

8 איך לשלוח מידע סודי: הצפנה, פענוח, ושבירה

קבוצת גיל:	13 ומעלה.
דרישות קדם:	כושר הפשטה. החלפת (הצבת) אותיות – אתב"ש. איסוף סטטיסטיקה על אותיות בטקסטים.
זמן:	45-90 דקות.
חומרים:	לכל ילדה, עותק אחד מכל אחד מדפי העבודה, פרט ל-5 ו-6: עשרה עותקים לכתה כולה, ו-1: שני עותקים לכתה כולה. עפרונות ומחק.
גודל הקבוצה	מתאים לגדלים שונים – מיחידים ועד כיתה שלמה

דגשים:

- הצפנה
 - פענוח בהינתן המפתח הסודי
 - "שבירת" מערכת הצפנה ללא המפתח הסודי
 - הפרד ומשול, עבודה קבוצתית, בקרת איכות.
 - תכונות סטטיסטיות של השפה העברית
- את דפי העבודה יש לחלק ע"פ ההנחיות ולא את כולם יחד.**

תקציר: בפעילות זו נסביר את המושגים של הצפנה ופענוח תוך שימוש במפתח סודי משותף. נדון במטרות המצפין, המפענחת, וביריב המאזין לתקשורת המוצפנת ומנסה לפענח אותה, מבלי שיש לו גישה למפתח הסודי. נדגים מושגים אלה באמצעות מערכת פשוטה של החלפת, או הצבת, אותיות. נתרגל הצפנה ופענוח "חוקיים", בהינתן המפתח הסודי. לבסוף נראה כיצד סטטיסטיקת האותיות של השפה (העברית במקרה שלנו) מאפשרת ליריב לשבור את המערכת גם ללא המפתח הסודי.

רקע: שני צדדים, אשר נכנה אותם (בעקבות מסורת עתיקת ימים) אליס ובוב, מעוניינים לשלוח זה לזו הודעות רגישות, כלומר כאלה שאם יחשפו יגרמו לשניהם החל ממבוכה ניכרת, ועד אסון ממשי הכרוך באבדן רכוש ו/או חיים. לו השניים היו באותו חדר, יכלו פשוט ללחוש את ההודעות זה לזו. אבל אליס ובוב נמצאים הרחק אחד מהשנייה, ולרשותם עומדת מערכת תקשורת שהיא אמינה בדרך כלל, אך אינה מוגנת בפני האזנות. למשל טלפון, פקס, דואר אלקטרוני, או מכשיר קשר (בימי קדם היינו יכולים להוסיף אולי גם רצים או יוני דואר). מערכות כאלה מעבירות בד"כ את המידע הנשלח (שיחת הטלפון, הפקס, הודעת הדוא"ל, ההודעה האלחוטית) לצד השני. יחד עם זאת, צד שלישי יכול במאמץ סביר לצותת (להאזין) למידע הנשלח (במקומות רבים ציתות כזה אינו חוקי ומבצעו, אם ייתפס, עשוי לבלות בכלא, אך זה כמובן לא מונע ניסיונות ציתות).

תורת ההצפנות עוסקת בשיטות להסתרת מידע רגיש כזה על ידי הצפנתו. הצפנה אמורה, מצד אחד לאפשר לצד המקבל הלגיטימי לשחזר מחדש (לפענח) את ההודעה המקורית. מאידך, ההצפנה אמורה למנוע מיריב, שהצליח לצותת לתקשורת או להשיג בצורה אחרת את ההודעה המוצפנת, להבין את המסר המקורי או אף את חלקו.

הצפנות שמשו כבר בימי קדם, למשל בצבא הרומי (צופן פשוט מאוד הידוע בשם "צופן קיסר"). יש הטוענים כי לשיטת הצפנה הידועה כצופן אתב"ש יש מקורות תנכיים. למשל בנבואות ירמיהו שבספר ירמיהו, פרק כ"ה, פסוק כ"ו, במשפט "וּמַלְךְ שֶׁשָׁךְ יִשְׁתָּה אַחֲרֵיהֶם" המילה שֶׁשָׁךְ פירושה "בבל" (האות ב הוחלפה באות ש, והאות ל הוחלפה באות כ).

בעבר (נניח עד שנות הששים של המאה העשרים), פעולות ההצפנה התמקדו בעיקר בהקשרים צבאיים. בימינו, עם השימוש היום יומי הנרחב בתקשורת דיגיטלית ובאינטרנט, יש שימוש רב בהצפנה גם

בהקשרים מסחריים, ואפילו של אזרחים "סתם" שאינם רוצים שמישהו על הקו, ובפרט ה"אח הגדול", יוכל לקרוא את הדואר האלקטרוני שלהם או את פרטי כרטיס האשראי שלהם.

הפן השני של תורת ההצפנות הוא פיתוח שיטות לשבירה של מערכות הצפנה קיימות, ללא גישה למפתח הסודי. הדוגמה המפורסמת ביותר מסוג זה היא הניסיון המוצלח של המודיעין הבריטי במלחמת העולם השנייה בשבירת מערכת ההצפנה הגרמנית, ה"אניגמה". במאמץ זה שיחק תפקיד מפתח המתמטיקאי ומדען המחשב המחונן אלן טיורינג (Alan Turing).

