פעילות בכיתה – הצפנה

מטרות

מטרת הפעילות היא להדגים מהלך שלם של הצפנה על כל שלביו:

1. תיאום בין השולח לנמען של שיטת ההצפנה ושל המפתח,
2. הצפנת מסר על-ידי השולח,
3. שליחת המסר המוצפן מהשולח לנמען,
4. פיענוח המסר המוצפן על-ידי הנמען.

הפעילות ממחישה הצפנה סימטרית. סוג זה של הצפנה היה קיים, בגרסאות פשוטות יחסית, כבר בימי קדם. גרסאות מתוחכמות שלו נמצאות בשימוש עד היום. לפני כ-40 שנה פותחו שיטות הצפנה חזקות שהן אסימטריות, כלומר אינן משתמשות באותו מפתח להצפנה ולפענוח, ואף אינן מחייבות תיאום מראש של מפתח מוסכם. למידע נוסף ראו בויקיפדיה, ערך מפתח_ציבורי.

ניתן לבצע את הפעילות בכיתה בהנחיית המורה, או גם על ידי זוג תלמידים בכוחות עצמם.

החומרים

תדפיס של דף חלוקה לזוגות (לשמוש המורה).

תדפיס של דף גלגלי הצפנה ושל טופס ההצפנה – סט אחד לכל תלמיד.

מספריים – זוג לכל תלמיד או כמה תלמידים.

מהלך הפעילות

הקדמה

מטרת השיעור היא ללמוד מה היא הצפנה ומהם התהליכים הנדרשים כדי להצפין מסר וכדי לקרוא מסר מוצפן.

הצפנה היא שיטה להסתרת תוכנו של מסר באופן שקורא מזדמן לא יוכל להבינו, בעוד שמי שאמור לקבלו יוכל לפענח אותו. להצפנה מגוון שמושים מועילים: בצבא, לדוגמא, משתמשים בהצפנה כדי להסתיר מידע מהאויב. במסחר ובבנקאות משתמשים בהצפנה כדי לבצע עסקאות דרך האינטרנט. באין ספור מחשבים ואתרי אינטרנט משתמשים בה כדי להבטיח שמידע רגיש לא ייפול לידיים לא נבונות. ברוב שיטות ההצפנה יש שימוש בסוד מוסכם בין השולח והמקבל (סוד שמכונה "מפתח" או "סיסמה") שבלעדיו בלתי אפשרי (או קשה) לפצח את המסר המוצפן.

שאלות לתלמידים:

- אילו שיטות הצפנה אתם מכירים? (לרשום תשובות על הלוח).
- איזו מבין השיטות שהועלו היא לדעתכם החזקה (חסינה בפני פיצוח) ביותר?
- איזו מבין השיטות שהועלו היא לדעתכם הנוחה ביותר לשימוש?

האתגר שלכם בשיעור הוא להעביר מסר קצר בין זוגות ולהסתיר ממני את המסר, אפילו אם אתפוס את הפתק. את המסרים תצפינו בעזרת גלגלי הצפנה.

כל המסרים יועברו באופן גלוי על ידי העברת פתקים. אין להשתמש בטלפון.

הסבר על גלגלי ההצפנה

מחלקים את הדף עם גלגלי ההצפנה.

מסבירים שיש בדף מרכיבים הדרושים למימוש 3 גלגלי הצפנה שונים הנקראים "צופן קיסר", "צופן אתב"ש" ו-"צופן החלפה שרירותי".

מבקשים מהתלמידים לנסות להבין בעצמם איך עובדים גלגלי ההצפנה ולהסביר את תהליך ההצפנה שמגולם בהם.

משלימים את ההסבר ככל הנדרש:

- אלו צפני החלפה, כלומר כל אות מוחלפת באות אחרת לפי טבלה מוגדרת מראש. הטבלאות מיושמות כאן בצורה מעגלית בגלגלים: אותיות המסר הגלוי במעגל החיצוני ואותיות המסר המוצפן במעגל הפנימי.
- בצופן אתב"ש האות א מוחלפת באות ת, האות ב באות ש, וכן הלאה.
- בצופן קיסר כל אות מוחלפת באות שנמצאת מספר מקומות קבוע אחריה באלפבית. מספר המקומות נקרא המפתח. למשל, אם המפתח הוא 3, אז האות א מוחלפת באות ד, ב מוחלפת ב-ה, וכן הלאה. **ההחלפה היא מעגלית,** כלומר ת מוחלפת ב-ג, ש מוחלפת ב-ב, ר מוחלפת ב-א.
- בצופן ההחלפה השרירותי טבלת ההחלפה נבחרה **מראש** באופן מקרי.
- בצופן קיסר ובצופן ההחלפה השרירותי ניתן לסובב את הגלגל הפנימי ביחס לחיצוני. המפתח הוא האות שתחת החץ האדום (כלומר האות שמחליפה את א), שהרי בהינתן הגלגלים והאות שמחליפה את א, כל יתר האותיות נקבעות אף הן.
- כדי ששני צדדים (השולח והמקבל) יתקשרו בצורה מוצפנת, עליהם להפגש ולהסכים באיזה צופן (גלגל) הם ישתמשו, ובאיזה מפתח (מלבד בצופן אתב"ש שאינו משתמש במפתח).
- להנחות את התלמידים לגזור מהדף את העיגולים הדרושים להם ולהסתיר את השאריות כדי שהמורה לא יוכל/תוכל לזהות את הגלגל שבו הם משתמשים.

