

יום שיא: דרכון ביומטרי

מתמטיקה



(בהשראת מערך הצפנה של התוכנית לנוער מוכשר למתמטיקה, אוניברסיטת בר אילן)

החומרים המובאים כאן נוצרו במסגרת פרויקט דיאלוגוס – מחקר משותף של אוניברסיטת תל-אביב, הטכניון, האוניברסיטה העברית בירושלים ומכון ויצמן למדע, במימון הקרן הלאומית למדע (מס' 2699/17).

© כל הזכויות שמורות

נושאים מרכזיים במערך:

- היכרות עם מושג ההצפנה
- התנסות בסוגים שונים של הצפנות פשוטות
- תנאי הכרחי בהצפנה
- מה היא הצפנה טובה?
- האתגרים באבטחת מידע באמצעות הצפנה

חלק ראשון - מושגים בסיסיים בהצפנה

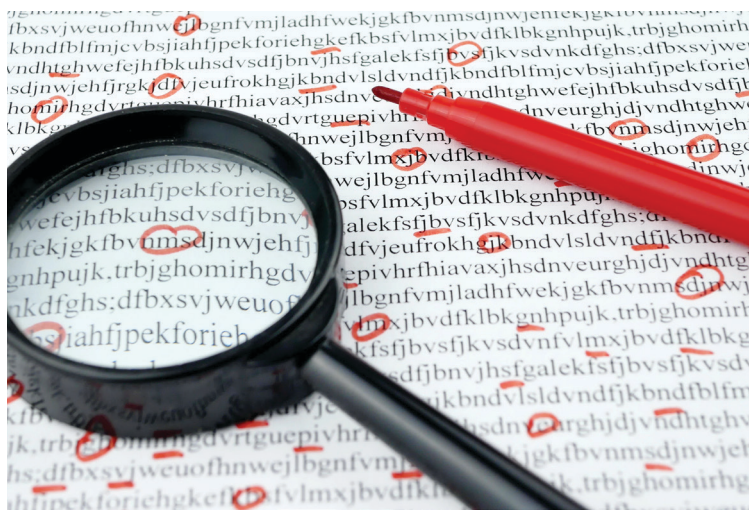
הצפנה - שימוש בקוד או בכתב סתרים לשם העברת ידיעות סודיות (מתוך מילון אבן שושן). כלומר, העברת מידע באופן שיהיה קריא רק לאנשים בעלי הרשאה, ויהיה קשה מאוד לפיענוח על ידי אנשים ללא הרשאה. קריפטוגרפיה היא התורה שעוסקת בעקרונות ובשיטות של הצפנת מידע.

תהליך ההצפנה כולל שני שלבים:

- הצפנה** - נעשה על ידי השולח. בתהליך זה המסר הגלוי מועבר למצב מוצפן.
- פענוח** - נעשה על ידי המקבל. בתהליך זה המסר המוצפן חוזר להיות גלוי.

מושגים בסיסיים נוספים:

- מפתח הצפנה** - השיטה המסוימת שבעזרתה ניתן לפענח את הצופן.
- פיתוח** - התהליך שבו ממציאים את מפתח ההצפנה
- פיצוח** - התהליך שבו מגלים את מפתח ההצפנה או את המסר הסודי המועבר.



שימוש בצפנים ובהצפנות היו לכל אורך ההיסטוריה. הצורך בהצפנה גבר עם התרחבות השימוש בהעברה נרחבת של מידע - בצבא, בפוליטיקה, בעסקים ובמחשבים. לכל אורך ההיסטוריה קיימת מלחמה בין המפתחים למפצחים. מי יגבר על מי. לאור זאת, כל הזמן צריך להמשיך ולפתח צפנים מורכבים יותר שיהיו קשים לפיצוח.

למורה:

החל מחלק זה התלמידים יהיו מחולקים לקבוצות קטנות, וכל המשימות והדיונים יעשו באופן קבוצתי. כל משימה היא תחרות בין הקבוצות. לשיקולכם, אפשר לאסוף נקודות ולהכריז על מנצח בסוף.