הפיתוח המואץ של מערכות מחשוב ושל אלגוריתמים מתקדמים הוביל גם להתקדמות ניכרת בשיטות ההצפנה המודרניות (וגם בשבירת חלקן). כדוגמה קונקרטית, מערכות כגון Advanced Encryption Standard (AES) הן מערכות מהירות מאוד, ונחשבות בלתי שבירות.

בכל מערכת הצפנה "קלסית" יש מפתח סודי המשותף לשולח ולמקבלת, בוב ואליס (ומוסתר מכל צד שלישי). מפתח זה הוא סוד המאפשר גם להצפין הודעה וגם "לפתוח" את ההודעה המוצפנת. בהינתן המסר הגלוי (הנקרא באנגלית plaintext), השולח מפעיל אלגוריתם הצפנה, המשתמש הן במסר הגלוי והן במפתח הסודי, כדי לייצר את המסר המוצפן (הנקרא באנגלית ciphertext). המסר המוצפן מועבר באמצעות מדיית תקשורת אמינה, אך ייתכן ומועדת לציתות. הוא מגיע למקבלת, וזו מפעילה עליו אלגוריתם פענוח, המשתמש באותו מפתח סודי. אלגוריתם הפענוח משחזר את המסר המקורי.

פרמטר חשוב של בטיחות המערכת הוא מספר האפשרויות למפתח הסודי. אם מספר המפתחות הסודיים האפשריים הוא קטן יחסית, היריב יכול לנסות את כולם, ולאתר מפתח מתאים (מפתח המעתיק את ההודעה המוצפנת להודעה "בלשון בני אדם", כלומר הודעה תקנית בשפה הרלוונטית, אשר קרוב לוודאי תהיה זהה להודעה המקורית). כפי שנראה בהמשך, מספר גדול של מפתחות לא מבטיח בטיחות (ולכן, בלשון המתמטיקאים, זה תנאי הכרחי אך לא מספיק).

פעילות: אנו נציג ונלמד מערכת הצפנה ותיקה - הצפנה באמצעות החלפת (הצבת) אותיות. נסביר תחילה את שיטת ההצפנה ושיטת הפענוח באמצעות מפתח החלפה סודי. נתנסה בהצפנת טקסט קצר, ואח"כ בפענוח טקסט שונה (בהינתן המפתח הסודי). אחר כך נראה כיצד לנצל תכונות סטטיסטיות של השפה העברית כדי למצוא את המפתח הסודי ו"לשבור" את מערכת ההצפנה. כדי לבצע התקפה זו, כל שנזדקק לו הוא טקסט מוצפן ארוך מספיק (נניח בן כמה מאות אותיות). נעיר כי פעילות זו רלוונטית גם לכל שפה כתובה אחרת. אנו נדבק כמובן בעברית, אך כ"תרגיל רשות" אפשר ומומלץ לבצע אותה באנגלית, ערבית, רוסית, או כל שפה כתובה אחרת שהקוראים בקיאים בה.

בשיטת ההצפנה באמצעות החלפת אותיות, המפתח הסודי הוא טבלת החלפה של אותיות. לצרכי נוחות, הרווחים אינם מוחלפים ואינם נמחקים (כלומר רווח מקורי נשאר רווח בטקסט המוצפן). כמו כן, אנו מזהים אותיות סופיות כבנות זוגן הלא סופיות. למשל, האות "ף" היא מבחינתנו האות "פ". אנו מתעלמים לחלוטין, דהיינו מוחקים, את כל סימני הפיסוק, ואת האותיות הלועזיות. לצרכי נוחות, ספרות אינן מוחלפות ואינן מוצפנות. (הסבר למורה - מוסכמות אלו מסייעות לא מעט בפעילות הלא פשוטה של "שבירת" מערכת כזו. יחד עם זאת, עקרונות השבירה בהם נדון, כוחם יהיה יפה גם למערכות החלפה בהן אין עושים את ההנחות המקלות הנ"ל).

אנו נשתמש כאן במפתח ההצפנה הבא, אותו בחרנו באקראי:

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

נניח למשל כי המסר המקורי הוא שני הפסוקים הראשונים מתוך ספר בראשית:

" בְּרֵאשִׁית בָּרָא אֱלֹהִים אֶת הַשָּׁמַיִם וְאֶת הָאָרֶץ: וְהָאָרֶץ הָיְתָה תֵהוֹ וְבָהוּ וְחָשֶׁךְ עַל-פְּנֵי תְהוֹם וְרוּחַ אֱלֹהִים מְרַחֶפֶת עַל-פְּנֵי הַמַּיִם: "

שימו לב כי הטקסט מנוקד, אך כשנסיר את הניקוד לצורך ההצפנה, הכתיב שיוותר הינו כתיב חסר (למשל "תהו ובהו"). כשאנו מצפינים, מוחלפת כל אות מקורית באות המתאימה לה על פי מפתח ההחלפה. כך למשל תוחלף "ב" ב-"ט", "ר" ב-"ח", "א" ב-"י", "ש" ב-"ה", "י" ב-"ר", ו-"ת" ב-"ד". המילה "בראשית" תוחלף אפוא ב-"טחיהוד".