הסבר על התהליך בביתה

מחלקים את התלמידים לזוגות. ניתן להיעזר בדף החלוקה לזוגות, כך:

- יש לגזור מראש את דף החלוקה לזוגות בהתאם למספר התלמידים בביתה.
- לחלק את הביתה לשני חלקים שווים, ימין ושמאל.
- לחלק לתלמידים פתקים עם מספרים כך שלכל תלמיד בחלק אחד יהיה בן זוג בחלק השני.

כל זוג צריך להפגש, לבחור בסוד באיזה צופן (גלגל) הם ישתמשו ובאיזה מפתח (מלבד בצופן אתב"ש), ולחזור למקומות. בהמשך יוכלו להשתמש בצופן ובמפתח שקבעו להעברת מסרים ביניהם בצורה מוצפנת.

מכינים את גלגל ההצפנה שנבחר: גוזרים את גלגל המסר הגדול, ואם נבחר צופן קיסר או צופן ההחלפה השרירותי, גם את גלגל הצופן הקטן המתאים, אותו ממקמים (או מדביקים) במרכז גלגל המסר במצב שמתאים למפתח שנבחר.

מסתירים את את שארית הדף. הדף עם החורים יכול לרמוז למורה באיזו הצפנה משתמשים.

כותבים בטופס את המסר שאותו רוצים לשלוח לבן הזוג.

מצפינים את המסר על פי השיטה שהוסכמה ורושמים את המסר המוצפן בטופס.

גוזרים את המסר הגלוי ושומרים.

מקפלים את המסר המוצפן וכותבים בחוץ את שם בן הזוג שאליו צריך להגיע המסר.

מעבירים את הפתק דרך החברים בלי לקום.

הנמענים מפענחים את המסר שקיבלו מבן זוגם בעזרת הגלגלים.

המורה יכול/ה לבחור "לחטוף" פתק בדרך כדי לנסות ולפענח אותו. (אפשר לנסות להתביית על זוגות שבחרו אתב"ש ואז הפיענוח קל).

סיכום

להצפנה עם מפתח קבוע יש חסרונות. אם מגלים את המפתח, אפשר לקרוא את המסרים ללא כל קושי. אפשר גם לפצח צפנים בלי לדעת את המפתח. לדוגמא, אם ההודעה ארוכה מאוד אז אפשר לנחש את האותיות על פי תדירות ההופעה שלהן. התחום המדעי שמטפל במשימה זו נקרא קריפטוגרפיה (למידע נוסף ראו בויקיפדיה, ערך קריפטוגרפיה).

במלחמת העולם השניה היתה לצבא הגרמני מכונת הצפנה שנקראה "אניגמה". במכונה הזאת האותיות הוחלפו על ידי מספר גלגלי הצפנה בזה אחר זה, והגלגלים שינו את מצבם אחרי כל אות שהוצפנה. התוצאה היתה צופן שנחשב בלתי ניתן לפיצוח, הנחה שעלתה לגרמנים ביוקר: הבריטים הקימו צוות מיוחד של מתמטיקאים שהצליח, אמנם במאמץ גדול, לזהות נקודות תורפה בשיטת ההצפנה הזאת ולפענח את השדרים מבלי שהגרמנים העלו בדעתם שהמסרים שלהם גלויים לצד השני.

היום, באינטרנט, כמעט כל המידע שעובר ברשת הוא מוצפן כך שאי אפשר לגלות מה כתוב, אפילו אם מצליחים ליירט את התשדורת בדרך. מחשבים ש"מדברים" אחד עם השני מבצעים תהליך מסובך של בחירת צופן משותף באופן שאפילו מישהו ש"מקשיב" לשיחה ביניהם, אינו יכול לגלות את הצופן. לאחר שבחרו את הצופן, הם מעבירים ביניהם מידע.

התהליך הזה קורה כל פעם שאנחנו מתחברים לחשבון הבנק שלנו דרך האינטרנט, קונים משהו באינטרנט או שולחים מייל.

מידע נוסף

מידע רב בנושא ההצפנה ומדעי המחשב בכלל יש באתר **תערוכת CAPTCHA** של מוזיאון המדע ע"ש בלומפילד בירושלים.

פתקים לחלוקה לזוגות

שמאל	
1	11
2	12
3	13
4	14
5	15
6	16
7	17
8	18
9	19
10	20

ימין	
1	11
2	12
3	13
4	14
5	15
6	16
7	17
8	18
9	19
10	20

www.mada.org.il/captcha CAPTCHA

גלגלי צופן

גלגל מסר

CAPTCHA www.mada.org.il/captcha

BY NC SA

- סודי ביותר -

חלק א:

לאחר שהצפנתם את ההודעה גזרו חלק זה ושמרו אותו אצלכם

המסר הגלוי (לא מוצפן):

☐☐☐