1. צופן החלפה (שחלוף): כל אות באלפבית מוחלפת באות אחרת

אחת ההצפנות הפשוטות נעשית על ידי צופן החלפה שבו כל אות מוחלפת באות אחרת. אחת משיטות השחלוף הפשוטות והעתיקות נקראת צופן אתב"ש: כדי להצפין בשיטה זו כותבים את הא"ב בשתי שורות באופן הבא, המהווה את המפתח של הצופן:

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

מפתח ההצפנה מורה לנו באיזו אות להחליף כל אחת מאותיות המסר המקורי כדי להצפינו. השימוש בצופן זה נעשה בתנ"ך שלוש פעמים בספר ירמיהו. למשל, "...ומלך ששך ישתה אחריהם" (ירמיהו כ"ה, כ"ו). מי זה מלך ששך? הכוונה היא למלך בבל בצופן אתב"ש.

משימה 1

הצפינו את המשפט הבא לפי צופן אתב"ש:

"אנחנו לומדים מתמטיקה"

פתרון: תטסטפ כפיקמי ישינמדצ.

משימה 2

פענחו את המשפט הבא לפי צופן אתב"ש:

"שצהוטא ימקז מבטף דגש תגפל פיאבל שמט ציואסמי פשמט ציוהסמי בכ צהוטמי"

פתרון: בהצפנת מידע ישנו קרב ארוך ומתמשך בין המפתחים ובין המפצחים של הצפנים.

דין קצר: מה החיסרון בשיטה הזו?

חסרונה הגדול של שיטת ההצפנה הזו הוא שקל יחסית לפצח אותה. כיוון שכל אות מוחלפת תמיד באותה אות אחרת אפשר לנתח כמות גדולה של הודעות ולמצוא את שכיחות האותיות, וכך להסיק מהן האותיות הנדירות והנפוצות. בצופן אתב"ש, האות הנפוצה ו' למשל מוחלפת ב'פ', השכיחה פחות, ועל כן פ' תופיע יחסית הרבה בטקסט המוצפן. להצפנה זו מפתח הצפנה פשוט ומכיוון שצריך לחשוב על האפשרות שהצופן יגיע לידיים הלא נכונות, צריך להקשות את פיצוח הצופן כמה שיותר.

"קוד הקיסר" (מיוחס ליוליוס קיסר) - צופן הזזה

צפני שחלוף מסוג אחר הם צפני הזזה. בשיטה זו מפתח ההצפנה הוא מספר המתאר את גודל ההזזה, והידוע רק לשולח המסר ולנמען. למשל, אם המפתח הוא המשמעות היא שמזיזים כל אות בא"ב במקום אחד. האות א' תוצפן לב', האות ב' תוצפן לג' וכן הלאה. מפתח ההזזה במקרה זה הוא. לאיזה אות תוצפן אות ת'?

למורה:

כאן נחלק לתלמידים גלגלי אותיות מוכנים שיוכלו לעבוד איתם במשימות הבאות. כל סיבוב של העיגול הקטן ביחס לגדול נותן מפתח הזזה.

הצפינו את המסר: "**המתמטיקה היא האלפבית שבו כתב אלוהים את העולם**".
בצופן הזה במפתח.

פתרון: "חגגעלמתח חמד חדסרהמג בהט נגה דסטחמע דג חקטסע".

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

פענחו את המסר: "**שלולד כדפסחכ כוטחכ ימחדנ**".

כאן התלמידים לא יקבלו את מפתח ההצפנה ויצטרכו לפענח אותו בעצמם.

פתרון: המספר הוצפן בצופן הזה במפתח +20 "אנחנו מוקפים מחכים לסיוע".