חלקי לתלמידים את מפתח ההצפנה (דף עבודה 1), ובקשי מהם להצפין את המסר תוך שימוש במפתח הסודי. חשוב להזכיר כי בשיטתנו מצפינים רק אותיות, כי אותיות סופיות מוצפנות כאילו היו מקבילותיהן הלא סופיות, וכי רווחים נשמרים. אחרי שרוב הכתה ישלים את המשימה, הזמיני את אחת התלמידות ללוח ובקשי ממנה שתסביר את הצפנת ההודעה.

למורה - ההודעה המוצפנת היא: טחיהוד טחי יפלוג יד להגוג עיד ליחק עליחק לודל דלע עטלע עאהס כפ שצו דלעג עחעא יפלוג גחאשד כפ שצו לגוג

הבנו אם כן כיצד בוב מצפין. אבל כיצד אליס, אשר בידה עותק זהה של מפתח ההחלפה הסודי, מפענחת?

הפענוח מתבצע בצורה דומה להצפנה. אליס עוברת אחת אחת על אותיות הטקסט המוצפן. היא מוצאת את האות הנוכחית בשורה התחתונה של מפתח ההצפנה. אות זו היא ה"אות המוחלפת". אליס רואה מי היא האות שמעליה במפתח ההצפנה. זוהי "האות המקורית". אליס רושמת את האות המקורית, ומתקדמת לאות הבאה בטקסט המוצפן, וכך הלאה עד לסוף הטקסט.

חלקי לתלמידים את דף עבודה מספר 2. בדף זה מופיע מפתח הצפנה (זהה לזה שבדף העבודה הקודם), ומשפט (אחר) מוצפן. המשפט המוצפן הוא

" יוצ פחיעד יד למטחוג לותט יפי טפט טפטמ סו למטח לאהעט טיגד רגעו גצ לכוצ "

הזכירי לתלמידים כי סימני פיסוק הושמטו בהצפנה, אותיות סופיות הפכו ללא סופיות, ורווחים נשמרו. בקשי מהתלמידים לפענח את המשפט ולרשום את המשפט המפוענח מתחת למקורי. אחרי שרוב הכתה ישלים את המשימה, הזמיני את אחד התלמידים ללוח ובקשי ממנו שיסביר את פענוח ההודעה.

למורה - ההודעה המקורית היא:

אין לראות את הדברים היטב אלא בלב בלבד כי הדבר החשוב באמת סמוי מן העין

(מתוך הספר "הנסיך הקטן" של אנטואן דה סנט-אכזופרי, בתרגומו של אריה לרנר). בהודעה המקורית היו גם שתי נקודות: לפני "כי" ואחרי "העין". אך משהושמטו, הפענוח כשלעצמו אינו יכול להוסיף אותן. כמובן שמפענח המבין את השפה יכול לנתח את הטקסט המפוענח, להבין היכן מסתיימים משפטים, ולנקד בהתאם.

כעת חלקי לתלמידים את דף עבודה מספר 3. בדף זה מופיעים שני עותקים של מפתח ההצפנה המוכר לנו. כל אחד מהתלמידים יכתוב את שמו או שמה: שם פרטי ושם משפחה, ללא רווח. השם יוצפן, ויכתב מתחת לשם המקורי. יש להעתיק את הטקסט המוצפן על דף חלק נפרד, ולמסור את הטקסטים המוצפנים (ורק אותם) למורה, שיחלק אותם באקראי בין התלמידים. עם קבלת הטקסט המוצפן, הוא יפוענח. צפו למספר שגיאות (משעשעות בד"כ). אחרי שרוב הכתה ישלים את המשימה, הזמיני את אחד התלמידים ללוח ובקשי ממנו שירשום את הטקסט המוצפן שקבל ואת פענוחו.

שבירה של מערכת הצפנה המבוססת על החלפת אותיות:

מערכת הצפנה שיש לה מספר קטן של מפתחות סודיים אינה בטוחה, כי היריב יכול לנסות את כולם (מספרם קטן) ולמצוא איזה מהם מייצר מתוך הטקסט המוצפן טקסט הגיוני (מבחינת השפה והתוכן) אשר סביר כי הוא הטקסט המקורי. אבל זה לא אומר כי מערכת שיש לה מספר גדול של מפתחות היא מערכת בטוחה. (בלשון המתמטיקאים, הרבה מפתחות הם תנאי הכרחי אך לא מספיק לבטיחות מערכת). למשל במערכת שלנו, מספר האפשרויות השונות להחליף בין עשרים ושתיים האותיות בשפה העברית הוא גדול: יותר מ-10 בחזקת 21 (ואם לדייק, המספר הוא $112400072777607680000 = 21!$). האם מספרם הרב של המפתחות פירושו שהמערכת בטוחה? כפי שניווכח מייד, התשובה היא לא (באלף רבת!).

