התבססה על צופן החלפה עבור כל אחת מאותיות המסר שיש להצפין. ההחלפה נעשתה באמצעות דיסקית-צופן שהייתה בשימוש במשך מאות שנים. שרביוס פרץ דרך בכך שיצר גרסה חשמלית לדיסקית, וכך נוצר האמצעי המכני הראשון ששימש להצפנה. יתרון נוסף של שיטתו היה שינוי של צופן ההחלפה לאחר כל אות באמצעות מערכת של דסקיות מסתובבות. האפשרות לשנות את סדר הדסקיות ואת מצבן ההתחלתי הקשתה עוד יותר על מלאכת פיצוח הצופן. בזכות התקשורת המוצפנת באמצעות ה**אניגמה**, הצליח הצי הגרמני, ובמיוחד צי הצוללות, להטיל מצור יעיל על בריטניה – מצור שמנע הובלת מזון ואמצעי לחימה לאי הבריטי. מתמטיקאים רבים הקדישו מאמץ רב לפיצוח ההצפנה. בין היתר הם בנו את המחשב הראשון קולוסוס (Colossus) ובסופו של דבר הם הצליחו בפענוח הצופן. היכולת לפענח את המסרים של האויב נשמרה בסוד, והקנתה לצי הבריטי יתרון משמעותי במלחמה מול חיל הים הגרמני.



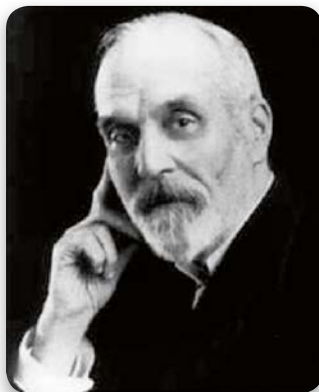
שומרים על כושר

לכל ביטוי, רשמו את כל המספרים השלמים שתוצאת ההצבה שלהם בביטוי היא מספר שלם בין 1 ל-22 (כולל).

- | | | |
|--------------|--------------|------------------------|
| א. $5x + 1$ | ד. $15 - 7x$ | ז. $4x + \frac{1}{4}$ |
| ב. $6x - 6$ | ה. $2 - 5x$ | ח. $2\frac{1}{3}x + 3$ |
| ג. $4x + 10$ | ו. $-x$ | ט. $5\frac{1}{4}x - 3$ |



חידה



אותיות ומספרים היא חידה שבה מוצגת פעולת חשבון, שספרותיה הוחלפו באותיות. על הפותרים לפענח את הצופן – כלומר, לזהות איזו ספרה מיוצגת על-ידי כל אות. חידה נודעת של אותיות ומספרים פורסמה על-ידי הנרי דודני (Henry Dudeney) בשנת 1924.

$$\begin{array}{rcccccc} & & S & E & N & D & \\ + & M & O & R & E & & \\ \hline M & O & N & E & Y & & \end{array}$$



אכזבה בבריטניה



בחודש אוקטובר 2012 מצא תושב בריטי בזמן שניקה את ארובת האח בביתו, יונת דואר שמתה לפני כ- 70 שנה. לעצמותיה היה קשור מכל אדום קטן שהכיל מסר מוצפן, ובו 27 "מילים" של חמש אותיות כל אחת. האיש העביר את המסר למוזאון היונים בבלצ'לי פארק (Bletchley Park), שמסר אותו הלאה ל-GCHQ – הסוכנות המרכזית לאיסוף מודיעין אלקטרוני, בתקווה שאנשיה יוכלו לפצח את הקוד.

אחרי כחודש הודו בסוכנות כי לא הצליחו לעשות זאת וסביר להניח שגם לא יצליחו בלי מידע נוסף. בבריטניה מעריכים כי היונה נשלחה לבריטניה על-ידי יחידות הצבא הבריטי בצרפת סביב יום הפלישה לנורמנדיה ב- 1944. "על אף שמאכזב לגלות שאנחנו לא יכולים לקרוא את המסר שנשאה יונת הדואר האמיצה, זוהי מחמאה לכישוריהם של המקודדים מימי המלחמה שלמרות שעבדו תחת לחץ רב, הצליחו להמציא קוד שאינו ניתן לפיצוח עד היום", נמסר מ-GCHQ. אבל במוזאון היונים בבלצ'לי פארק, שהוקם במקום שבו ישבו מומחי ההצפנה הבריטיים בזמן המלחמה, מסרבים לוותר. האוצר, קולין היל, אמר כי הוא מפקפק במאמצי GCHQ לפענח את הקוד וממשיך לנסות לעלות בעצמו על זהותה של היונה המנוחה – בתקווה שכך יוכל לפתור את התעלומה.

נסמך על מאמר מ-Ynet מתאריך 24.11.2012