הצפנת מידע

קריפטוגרפיה היא ענף במתמטיקה ובמדעי המחשב. ישנם סוגים שונים של הצפנת מידע, ובפרק זה יוצגו בפני התלמידים מספר סוגים קלאסיים של הצפנת מידע: הסתרת מידע, צופני העברה, צופני החלפה, צופן קיסר, פענוח על-ידי טבלת שכיחויות, צפנים ליניאריים וצופן ויז'נר. בכל צופן, בו כל אות מוחלפת על-ידי אות (יחידה) אחרת, ניתן להיעזר בטבלת שכיחויות על מנת לנסות ולפענח את הצופן, לכן לפענוח על-ידי טבלת שכיחויות נשמר מקום ייחודי בין שיטות ההצפנה השונות. הפרק עוסק גם בפענוח מידע וגם בהצפנה לפי השיטות השונות. לסיכום: מה לומדים בפרק זה? שימוש בכלים מתמטיים, פעולות מתמטיות, בדיקת תבניות ומציאת חוקיות ובעיקר - להיות נחושים ולהתאזר בסבלנות.

שיעור ראשון: **סוגים שונים של הצפנה**, עמ' 69 (כשני שיעורים).

<u>מושגים מרכזיים</u>:

סוגים של הצפנה: הסתרת מידע (הוספת סמלים מיותרים למסר), **צופני העברה** (הזזת אותיות במסר) **וצופני החלפה** (החלפת אותיות בסמלים אחרים).

<u>המלצה להוראה</u>:
מומלץ להעביר את החלק הראשון כסדנא של עבודה עצמית (בזוגות או בקבוצות קטנות). במידה ועולה קושי בפענוח של צופן מסוים, ניתן לתת רמזים – להסתכל על כל אות שלישית/רביעית; להסתכל על היפוך אותיות, לסדר אותיות בשורות או בטורים ולנסות לראות אם מתקבלות מילים שניתן לקרוא.
כדאי לבדוק ביחד את הסעיפים 1 ג', 3ב' בהם מופיע סיכום שיטות ההצפנה השונות על מנת לבדוק שהתלמידים אכן הבינו את שיטות ההצפנה. אחרי השיעור הראשון מומלץ לבקש מהתלמידים לכתוב על פתק משפטים קצרים בשיטות ההצפנה השונות שנלמדו בפרק ולהתחלף בדפים עם תלמידים אחרים שינסו לפענח את הצפנים השונים. אם נתקלים במגבלת זמן, אפשר לקחת את הפתקים הביתה ושם לנסות ולפענח את המשפטים.

<u>תשובות והערות לתרגילים</u>:

(1) א) אני אוהב אותך.
ב) המשפט מוצפן בשפת ה-ב'. לאחר כל הברה מוסיפים את האות ב' עם הניקוד או עם אותיות הניקוד המתאימות.
ג) צריך למחוק את אותיות ה-ב', כולל את אותיות הניקוד שלאחר כל הברה.
ד) אחד היתרונות הוא גם חיסרון. קל מאוד להצפין וקל מאוד לפענח.
ה) אפשר להצפין ע"י בחירה של כל אחת מאותיות הא"ב, בדומה לבחירה באות ב' שלעיל.
אפשר גם להוסיף יותר מאות אחת ואפילו מילה שלמה לאחר כל הברה.

(2) א) המשפט המקורי הוא: בוקר טוב. מכל מילה במשפט המוצפן לוקחים את האות הראשונה
ב) משתמשים במילים הנתונות, כאשר צריכים לכתוב אותיות – האות הראשונה של המילה היא האות שתרכיב את המילה.