מציאת המפתח ושבירת המערכת מבוססת על כך שבשפה העברית (ובכל שפה כתובה אחרת) יש חוקים סטטיסטיים, כלומר חוקים שהם תקפים ביחס לרוב הטקסטים הכשרים בעברית, ובלבד שאלה ארוכים מספיק. חוק סטטיסטי מסוג זה הוא **שכיחות האותיות**. האות השכיחה ביותר בטקסט עברי היא האות "י", ותדירות הופעתה ("ב"עברית ממוצעת") היא 11.4%. אחריה באה "ו", ותדירות הופעתה 10.6%. אחרונות משתרכות "ט" ו-"ז", עם 1.3% ו-0.8% בהתאמה. חוק סטטיסטי אחר דן בשכיחות של **מילים בנות שתי אותיות**. למשל, שלוש המילים השכיחות ביותר בטקסטים בשפה העברית הן "של", "על", ו-"את", לאו דווקא בסדר זה. (דרך אגב, שימו לב כי "את" ו"על" הופיעו בשני הפסוקים הראשונים בספר בראשית, אפילו פעמיים כל אחת, ו"את" הופיעה בטקסט הקצרצר מן הנסיך הקטן.)

הטבלה שלמטה מכילה את שכיחות האותיות בטקסט עברי "מודרני" המבוסס על עשרות מסמכים מהרשת שמקורם בעיתונים (הארץ, דה-מרקר, וואי-נט). האחוזים מסתכמים רק ל-99.9, וזאת בגלל שגיאת עיגול, הנובעת מכך שהדיוק הוא של ספרה אחת בלבד אחרי הנקודה העשרונית. מימין מופיעות האותיות השכיחות ביותר (י, ו, מ, ה). משמאל הנדירות ביותר (צ, ג, ט, ז). אותיות סופיות נכללות כחלק מ"אותיות האם" שלהן.

כדאי לפנות לתלמידים ולשאול לדעתם מיהן האותיות הנפוצות ביותר, ומיהן הנדירות ביותר. כדאי להעיר לתלמידים כי פילוג האותיות הוא **מאוד לא אחיד**. למשל, "י" מופיעה בערך פי 14 יותר מ"ז", ובערך פי 9 יותר מ"ט". חוסר אחידות זה הוא אחד הכלים המרכזיים שיאפשר לנו לפרוץ את שיטת ההצפנה שתיארנו. כתבי על הלוח את הטבלה כולה, אות אות ושכיחותה, כפי שהיא מופיעה כאן.

אות	י	ו	מ	ה	ל	ת	ר	ב	ש	א	נ	ע	כ	ח	ד	פ	ק	ס	צ	ג	ט	ז
%	11.4	10.6	9.1	8.2	7.0	5.9	5.7	5.4	4.9	4.8	4.3	3.0	2.7	2.6	2.6	2.4	2.3	1.9	1.6	1.4	1.3	0.8

נתאר כעת שיטה בת שני שלבים לשבירת ההצפנה. המפתח הסודי אינו ידוע לנו. נתון לנו טקסט מוצפן, ארוך מספיק (השיטה לא תעבוד על טקסטים קצרים מאוד). בשלב הראשון אנו מחשבים את שכיחות האותיות בטקסט המוצפן. אנו בונים טבלה ובה, לכל אחת מ-22 האותיות, נמלא את מספר ההופעות בטקסט המוצפן. בשלב שני אנו מסדרים את האותיות על פי שכיחות הופעתן. נסדר אותן כך שהאות השכיחה ביותר בטקסט המוצפן נמצאת מימין, זו הנפוצה פחות מכולן תהיה משמאל, וכל השאר ביניהן, על פי שכיחותן.

בהינתן סידור זה, מהי ההשערה הסבירה ביותר לגבי ההצפנה המקורית? הפני שאלה זו לכיתה. ההשערה הסבירה ביותר היא שהאות המוצפנת השכיחה ביותר מתאימה לאות השכיחה ביותר בעברית, דהיינו "י". השניה בשכיחותה תתאים לאות השניה בשכיחותה בעברית, דהיינו "ו", וכך הלאה. זוהי השערה סבירה בהחלט, אך האם היא נכונה? במקרה שלפנינו, כדאי לערוך ניסיון!

אנו עומדים לחלק לתלמידים את דף עבודה מספר 4. בדף זה יש טבלה ובה שכיחויות האותיות בעברית. בדף עבודה מספר 5, הצמוד אליו, מופיע משפט קצר, מוצפן באמצעות מפתח הצבה שונה מהקודם.

משפט זה מתאר מיקומו של אוצר. אם נפענח את המשפט נוכל למצוא את האוצר ולהשתקע באי טרופי, תחת עצי קוקוס, שמי תכלת, ולטייל על חופים זהובים.