למורה:

במשימה זו עשוי להתפתח דיאלוג בין תלמידי הקבוצה בנוגע לאסטרטגיית זיהוי מפתח ההצפנה. למשל, דרך אפשרית היא לנסות להזיז למשל ב-1, ולבדוק אם המילה הראשונה יוצאת הגיונית. אם לא, מנסים הלאה להזיז ב-2 וכן הלאה עד שמוצאים את המפתח הנכון. יתכן שהתלמידים יעשו זאת באופן אינטואיטיבי בלי לתכנן מראש, ואז בשלב הדיון נרצה שיסבירו במילים את האסטרטגיה.

דיון קצר:

1. איך פיצחתם את המסר המוצפן?
2. האם לפי דעתכם שיטת הצפנה זו היא טובה?
3. שיטה זו אמנם קשה יותר לפיענוח משיטת האתב"ש, אבל יש בה מספר סופי של מפתחות הצפנה. בשפה העברית יש 21 מפתחות בלבד משום שיש 22 אותיות ולכן בכל מקרה, בזמן לא ארוך ניתן לגלות את המפתח.

תנאי הכרחי בהצפנה – דיון

מה לא בסדר בצופן הבא?

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

תשובות אפשריות: זה כמו אתב"ש אבל עם טעות, כתבו מ' במקום ט'. יש להדגיש שזו לא מהות הבעיה.

מפתח הצפנה צריך לקיים את התכונה שהוא **חד חד ערכי**, כלומר לכל אות במסר המקורי קיימת אות אחת שמחליפה אותה, ולכל אות במסר המוצפן קיימת אות אחת שמחליפה אותה. ניתן לראות שבמפתח הזה גם האות י' וגם האות נ' מוחלפות באות מ'. לכן כאשר נרצה לפענח את הצופן, אם תופיע בו האות מ לא נדע מאיזה מקור היא הגיעה, י' או נ'.
הצפנה שמבטיחה התאמה חד חד ערכית בין אותיות המסר לאותיות המוצפן משמעותה היא שבעת ההצפנה מוחלפת כל אות במסר על ידי אות אחת ורק אחת במסר המוצפן. כנ"ל בפיענוח. כל אות במסר המוצפן מתפענחת לאות אחת ורק אחת במסר המקורי. לצופן חד חד ערכי מקובל לקרוא **צופן מונו-אלפבתי**.

הצפנה באמצעות מספרים

כדי לסבך מעט את העניינים ולהקשות יותר על פענוח צפנים ניתן להמיר את האותיות במספרים. ההתאמה הבסיסית היא להתאים לכל אות מספר כשאנו שומרים על הסדר של האותיות ועל הסדר של המספרים, כמו בטבלה הבאה:

ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

לאחר שהמרנו כל אות למספר אפשר לבצע הצפנה על המספרים באמצעות נוסחה מתמטית.

דוגמה להצפנת הזזה במפתח +6: הצפנת אות בצופן הזזה במפתח +6 תוסיף 6 לערך המספרי של אותה אות. למשל האות ג' תוצפן למספר 9 (3+6). האות ש' תוצפן למספר 27=21+6.

דוגמא להצפנה על ידי כפל במספר קבוע, למשל 6: הצפנת אות על ידי הכפלה של הערך המספרי של אותה אות במספר קבוע. האות א' תוצפן למספר 6 (6=6·1), האות ח' תוצפן למספר 48. ניתן להראות את שתי הדוגמאות האלו על ידי הוספת שורות לטבלה הבסיסית על הלוח.

ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
														14					9		7
														48					18		6

למורה: טבלה כזו עם שורות נוספות ריקות תחולק לתלמידים לצורך המשימות הבאות.