(3) א) המשפט המקורי: נצפין את הטקסט דרך כתיבה בטורים ונשלח לפי שורות.
ב)

נ	ט	ת	י	פ
צ	ק	י	מ	י
פ	ס	ב	ו	ש
י	ט	ה	נ	ו
נ	ד	ב	ש	ר
א	ר	ט	ל	ו
ת	כ	ו	ח	ת
ה	כ	ר	ל	

יש לכתוב את המילים בשורות ללא רווחים. אורך השורה ניתן לבחירה. השורה האחרונה יכולה להיות יותר קצרה מהאחרות. (בדוגמה שלעיל, אורך כל שורה 8 אותיות). מתקבלים טורים של אותיות. כל טור הוא מילה בטקסט המוצפן. .(בדוגמה שלעיל התקבלו 5 שורות, לכן יש 8 מילים בנות 5 אותיות, במילה האחרונה רק 4 אותיות).

הצפנת מידע

ג) זו אכן שיטה להצפנת מידע.
ד) יש לכתוב כל מילה בטור, מלמעלה למטה. לקריאה יש להסתכל על השורות. סדר הקריאה המתקבל הוא תחילה האות הראשונה מכל מילה, אח"כ האות השנייה, האות השלישית, וכו'. יש לחלק את הטקסט המתקבל למילים ,לפי ההקשר/התוכן.
ז) המשפט המקורי: לכובע שלי שלוש פינות, שלוש פינות לכובע שלי.
ח) המשפט המקורי: לכה דודי לקראת כלה, פני שבת נקבלה (רושמים את המילים בטורים של שלוש אותיות).

(4) א) המשפט: "מורס זה לא קשה". ב) ס . _ . _ ק _ . _ _ ה _ _ _
יש להסב את תשומת לב התלמידים לכך שהמילים כתובות משמאל לימין כמו בלועזית.
ג) זוהי החלפה מסוג העברה - שיטת החלפה.
ד) בזמני מלחמת העולם השנייה השתמשו בקוד מורס. כיום יש שיטות הרבה יותר מתוחכמות.

(5) א) המשפט: "מי שהאמת עתו הוא הרבים, ואפילו הוא לבדו".
שימו לב! נפלה טעות היה צריך להיות כתוב "אתו", כלומר במורס "_.".

שיעור שני: **צופן קיסר** עמ' 73 (שיעור אחד)

מושגים מרכזיים:

צופן קיסר – במשפט המקורי מחליפים את האותיות באותיות שמוזזות לפי סדר הא"ב.

המלצה להוראה:
מומלץ להעביר את הפרק כסדנא בעבודה עצמית (בזוגות או בקבוצות). יש להתייחס בדיון לסעיפים ה', ו', ז' על מנת לוודא שתלמידים הגיעו להכללה הנדרשת והבינו מה המשמעות של מודולו 22 בהקשר הזה. במידה והתעורר קושי בהבנת הקשר של מודולו 22 לשיטת ההצפנה בצופן קיסר, ניתן לעשות הקבלה עם שעון – בכל פעם שמזיזים ב- 24 שעות, השעון מראה אותה השעה. כך גם פה, בכל פעם שמזיזים ב-23 אותיות, חוזרים לאות הראשונה.

תשובות והערות לתרגילים:

(1) א) כל אות מוחלפת באות הנמצאת 3 אותיות אחריה בסדר הא"ב. (הזזה של 3 אותיות).
ב) האות ר' מוחלפת באות א'. הזזה של 3 אותיות מחזירה אותנו לתחילת הא"ב.
ג) את האות ג' במשפט המקורי מחליפה האות ו'. את האות ש' מחליפה האות ב'.
ד) האות ג' במשפט המוצפן היא האות ת' במשפט המקורי. האות ש' היא האות צ'.
ה) מזיזים ב- 3 אותיות. כאשר מגיעים לאות האחרונה, האות ת' שמספרה 22, חוזרים לתחילת הא"ב. אורך המחזור הוא מספר האותיות. במקרה שלנו 22 אותיות.
ו) 22 הזזות. ההזזה ה- 22 משאירה את האות במקומה. ההזזות ה- 23 ומעלה חוזרות על ההזזות 1 - 22.
ז) הזזה ב-22 אותיות משאירה את המשפט המקורי כפי שהיה.
ח) הזזה של 24 אותיות זהה להזזה של 2 אותיות. הזזה של 111 אותיות זהה להזזה של אות אחת קדימה. הזזה של 109 אותיות זהה להזזה של 21 אותיות קדימה, או אות אחת אחורנית.
ט) המשפט המוצפן: בלגך בליגז בסנזך יזאם ילגגת.
במקום להזיז 19 אותיות קדימה אפשר להזיז 3 אותיות אחורנית.
י) הזזה ב- 1,000 אותיות שקולה להזזה ב- 10 אותיות.
המשפט המוצפן: סגעב סגאער סוהרב ארנד אגעעם.
יא) אפשר לנסות לבדוק את כל ההזזות האפשריות – בסה"כ 22 אפשרויות לבדיקה.
הבדיקה מס' 23 תחזור להתחלה.