המשפט המוצפן: בא פעברמ כשש טעקל מסמ נזא טאגזחתק

דיון קצר בכתה ישכנע את התלמידים כי לא ניתן לפענח טקסט מוצפן כה קצר. אבל לו עמד לרשותנו טקסט ארוך יותר המוצפן באמצעות אותו מפתח, המשימה תעשה אפשרית, באמצעות שימוש בשכיחות האותיות. חלקי כעת לתלמידים את דף עבודה מספר 6א'. זהו חלק מטקסט ארוך מספיק (6א' וגם 6ב'), אשר הוצפן תוך שימוש במפתח החלפה בו השתמשנו גם למיקום האוצר. לו לא היו לנו מגבלות של זמן ואורך רוח, ניתן היה לבקש מן התלמידים לחשב את שכיחות האותיות בטקסט המוצפן כולו. אבל בטקסט המלא יש 458 מילים, ובהן 1812 אותיות. ספירת אותיות כה רבות על ידי התלמידים תיקח זמן רב, ועלולה להיות מייגעת למדי. לכן בקשי מהכיתה לספור את השכיחויות רק בפסקה הראשונה, והשלימי להם את היתר ("ידע אישי"). בכיתות עקשניות במיוחד ניתן לחלק את כל הטקסט (6א' וגם 6ב'), אך ברוב הכיתות נסתפק בחלוקת 6א'. כדי להקל על המשימה של ספירת האותיות בפסקה הראשונה של 6א', נחלק את הכתה לארבע או חמש קבוצות. הקבוצה הראשונה תהיה אחראית על האותיות א' עד ה', השניה על ו' עד כ', וכדומה. חלקי לכתה ארבעה או חמישה עותקים של דף עבודה 7, אחד לכל קבוצה, בו יסכמו את מספרי ההופעות. בקשי לרכז זאת אח"כ על הלוח, ואז כתבי על הלוח את טבלת מספר מופעי האותיות השונות בטקסט.

למורה: הטבלה הסופית של מספר מופעי האותיות בטקסט, אותה נמסור לתלמידים, היא

אות	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
הופעות	127	50	51	20	151	161	21	101	105	23	95	42	79	43	45	75	48	13	104	207	208	43

שימו לב כי "נ" ו-"ת" מופיעות בדיוק אותו מספר פעמים (שתיהן 43). כעת בקשי משני תלמידים לגשת ללוח, לרשום תחילה את טבלת השכיחויות, וכעת למיין אותה כאשר האות השכיחה ביותר, במקרה שלנו "ש", נמצאת מימין. את זוג השווים ניתן לרשום כך או כך.

אות	ש	ר	ו	ה	א	ט	ק	ח	כ	מ	ע	ג	ב	פ	ס	נ	ת	ל	י	ז	ד	צ
הופעות	208	207	161	151	127	105	104	101	95	79	75	51	50	48	45	43	43	42	23	21	20	13

נזכיר כי בעברית "ממוצעת", סדר האותיות הוא

ז	ט	ג	צ	ס	ק	פ	ד	ח	כ	ע	נ	א	ש	ב	ר	ת	ל	ה	מ	ו	י	אות
0.8	1.3	1.4	1.6	1.9	2.3	2.4	2.6	2.6	2.7	3.0	4.3	4.8	4.9	5.4	5.7	5.9	7.0	8.2	9.1	10.6	11.4	%

ועל כן ההשערה הסבירה ביותר היא שמפתח ההחלפה המקורי (בסדר לא אלפביתי, דבר שאין לו משמעות) היה

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

(נזכיר כי "נ" ו-"ת" המוחלפות יכלו להיות גם בסדר ההפוך).

למורה: חשוב להבהיר מדוע אין להחליף את היוצרות ולהפוך את השורות: "י" היא האות הנפוצה ביותר בעברית. "ש" היא האות הנפוצה ביותר בטקסט המוצפן. לכן סביר כי בהצפנה "י" הוחלפה על ידי "ש", אך לא להיפך! כעת, "שאלת מיליון הדולר" היא האם מפתח ההצפנה המשוער הוא אכן המפתח הנכון. ניתן לערוך על כך דיון מעניין. אנו ממליצים להימנע מדיון כזה כרגע, ופשוט לנסות לפענח על פי המפתח המשוער. חלקי לכתה עותקים של דף עבודה מס' 8, עותק אחד לכל תלמיד/ה. הדף מכיל את המפתח המשוער, ואת שבע השורות הראשונות של הטקסט המוצפן. המשימה היא לבצע את הפענוח על פי המפתח, ולבדוק האם הצלחנו במשימה. "הצלחה" תוגדר כטקסט בעל משמעות בעברית מתקבלת על הדעת. אחרי שרוב הכיתה סיים את ניסיון הפענוח, בקשי מאחד התלמידים לרשום את השורה הראשונה (בלבד) על הלוח.