משימה 5 – התנסות
 כל תלמיד יכתוב את שמו בצופן עם מפתח "כפול 2 פלוס 1".
 למשל: רעות = 41, 33, 13, 45
 תמי = 27, 45

משימה 6 – פענוח צופן

למורה:

משימה זו אינה פשוטה. היא כוללת שני שלבים:

1. פיצוח מפתח ההצפנה בעזרת המילה הראשונה.
2. ביצוע הפעולה ההפוכה על מנת להגיע מהמספרים הנתונים אל האות המוצפנת. למשל, אם מפתח ההצפנה הוא, על מנת לפענח אותו צריך להוסיף 1 ולחלק ב-3. יתכן שחלק מהתלמידים יתקשו בכך, ויהיה צורך לפתוח את העניין לדיון. התנסות נוספת מסוג זה תהיה במשימה הבאה.

נסו לפענח את הצופן הבא אם ידוע כי המילה הראשונה בצופן היא "אני"

65 26 29 62 11 38 17 35 29 41 2

14 62 11 23 14 41 50 53 14

14 56 29 26 38 65 38 59 17 47 29 62 5

פתרון: אני לומד שיטת הצפנה חדשה בשיעור מתמטיקה

מפתח ההצפנה הוא $3x-1$. על מנת לפענח אותו צריך להוסיף 1 ולחלק ב-3. מתקבלת הטבלה:

ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
65	62	59	56	53	50	47	44	41	38	35	32	29	26	23	20	17	14	11	8	5	2

משימה 7 – המצאת מפתח הצפנה

כל קבוצה תחשוב על מפתח הצפנה קשה ככל שתוכל, ותצפין מסר בן 5 מילים.

לאחר שכל קבוצה תצפין את המסר שלה הקבוצות יחליפו את המסרים המוצפנים, וכל קבוצה תנסה לפענח את הצופן שקיבלה. (המילה הראשונה תהיה נתונה כמו בדוגמה הקודמת).

למורה:

משימה זו היא בעלת פוטנציאל לעורר דיאלוג בין תלמידי הקבוצה בשני עניינים:

האחד – איזה מפתח הצפנה כדאי להמציא על מנת שלקבוצה המתחרה יהיה קשה?

השני – איך לפצח את הצופן של הקבוצה היריבה בצורה היעילה ביותר?

חלק שלישי – דיון מסכם

המטרה היא שהתלמידים יחשפו לעמדות שונות בנוגע לשאלה: עד כמה מידע רגיש שהוצפן הוא אכן מאובטח מול גורמים פורצים?

שאלות לדיון:

1. מהי, לדעתכם, הצפנה טובה?
 2. מתי הצפנה היא טובה? האם הצפנה באמצעות הזזה היא טובה לדעתכם? מדוע?
- כמה זמן לקח לכם לפענח את הצופן במשימה 6 למרות שלא ידעתם את המפתח? האם הצופן הזה הוא טוב לדעתכם?
 - מספר מפתחות ההזזה אינו גדול ולכן פיצוחם אינו קשה. מה גם שפיצוח של אות אחת מגלה מיד את מפתח הצופן של כל שאר האותיות משום שהן כתובות בסדר הקבוע והידוע של אותיות הא"ב.
 - גם צפנים מסובכים יותר כמו הצופן במשימה 6 שמספר המפתחות שלו גדול מאד (כל המפתחות המקיימים שהאותיות של המילה "אני" עוברים למספרים 2, 41, 29) אינם מספקים את האבטחה הדרושה. מסתבר שתכונת החד חד ערכיות מהווה גם מגבלה הקשורה לעובדה שלכל שפה תכונות לשוניות אופייניות שאינן משתנות בהצפנה מונואלפביתית. אחת מהתכונות למשל היא שכיחות אופיינית של אותיות מסוימות במילים של אותה שפה (אותיות שמופיעות הרבה יותר מן האחרות הן למשל האות 'י' בעברית, או האות e באנגלית). גם צירופי אותיות וגם מילים מסוימות הם יותר שכיחים מאחרים. תכונות אלה ניתנות לגילוי בשיטות סטטיסטיות ויכולות לסייע לפיצוח טקסטים מוצפנים בצופן מונואלפביתי.
 - **הצפנה טובה היא כזו שמי שמכיר את המפתח מצפין ומפענח בקלות ובמהירות, ומי שאינו מכיר את המפתח יתקשה מאד בפיענוח הצופן.**