הצפנת מידע

שיעור שלישי: **פענוח על-ידי טבלת שכיחויות**, עמ' 75 (שיעור אחד)

מושגים מרכזיים:

פענוח על ידי טבלת שכיחויות

המלצה להוראה:

מומלץ להעביר את השיעור כסדנא בעבודה עצמית (בזוגות או בקבוצות קטנות). לפני תחילת העבודה יש להסביר את המשמעות של טבלת השכיחויות המופיעה בטבלה ב'. הטבלה מציגה אחוזים של הופעת האותיות השונות לאחר שנבדקו טקסטים רבים. זוהי שכיחות יחסית של הופעת האותיות השונות ואין להתייחס לערכים כערכים מדויקים. ניתן להתייחס לטבלה על מנת לראות איזו אות באלף–בית שכיחה יותר, ואיזו שכיחה פחות בהתייחס לאותיות האחרות. גם חלוקה זו אינה אבסולוטית מכיוון שכאשר מדובר בערכים מאוד קרובים (כמו האותיות א' ו- ב' בטבלה ב') לא ניתן לקבוע איזו אות שכיחה יותר. במידה ויעלה קושי בהשוואה בין שתי הטבלאות (טבלה א' ו- ב'), ניתן לבקש מהתלמידים לבנות טבלה שבה ידרגו את שכיחות האותיות בשתי הטבלאות.

הצעה לטבלה:

כדאי לבחור טקסטים ממקורות שונים כמו ספר הלימוד, עיתון מדעי, עיתונות יומית ועוד. ככל שהתלמידים יעסקו ביותר מקורות, כך תהיה טבלת השכיחויות של האותיות מהימנה יותר.

מספר האות לפי שכיחות – משכיחות גבוהה לשכיחות נמוכה	אותיות במשפט המוצפן (טבלה א')	אותיות באלף – בית (טבלה ב')
1	מ	י
2	פ	ו
3	צ, י	מ

על מנת להקל על העבודה ולאפשר כתיבה נוחה של האותיות מעל אותיות הצופן, ניתן לצלם על דפים בהגדלה את המשפט שצריך לפענח. לסיכום, ניתן לבקש מתלמידים להצפין משפטים קצרים נוספים באמצעות טבלת השכיחויות (טבלה ב') ולתת לילדים אחרים לפענח את המשפטים המוצפנים.

יש להדגיש את המקום המיוחד של הצפנה באמצעות טבלת שכיחויות יחסית לשאר שיטות ההצפנה. בכל השיטות, שבהן מחליפים אות מקורית באות (יחידה) אחרת ניתן לנחש את האותיות באמצעות טבלת השכיחויות. לדוגמה, אם בטקסט המוצפן האות "ב" חוזרת על עצמה הכי הרבה פעמים, הסתברות גבוהה שאות זו מחליפה את האות "י" שבטקסט המקורי.

תשובות והערות לתרגילים:

(1)

אות	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ/ך
שכיחות	11	3	8	2	3	2	3	3	5	13	8
אות	ל	מ/ם	נ/ן	ס	ע	פ/ף	צ/ץ	ק	ר	ש	ת
שכיחות	4	21	0	4	0	17	13	4	0	6	5

א) האות י' הוצפנה ע"י האות מ'.