למורה: שלוש השורות הראשונות בתוצאת ניסיון הפענוח הן

שלושה שירי של להסא עוורא

חלשב

מילים ומבחיבה קבי גבקרוב

הטקסט שהתקבל אינו כתוב בעברית תקנית, ולכן לכאורה נכשלנו בניסיון הפענוח. מאידך ברור כי מתוך 10 המילים שלמעלה, 3 פוענחו נכון. למעשה סביר כי כבר בשלב זה יהיו תלמידים שיצליחו בהשלמת הפענוח על ידי ניחוש מוצלח ביחד עם אינטואיציה בריאה. אבל עדיף שקודם נדון במקור הכישלון! המסמך המוצפן המקורי "פוענח" על פי שכיחות אותיות בעברית "ממוצעת". אבל שכיחות האותיות בטקסט המקורי (וברוב הטקסטים) אינה תואמת בדיוק את הממוצע (כשם שאף אחד מאיתנו אינו תואם בדיוק את הממוצע באוכלוסייה של הגובה, המשקל, הגיל, קצב הנשימה, וכו'). לכן ה"פוענח" עדין לא הניב את הטקסט המקורי, או טקסט עברי תקין כלשהו. מאידך, ה"פענוח" הצליח להביא אותנו קרוב יותר למקור. כדי להבין מדוע, נזכיר את התכונה הסטטיסטית הברוכה לפיה אם המדגם גדול מספיק (וגם "אקראי מספיק"), אזי הפספוסים היחסיים אינם עצומים. למשל, האות השכיחה ביותר בעברית "ממוצעת" לא תהפוך לפתע לאות הנדירה ביותר במסמך המקורי. אם אינה השכיחה ביותר, היא תוכל להיות השנייה, השלישית או הרביעית בשכיחותה, אך בד"כ לא הרחק מזה.

ספציפית לענייננו, ניתן לתת לכתה את הרמזים הבאים (רצוי לרשום על הלוח):

ארבע האותיות השכיחות ביותר ב"עברית ממוצעת" הן (י, ו, מ, ה, ל), והן גם חמש האותיות השכיחות ביותר במסמך שהוצפן (ואפילו בסדר זה!).

מתברר גם כי מספר אותיות אף נשארו במקומן ביחס לעברית ממוצעת. אותיות כאילו הן "ר" ו-"ש". לכן מילים המכילות רק אותיות משבע אותיות אלו מפוענחות נכון. לזו הסיבה שהמילים "שלושה", "שירים", "של" ו-"מילים" מזדקרות לעינינו.

תכונה סטטיסטית נוספת שיכולה להועיל בפענוח הסופי: שלוש המילים הנפוצות ביותר בנות שתי אותיות בשפה העברית הן "של", "על", "את" (לאו דווקא בסדר זה). שלוש המילים בנות שתי אותיות הנפוצות ביותר במסמך המוצפן שלנו הן "כא", "טא", "טמ".

נזכיר גם כי בפענוחים שלנו רווחים ומספרים נשארו ללא שינוי. סימני פיסוק אחרים מן המסמך המקורי הושמטו. אותיות סופיות (ם, ן, ף, ה) הוחלפו באחיותיהן הלא סופיות (מ, נ, צ, פ).

יש לנו כעת את כל הכלים כדי להתבונן שוב במסמך המוצפן, לחשוב עוד, ולבצע פענוח סופי שלו. לפני ההסתערות הסופית, הזכירי לכתה כי ניחוש אינטליגנטי הוא בסיס חשוב לכל פעילות אינטלקטואלית-יצירתית. אל תחששו לנחש, אך גם דעו לא להתעקש אם הניחוש אינו מתפתח לטקסט קריא.

המשימה הסופית: פענוח המשפט בדף עבודה מספר 5. לשם כך נצטרך לפענח תחילה את הטקסט בדף עבודה 9: מהו המסמך הזה ומהן שבע השורות המופיעות בו. מכאן נקבל את מפתח ההצבה כולו, ובעזרתו נפענח את מיקום האוצר. בקשי מהפותרים רק להצביע, בלי לגלות לאחרים. אחרי שעשרה תלמידים יצליחו לפתור, קראי לראשונה מביניהם ללוח ובקשי שתסביר כיצד הגיעה לפתרון.

למורה: המסמך כולו (6'א ו-6'ב) מכיל שלושה שירים של להקת כוורת: גלשן (פאכח), שיעור מולדת (כשברק וראתמ), והמגפיים של ברוך (הופנששו כא עקרג). שבע השורות המדוברות הן

שלושה שירים של להקת כוורת

גלשן

מילים ומנגינה דני סנדרסון

יום בהיר של שמש אין שום עננים אני וכל החברה אל הים נוסעים

לקחנו את האוטו הבנות כבר שם כשלחוף נגיע נוציא את הגלשן

שוב אנחנו מתגלשים רוכבים על הגלים הנה בא עוד גל גדול

זהירות רק לא ליפול מחוף בת ים עד הרצלייה זה רק אני והגלשן שלי

פענוח מיקום האוצר מוביל למשפט: על גבעות שייח אברק תחת פסל אלכסנדר

(ביאור גיאוגרפי קצר: גבעות שייח אברק נמצאות בחלק המזרחי של עמק יזרעאל, סמוך לקריית טבעות וצמוד לאתר בית שערים. על הפסגה הגבוהה נמצא פסל "השומר" אלכסנדר זייד, זקוף על סוסו, משקיף על העמק.)

אחרי ששבירת ההצפנה תופנם על ידי מרבית התלמידים, ניתן לשאול את הכתה כיצד היתה השבירה מושפעת לו רווחים היו מושמטים, וספרות היו מוצפנות. לסיכום, חשוב להדגיש כי פעילויות של תכנון מערכות הצפנה חדשות וניסיונות לשבירתן ממשיכות למשוך חוקרים בתעשייה, באוניברסיטאות, ובארגוני ביון. יש היום מערכות הנחשבות בלתי שבירות, אפילו בעזרת מחשבי על. ואם הגענו בשלום עד כאן, המשתתפים ראויים בהחלט לטפיחה על השכם.

