

העברת מידע מוצפן ברשת

חקר הצפנה – מערך שיעור ודף לתלמיד

פותח ע"י מורים מובילים בשנת תשע"ד

בהנחיית ד"ר דורון זוהר

תודה לפרופ' עירד יבנה על

על הייעוץ האקדמי, התמיכה והסיוע בהכנת החומרים

הצפנה – מערך שיעור ודף לתלמיד

פיתוח: ויוי טרנר, ריקי יפה

נושא השיעור: הצפנה סימטרית - סוגי הצפנה - דף מלווה למורה

נושא השיעור: הצפנה – העמקה ותרגול 5 שיטות הצפנה סימטרית עיקריות יש לחלק את הכיתה לקבוצות של 5 תלמידים (להוראת כלל שיטות ההצפנה שבתכנית הלימודים).

שני מפגשים לאחר שיעור מבוא להצפנה: שיעור מעשי לאחר הקדמה כללית בנושא הצפנה.

קהל יעד: תלמידי כיתה ט' הלומדים במסגרת העתודה מדעית טכנולוגית.

מיקום: מעבדת מחשבים עם חיבור לאינטרנט.

ידע קודם: היכרות עם המושג הצפנה ופיענוח.

קשר לתכנית הלימודים במדעי המחשב: פרק 3

פירוט סוגי הצפנה שהתלמידים יחקרו, ילמדו וילמדו את חבריהם לקבוצה:

צופני שחלוף פשוטים

צופני הזזה (Shift) – צופן יוליוס קיסר (כולל הזזה מודולרית)

צופן ערבול - על ידי היפוך סדר האותיות במסר

צופן "זיגזג"

צופן השביל המתפתל

ילמד בעזרת סרטון (שיעור הפוך):

one time pad (פנקס חד פעמי/http://en.wikipedia.org/wiki/One-time_pad)

חומרי עזר למורה ולתלמידים:

דף תבנית לחקר הנושא

מטרות:

- התלמידים יחקרו וכירו ויתרגלו שיטות הצפנה סימטרית.
- במסגרת העבודה התלמידים יתנסו מעשית בהצפנה ובפיענוח מסרים לפי שיטות הצפנה שונות.
- בכל קבוצה כל תלמידי יציג, יסביר וייתן משימות לשיטת ההצפנה אותה חקר בפני כל חברי קבוצתו (שיטת גייקסו – [הסבר בסוף השיעור](#)).
- התלמידים יעבדו בעבודת צוות, בשיתוף פעולה ובכבוד הדדי.

מהלך השיעור:

הערות	תיאור	זמן כ-	שלב השיעור
מפגש 1			
	הצגת הנושא : תזכור קצר לגבי מושגי הצפנה ופיענוח.	כ- 10 דק'	פתיחה
צרוף דף משימה למורה	דרך השיר " אבא ניבי אובות בך..." הכרת המושגים : מפתח הצפנה ואלגוריתם ההצפנה	כ- 15 דק'	פעילות מקדימה
כל תלמיד מקבל דף תבנית מובנה	הסבר המשימה, חלוקה לקבוצות בנות 5 תלמידים וחלוקת דף תבנית לכל תלמיד.	כ- 15 דק'	התארגנות
על כל תלמיד להכין דף מפורט בהתאם לדף התבנית הכולל הסבר קצר, הדגמה ושניים שלושה תרגילים בנושא	כל תלמיד אחראי לחקור, להתעמק ולהבין שיטת הצפנה אחת מתוך הרשימה 1. צופני שחלוף פשוטים 2. צופני הזזה (Shift) – צופן יוליוס קיסר (כולל הזזה מודולרית) 3. צופן ערבול - על ידי היפוך סדר האותיות במסר 4. צופן "זיגזג" 5. צופן השביל המתפתל	כ- 50 דק'	עבודת חקר בשיטת ג'קסו (ראה הסבר בהמשך)
מפגש 2			
	להסביר בכמה מילים את תהליך הלמידה, שבו כל תלמיד בתורו מלמד, מדגים ומתרגל את יתר חברי קבוצתו את שיטת ההצפנה אותה חקר/ה	כ- 10 דק'	הקדמה והסבר לתהליך השיעור
בסיום תהליך הלמידים כל התלמידים הבינו ותרגלו את חמשת שיטות ההצפנה	כל תלמיד/ה בתורו/ה בהתאם למספור השיטה (1-5) מלמד, מדגים מתרגל את השיטה אותה למד/ה	כ- 16 דק' X 5 = 80	תהליך הלמידה, הדגמה, תרגול

שלב השיעור	זמן כ-	תיאור	הערות
מפגש 3			
פתיחה	15 דק'	סיכום כללי על חמשת שיטות ההצפנה שנלמדו עד כה	
תרגול כיתתי	30 דק'	חידות הצפנה (כל מורה מכין לעצמו)	המורים מוזמנים לשלוח לנו רעיונות לחידות
שיטת הצפנה One time pad	15 דק'	הפניית התלמידים לצפייה בסרטון + זמן צפייה	הבנת שיטת הצפנה
תרגול כיתתי	30 דק'	תרגול ההצפנה ע"י המורה בכיתה	
מפגש 4 - בוחן			

קבוצות הרכבה Jigsaw

פותחה על ידי ארונסון ואחרים (1978; מתוך ריץ, 1996). לשיטה זו ארבעה שלבים:

- חלוקת הכיתה לקבוצות אם הטרוגניות של 4-5 תלמידים ומתן משימה לימודית כוללת וזהה לכל הקבוצות, המתחלקת למספר החברים בכל קבוצה. כל חבר קבוצה מקבל מספר מ-1 עד 5 על פי תתי הנושאים של המשימה הכוללת.
- קבוצות מומחים - כל התלמידים שבחרו אותם תתי-נושא מתקבצים לקבוצות חדשות. בקבוצות אלה התלמידים לומדים באופן מעמיק את הקטע המסוים שלהם, כדי להורותו לאחר מכן בקבוצות האם.
- הוראה בקבוצות האם - כל מומחה מגיע לקבוצת האם שלו ומלמד את נושא התמחותו. לאחר שכל הצוות הסביר את הנושאים, מתנהל דיון משותף להבהרת כל החומר.
- מבחן אישי - כל תלמיד נבחן על החומר כולו.
- פרסום התוצאות.