ב) האות ו' הוצפנה ע"י פ'. האות מ' ע"י צ' או י'. האות ה' ע"י צ' או י'. האות ב' ע"י ש'.

ג) האות ל' ע"י האות א'. האות ר' ע"י כ' או ג'. האות ת' ע"י כ' או ג'.

הטקסט המוצפן הוא תחילתה של מגילת העצמאות . "בארץ–ישראל קם העם היהודי, בה עוצבה דמותו הרוחנית,הדתית והמדינית, בה חי חיי קוממיות ממלכתית, בה יצר נכסי תרבות לאומיים וכלל-אנושיים והוריש לעולם כולו את ספר הספרים הנצחי".

ד) לא. לפי טבלת השכיחות האות ל' הייתה צריכה להיות מוצפנת ע"י האות א'.

לפי התוכן האות ל' מוצפנת ע"י האות כ' והאות א' מצפינה את האות ת'.

ו) השם לשיטת ההצפנה הוא "פענוח על-ידי טבלת השכיחויות".

הצפנת מידע

שיעור רביעי: **צפנים ליניאריים**, עמ' 77 (כשני שיעורים)

מושגים מרכזיים:

צפנים ליניאריים – הצפנה על-ידי הכפלת המספר הסידורי של אות קבועה והוספת מספר מודולו 22.

המלצה להוראה:
מומלץ להעביר את השיעורים כסדנא בעבודה עצמית (בזוגות או בקבוצות קטנות). בשאלה 1 יש להתייחס לסעיפים ד', ו', ז'. את שאלה 2 כדאי להעלות בדיון כיתתי ולראות שכולם מבינים מדוע נבחר דווקא המספר 3, שהוא המספר ההפוך ל- 15 בכפל מודולו 22. חשוב שהתלמידים יבינו את השימוש בכפל במספר הפוך לפני שהם ניגשים לפתרון של שאלה 3. בשאלה 3 התלמידים מתבקשים גם למצוא את מקדם הכפל וגם למצוא את המספר ההפוך של מקדם הכפל ולהשתמש בו. מומלץ ללוות את הפתרון של התרגיל על-ידי דיון כיתתי או לכל הפחות לבדוק את הפתרון. את הפתרון של תרגיל 4 מומלץ לבדוק במליאה.

תשובות והערות לתרגילים:

(1) א) האות א' הוצפנה ע"י ג'. האות ב' ע"י ו'. האות ה' ע"י ס'. האות ו' ע"י צ. ערכה המספרי של כל אות מוכפל ב-3.
ב) ההצפנה היא כפל ב-3 מודולו 22.
ג) בלידרד ני דתבב בב ילנץ תרדדרחרד.
ד) לא. בשיטה זו יש זוגות של אותיות המוצפנות ע"י אותה אות. לדוגמה: האותיות מ' ו-ב' מוצפנות ע"י ד'. האותיות א' ו-ל' מוצפנות ע"י האות ב'.
ה) כן.לדוגמה: האותיות ל' ו-י' מוצפנות ע"י האות ת'. האותיות פ' ו-מ' מוצפנות ע"י האות כ'.
ו) המספרים 2 ו-11 הם מחלקים של המספר 22.
ז) כל המספרים האי-זוגיים לא כולל 11.

(2) א) הערך 1.
ב) המספר 3 זר למספר 22, מספר האותיות.
המספרים 3 ו- 15 הם מספרים הפוכים בכפל מודולו 22, לכן ניתן לעשות פעולה הפוכה ו"להחזיר" את הערכים המקוריים של האותיות, וכך לפענח את הצופן.
ג) האוצר נגנז תחת הדקל.

(3) א) האות י' הוצפנה ע"י האות ב'. זו האות שלפי טבלת השכיחויות בעמ' 75 היא השכיחה ביותר ושכיחותה במשפט הנתון היא הגדולה ביותר.
ב) המספר יכול להיות 9 או 20. נבחר מס' 9.
ג) נמצא מספר הפוך למספר 9 בכפל מודולו 22.