אִישׁ אֶת רֵעֵהוּ יַעֲזְרוּ וּלְאָחִיו יֵאמֶר חֲזֵק

דף עבודה מס' 1

מפתח סודי לקוד החלפת אותיות:

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

עליכם להצפין את המשפט

"בראשית, ברא אלהים, את השמים, ואת הארץ. והארץ היתה תהו ובהו, וחשך, על פני תהום. ורוח אלהים, מרחפת על פני המים."

דף עבודה מס' 2

מפתח סודי לקוד החלפת אותיות:

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

עליכם לפענח את המשפט המוצפן

" יוצ פחיעד יד למטחוג לותט יפי טפט טפטמ סו למטח לאהעט טיגד רגעו גצ לכוצ "

דף עבודה מס' 3

מפתח סודי לקוד החלפת אותיות:

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

1) כתבי/כתוב את שמך המלא (ללא רווח בין השם הפרטי ושם המשפחה).

שם מקורי:

2) הצפיני/הצפן את הטקסט המקורי על פי מפתח ההצבה בראש העמוד.

שם מוצפן:

3) העתיקי/העתק את השם המוצפן לכאן. השווי/ה לוודא כי אין טעויות.

שם מוצפן מועתק:

4) מסרי/מסור את הטקסט המועתק למורה וקבלי שם מוצפן אחר. בעזרת מפתח ההחלפה, פענח/י אותו ושחזר/י את השם המקורי (ניתן לעשות זאת כי שני הצדדים השתמשו באותו מפתח).

פענח את השם שקבלתם:

5) השוו את השמות המפוענחים למקוריים. האם דייקתם בכל האותיות?

דף עבודה מס' 4

טבלת שכיחות האותיות בשפה העברית:

אות	י	ו	מ	ה	ל	ת	ר	ב	ש	א	נ	ע	כ	ח	ד	פ	ק	ס	צ	ג	ט	ז
%	11.4	10.6	9.1	8.2	7.0	5.9	5.7	5.4	4.9	4.8	4.3	3.0	2.7	2.6	2.6	2.4	2.3	1.9	1.6	1.4	1.3	0.8

דף עבודה מס' 5: מיקום האוצר (קטע מוצפן קצר)

משפט המתאר את מיקומו של אוצר יקר ערך. המשפט מוצפן באמצעות מפתח הצבה לא ידוע (ושונה מן הקודמים):

בא פעברמ כששס טעקל מסמ נזא טאגזחתק

האם יש לנו מספיק אינפורמציה כדי לפענח את המשפט?

דף עבודה מס' 6א': קטע טקסט ארוך יותר, מוצפן ע"י אותו מפתח הצבה

למרבית המזל, התגלה יחד עם המשפט טקסט מוצפן באמצעות אותו מפתח הצבה לא ידוע. הטקסט ארוך בהרבה, ולכן נוכל אולי, בכוחות משותפים, לפענחו. בשלב ראשון, נספור את שכיחות האותיות בפסקה הראשונה (שבע שורות) בלבד.