תבנית חקר לתלמיד על פי נושא – דפים לתלמיד

בדפים הבאים מובאות 5 תבניות לדפי עבודה לתלמיד:

1. צופני שחלוף פשוטים
2. צופני הזזה (Shift) – צופן יוליוס קיסר (כולל הזזה מודולרית)
3. צופן ערבול - על ידי היפוך סדר האותיות במסר
4. צופן "זיגזג"
5. צופן השביל המתפתל

דף משימה לתלמיד – תבנית חקר

הנחיות למילוי דף העבודה :
1. יש להגיש את דף העבודה לבדיקת המורה לפני מועד השיעור
2. עליך לדאוג שלכל חבר בקבוצתך יהיה עותק מדף משימה זה!

מספר הקבוצה: _____

שם התלמיד: _____

שיטת ההצפנה: (1) צופני שחלוף פשוטים

א. תיאור כללי של שיטת ההצפנה:

ב. מפתח ההצפנה: תלמידי כיתה ט' הלומדים במסגרת העתודה מדעית טכנולוגית.

ג. אלגוריתם ההצפנה: מעבדת מחשבים עם חיבור לאינטרנט.

ד. דוגמא להצפנה ופיענוח על פי השיטה והסבר:

ה. תרגילים לתרגול

עבודה נעימה!

דף משימה לתלמיד – תבנית חקר

הנחיות למילוי דף העבודה :
1. יש להגיש את דף העבודה לבדיקת המורה לפני מועד השיעור
2. עליך לדאוג שלכל חבר בקבוצתך יהיה עותק מדף משימה זה!

מספר הקבוצה: _____

שם התלמיד: _____

שיטת ההצפנה: (2) צופני הזזה (Shift) – צופן יוליוס קיסר (כולל הזזה מודולרית)

א. תיאור כללי של שיטת ההצפנה:

ב. מפתח ההצפנה: תלמידי כיתה ט' הלומדים במסגרת העתודה מדעית טכנולוגית.

ג. אלגוריתם ההצפנה: מעבדת מחשבים עם חיבור לאינטרנט.

ד. דוגמא להצפנה ופיענוח על פי השיטה והסבר:

ה. תרגילים לתרגול

עבודה נעימה!

דף משימה לתלמיד – תבנית חקר

הנחיות למילוי דף העבודה :
1. יש להגיש את דף העבודה לבדיקת המורה לפני מועד השיעור
2. עליך לדאוג שלכל חבר בקבוצתך יהיה עותק מדף משימה זה!

מספר הקבוצה: _____

שם התלמיד: _____

שיטת ההצפנה: (3) צופן ערבול – על ידי היפוך סדר האותיות במסר

א. תיאור כללי של שיטת ההצפנה:

ב. מפתח ההצפנה : תלמידי כיתה ט' הלומדים במסגרת העתודה מדעית טכנולוגית.

ג. אלגוריתם ההצפנה : מעבדת מחשבים עם חיבור לאינטרנט.

ד. דוגמא להצפנה ופיענוח על פי השיטה והסבר :

ה. תרגילים לתרגול

עבודה נעימה!

דף משימה לתלמיד – תבנית חקר

הנחיות למילוי דף העבודה :
1. יש להגיש את דף העבודה לבדיקת המורה לפני מועד השיעור
2. עליך לדאוג שלכל חבר בקבוצתך יהיה עותק מדף משימה זה!

מספר הקבוצה: _____

שם התלמיד: _____

שיטת ההצפנה: (4) צופן "זיגזג"

א. תיאור כללי של שיטת ההצפנה:

ב. מפתח ההצפנה: תלמידי כיתה ט' הלומדים במסגרת העתודה מדעית טכנולוגית.

ג. אלגוריתם ההצפנה: מעבדת מחשבים עם חיבור לאינטרנט.

ד. דוגמא להצפנה ופיענוח על פי השיטה והסבר:

ה. תרגילים לתרגול

עבודה נעימה!

דף משימה לתלמיד – תבנית חקר

הנחיות למילוי דף העבודה :
1. יש להגיש את דף העבודה לבדיקת המורה לפני מועד השיעור
2. עליך לדאוג שלכל חבר בקבוצתך יהיה עותק מדף משימה זה!

מספר הקבוצה: _____

שם התלמיד: _____

שיטת ההצפנה: (5) צופן השביל המתפתל

א. תיאור כללי של שיטת ההצפנה:

ב. מפתח ההצפנה: תלמידי כיתה ט' הלומדים במסגרת העתודה מדעית טכנולוגית.

ג. אלגוריתם ההצפנה: מעבדת מחשבים עם חיבור לאינטרנט.

ד. דוגמא להצפנה ופיענוח על פי השיטה והסבר:

ה. תרגילים לתרגול

עבודה נעימה!