$9 \cdot 5 = 1 \pmod{22}$. לכן מס' 5 הוא המספר ההפוך של 5 בכפל מודולו 22.

ד) $y=5$.
ה) המשפט המקורי: היום גיליתי שיטת הצפנה חדשנית.

(4) א) המשפט המוצפן: שר דשר ככדומרש.
ב) אפשר לפעול בשלבים: למצוא ערכים של אותיות במשפט המוצפן; להחסיר מערכים הללו 2; את התוצאה לכפול במספר הפוך של 15 במודולו 22 (לפי תרגיל 2 זה מספר 3) וכך להגיע לערך של האות המתאימה באלף – בית.
ג) אפשר לנסות בשלבים: למצוא את האות השכיחה ביותר במשפט המוצפן ולפי טבלת השכיחויות לקבוע שזו "י". לקחת אות אחרת ולנסות לנחש מהי לפי טבלת השכיחויות בעמ' 75 (טבלה ב'); לנסות לנחש לפי שתי אותיות את קבוע ההזזה ואת מקדם הכפל (או לנסות לפתור מערכת משוואות $y=ax+b \pmod{22}$, כאשר y הוא הערך של האות המוצפנת ו- x הוא הערך של האות במשפט המקורי).
אחרי הניחוש, מהערכים של האותיות בצופן להחסיר את קבוע ההזזה ולכפול בהופכי של מקדם הכפל במודולו 22. השיטה מורכבת ויש יותר מידי דברים שצריך לנחש לכן לא קלה לשימוש.
ד) אפשר לראות את שיטת אתב"ש (שיטה המוזכרת ב- עמ' 68) ככפל ב-(-1) והזזה ב-23.

הצפנת מידע

שיעור חמישי: **צופן ויז'נר**, עמ' 80 (שיעור אחד)

מושגים מרכזיים:

צופן ויז'נר – הצפנה על ידי מילת מפתח

המלצה להוראה:

את השיעור האחרון מומלץ להעביר כסדנא בעבודה עצמית (בזוגות או בקבוצות). במהלך העבודה יש לוודא שכולם הבינו את המושג של "חיבור של האותיות בטור" ושהכוונה היא לערכים של האותיות. כדאי לדון גם בשאלה "האם ניתן לפענח את הצופן אם לא יודעים את מילת המפתח". התשובה לשאלה היא מורכבת. אחד הכיוונים האפשריים לדיון – האם ניתן להיעזר בטבלת שכיחויות שבעמ' 75, טבלה ב'. התשובה היא לא כי למשל, האות "י" במשפט המקורי שהיא האות השכיחה ביותר לפי הטבלה יכולה להיות מוצפנת על ידי מספר אותיות (סעיף ד') ולכן לא ניתן להיעזר בטבלת השכיחויות.

תשובות והערות לתרגילים

(1) א) ירון רשם את המילה "אגב" כמה פעמים מתחת לאותיות המשפט המקורי. (אות מתחת אות). אח"כ חיבר כל 2 אותיות בטור.
ב) לא. ההצפנה תלויה באותיות המילה "אגב", איזה אות נמצאת מתחת לכל אות במשפט המקורי. לדוגמה: מתחת האות י' במשפט המקורי נמצאת פעם האות ג' ופעם האות א'. לכן האות י' מוצפנת פעם ע"י מ' ופעם ע"י כ'.
ג) לא. תלוי איזה מאותיות המילה "אגב" הייתה רשומה מעליה. לדוגמה: האות ס' הצפינה פעם את האות נ' ופעם את האות מ'.
ד) טבלת שכיחויות לא תעזור בפענוח לפי שיטה זו. אותיות המילה "אגב" רשומות בכל פעם מתחת לאות אחרת.
ה) אחת האפשרויות לרשום את המילה "אגב" מתחת לאותיות המשפט המוצפן וחסר את הערכים.
ו) המשפט המוצפן: נשקכפלן עפשמס פס-להם סכסב נרבט.
ז) המשפט המקורי: המקום הזה מסוכן.