כארכה כשקשו כא אהלמ גררקמ

פאכח

ושאשו רוחפשחה תחש זחתקזרח

שרו עהשק כא כוכ טשח כרו בחחשו טחש רגא הסעקה טא השו חרזבשו

אלסחר טמ הטרצר העחרמ געק כו גכאסרנ חפשב חרדשט טמ הפאכח

כרע טחסחר ומפאכשו קרגעשו בא הפאשו החה עט ברת פא פתרא

יהשקרמ קל אט אשנרא וסרנ עמ שו בת הקדאששה יה קל טחש רהפאכח כאש

וסגשו עושו כשערט הפא טו הרט אט פערה טי אט יישו עגאא

קרט וחכעמ רהשו פרבכ קל איה סשגשחר טנכק אהמפאכ

כרע טחסחר ומפאכשו קרגעשו בא הפאשו החה עט ברת פא פתרא

יהשקרמ קל אט אשנרא וסרנ עמ שו בת הקדאששה יה קל טחש רהפאכח כאש

כוכ געק כרלבמ רהשו חזפק גא טסת עעשמ בדרע כיה חפוק

יהר זרנ אסרנכ כרע אאשורתשו טג אט שהשה עשמ זנק טו שכ וסק פאשו

כרע טחסחר ומפאכשו קרגעשו בא הפאשו החה עט ברת פא פתרא

דף עבודה מס' 6ב' : המשך קטע הטקסט הארוך, מוצפן ע"י אותו מפתח הצבה

יהשקמ קל אט אשנרא וסרנ עמ שו בת הקדאששה יה קל טחש רהפאכה כאש

כשברק וראתמ

ושאשו באש ורהק

וחפשחה טנקשו כושק

טי עעשמ הזנק בא הלשק מורחה רהטשגק סרקכ עה טמ הטתוה

רעקלב העקרכשו כוש קקע ששררקשו הטשגק שדושס אחר אסו כחהשה פתראשו

רהורקה טרוקמ ברת ובצ געק זמשר עכשברק וראתמ השט וקטה סדע

השרקה שערט בגכשר כנב צשנרמשר גרשארח כלרנ בא נחש הבול הנרקכ כתרמשר

גג יה השה נכצרמ קגה יה הדצששק עשאתרמחר כהשמה שנה

רגג עתושרהחר המקער נאטרמ הנצשכשו חשפחר וסקכרמ קחרמ

שכ שרפעשו רשכ גרקושו טקד כא קרבשו גג יה הדצששק עשאתרמחר כהשמה שנה

הופנשו כא עקרג

ושאשו טארח טראטקדשל תחש זחתקזרח רוחסו ישאעקוח

וחפשחה תחש זחתקזרח

הרט לחה טרמח עירא הח השר ואתרמ עסרא הרט חשלה טרמח עזנשקצ גא כבמששו

הטגשא טרמח וקל גכהלשטר הרט כמל הרט אלס טרמח אזקצ גא שרושו

טעא שרו טסת הרט לו בתששח וחרוחו סשנכ מופנששו עטקרה
רעולרו כהח השר קל פקעששו חכטקר כזשנקר אר טמ הגא עהשפשרח כ

חבאששו לרחשו והק רפקעששו אט סזק טג ופנששו רוגחזששו
כמושח לרחשו לרונאצ לכה וטרח אהכשפ טרמו גבמ חפחש חפחש פשצקה

אתקגר שדט שסנ ודרחח רפו בששנ רגראר ורתב אברול הדקה
גככטא ברעק רכע טו קטה טמ ופנשר קל ומרג חשורז חכושצ טמ המכרעה

עקרג מק ענגק רבשק עודע וטרח כעשק התנקזשה עורסר הכמראאה
גכנחה סזק טרחשו אותרק ששנרכ לקרעשו המקפי באשר נלשת הלעאה גש

חבאששו לרחשו והק

רהחה אשת סרה כו ושאה מושושה הרט פשאה בלערמ כאט חבכר ויוח
רנמטרו עשח הכשששו הרט כוב כו אסכרכשו עיקרברמ עסרק טסק קטה טרמה

אט שתב הרט וה אבכרמ טו אדסרל טר קל אעגרמ וה כאט שהשה הרדשט טמ הוצנסמ
טמ ההרט אדת אלס רכאנ טמ הטלתס כשקה באשר גתרק טסת עמסמ גש

חבאששו לרחשו והק

טי ההרט טוק זאססה לשנא טמ הכושגה רהאג העשמה עאש אבכרמ סגורמ
רוטי רבת השרו פו עפכו פו עסרו הח מנרקרמ טדאר שכק אבדורמ גש

חבאששו לרחשו והק

רטו טמה אט וטושה

מכטא טמ עקרג

דף עבודה מס' 7: ספירת שכיחות האותיות בקטע טקסט מוצפן (בפסקה 1 בלבד)

אות	מספר הופעות (סימון ע"י קוים)	מספר הופעות
א		
ב		
ג		
ד		
ה		
ו		
ז		
ח		
ט		
י		
כ		
ל		
מ		
נ		
ס		
ע		
פ		
צ		
ק		
ר		
ש		
ת		

דף עבודה מס' 8: פענחו את שמונה השורות שלמטה על פי המפתח המוצע כאן

טבלת שכיחות האותיות בשפה העברית:

אות	י	ו	מ	ה	ל	ת	ר	ב	ש	א	נ	ע	כ	ח	ד	פ	ק	ס	צ	ג	ט	ז
%	11.4	10.6	9.1	8.2	7.0	5.9	5.7	5.4	4.9	4.8	4.3	3.0	2.7	2.6	2.6	2.4	2.3	1.9	1.6	1.4	1.3	0.8

מופעי אותיות בטקסט

אות	ש	ר	ו	ה	א	ט	ק	ח	כ	מ	ע	ג	ב	פ	ס	נ	ת	ל	י	ז	ד	צ
הופעות	208	207	161	151	127	105	104	101	95	79	75	51	50	48	45	43	43	42	23	21	20	13

מפתח סביר לניסיון פענוח

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

כארכה כשקשו כא אהלמ גררקמ

פאכח

ושאשו רוחפשחה תחש זחתקזרח

שרו עהשק כא כוכ טשח כרו בחחשו טחש רגא הסעקה טא השו חרזבשו
אלסחר טמ הטרצר העחרמ געק כו גכאסרנ חפשב חרדשט טמ הפאכח

כרע טחסחר ומפאכשו קרגעשו בא הפאשו חחה עט ברת פא פתרא
יהשקרמ קל אט אשנרא וסרנ עמ שו בת הקדאששה יה קל טחש רהפאכח כאש

תוצאת ניסיון הפענוח:

דף עבודה מס' 9 פענחו באופן מלא את תחילת הטקסט המוצפן (שבע שורות) מדף עבודה 6א'. מומלץ להיעזר בניחושים אינטליגנטיים וכן ברמזים שקבלתם מהמורה. עם השלמת המשימה, מצאו את מפתח ההצבה ובעזרתו את מיקום האוצר (לא לרוץ, יש מספיק אוצרות לכוווולם).

פיענוח שבע השורות:

מפתח ההצבה הסודי

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

מיקום האוצר (מוצפן): בא פעברמ כששס טעקל מסמ נזא טאגזחתק

מיקום האוצר (טקסט מקורי):