למורה:

בפעילות זו כל קבוצה תקבל טקסט אחד. הטקסטים מתייחסים לחוזק של ההצפנה וליעילות שלה. המסקנה היא שכמעט כל צופן אפשר לפרוץ באופן תאורטי, אבל באופן מעשי יש הצפנות שאי אפשר לפרוץ בזמן סביר או עלויות סבירות. עם זאת, התפתחות מהירה של הטכנולוגיה דורשת התפתחות של דרכי הצפנה מסובכות בהתאם. כל קבוצה תקרא את הטקסט ותענה על פיו על השאלה:

- דמיינו לעצמכם שיש בידיכם מידע מאוד מאוד אישי וסודי, ואתם צריכים להעביר אותו לאדם רחוק אחר. אתם יודעים שלהרבה אנשים יש גישה אל המסר שאתם מעבירים.
- האם הייתם מצפינים אותו באחת משיטות ההצפנה שראינו עד עכשיו?
- האם בכלל אפשר להצפין מידע ולהיות בטוחים ב-100% שהוא מוגן?

טקסט מספר 1:

הצפנה - הפתרון האולטימטיבי לשמירה על מידע סודי

מאת אילן סגלמן, 19 בספטמבר 2016

למורה: רעיון מרכזי של הטקסט - הצפנה היא אמצעי הכרחי להגנה על המידע והפרטיות שלנו.

ניתן למנוע גניבה של המידע באמצעות הצפנה, אך ארגונים רבים לא עושים זאת עד אשר הם חווים פריצה.

טקסט מספר 2:

עדי שמיר: "חברות האבטחה לא מצליחות לשמור על המידע"

מאת רפאל קאהאן, 03 במרץ 2013

למורה: רעיון מרכזי של הטקסט - ההצפנה המודרנית לא מאבטחת את המידע מפני נזקות ווירוסים היושבים במחשב

ועוקבים אחרי התהליכים והמידע המתרחשים בו. על כן היא הופכת לא רלוונטית לשמירה על המידע שלנו.

טקסט מספר 3:

גוגל השיגה עליונות קוונטית. מה זה אומר?

מאת טל שחף, 24 באוקטובר 2019

למורה: רעיון מרכזי של הטקסט - גוגל מאשרת כי מחשב הקוונטום שהיא מפתחת הצליח לעקוף בביצועיו את מחשב

העל החזק בעולם. יכולות החישוב שמחשב זה מסוגל להן יאפשרו לפתח יכולות הצפנה בלתי ניתנות לפריצה. יחד עם זאת, ייקח עוד זמן עד שהמחשב הקוונטי יהיה זמין לשימוש.

טיעונים מתמטיים העולים ממערך השיעור בהקשר לשאלה -

האם אתם תומכים או מתנגדים להוספת מידע ה-DNA שלכם לדרכון הביومتر

- הצפנות ניתנות לפיצוח גם אם מפתח ההצפנה שלהם אינו ידוע (למשל על ידי ניחוש מילה, שכיחות אותיות ועוד).
- הצפנה ניתנת לפיצוח בהינתן מספיק משאבים וזמן.
- ההצפנות היום הן חזקות מאד ויגנו על המידע שלנו כל עוד ימשיכו לשכלל אותן בהתאם להתפתחות הטכנולוגית המשכללת את יכולות הפיצוח.
- המחשב הקוונטי שעשוי לפצח את ההצפנות הקיימות היום במהירות רחוק עדיין מפיתוח, ובמקביל לפיתוחו מתפתחת טכנולוגית הצפנה קוונטית שהוא לא יצליח לפצח.
- גם אם לא יצליחו לפצח הצפנה, המידע הפרטי שלנו חשוף לוירוסים ונזקות היכולות לגשת אליו. לכן לא כדאי מראש לשמור במחשב מידע רגיש.