תכנית לימודים במודול

סייבר ואינטרנט

במקצוע מדעי המחשב, לחטיבת הביניים

בכל המגזרים

תכנית לימודים במקצוע מדעי המחשב

לחטיבת הביניים

מודול – סייבר ואינטרנט

מבוא

תכנית הלימודים במודול סייבר ואינטרנט באה לחשוף את התלמידים לתכנים המשמשים כבסיס לעולם הסייבר.

מודול זה מיועד לתלמידי חטיבות הביניים בכיתה ט', אשר למדו מבוא למדעי המחשב ויודעים לממש אלגוריתמים באמצעות פקודות בקרה כגון IF-THEN-ELSE, FOR, WHILE בכל שפת תכנות שהיא, למשל, Scratch.

מטרת המודול לפתח יכולות חקירה אצל התלמיד ולחשוף אותו לנושאים שונים במדעי המחשב תוך הצגת בעיות מהחיים.

התכנית תלמד כולה במעבדת מחשבים. הלימוד יתקיים תוך ביצוע משימות מובנות ומשימות התנסות חופשית בסביבה.

מסמך זה יפרט את תכנית הלימודים במודול סייבר ואינטרנט, שמטרתו לחשוף את התלמידים למרכיבי עולם הסייבר.

נושאי המודול וחלוקת השעות

פרק מס'	שם הפרק	שעות התנסות	שעות עיוניות	סה"כ שעות
1	מבוא למערכות ספרתיות (דיגיטליות) – ייצוג מידע	4	10	14
2	תקשורת נתונים	8	8	16
3	העברת מידע מוצפן ברשת	8	10	18
4	הגנת סייבר		8	8
	סה"כ:	**20**	**36**	**56**

פרק 1: מבוא למערכות ספרתיות – ייצוג מידע

<u>יעדים:</u> ייצוג נתונים במחשב: ייצוג מספרים, טקסט ותמונות.

<u>תכנים</u>

- ייצוג מספרים
  - ביט, בית, מילה
  - ייצוג מספרים בבסיס הבינארי
  - מעבר מבסיס בינארי לבסיס אוקטלי והקסה דצימלי.
- ייצוג טקסט
  - ייצוג אתיות באמצעות טבלת ASCII
- ייצוג תמונות
  - מה זה פיקסל
  - מה זה רזולוציה (הפרדה)
  - ייצוג ב- BMP וייצוג ב RLE (דחיסת מידע על קצה המזלג)
  - ייצוג תמונות צבעוניות RGB

<u>מטרות ביצועיות</u>[1]

- התלמיד יסביר כמות המידע הנשמרת בביט, בית, מילה, KB וכו'.
- התלמיד יכתוב טבלה להמרה בין בסיס 10 לבסיס 2 ולהפך.
- התלמיד ידע להמיר מבסיס בינארי לבסיס אוקטלי ולהפך כאשר טבלת ההמרה לפניו.
- התלמיד ידע להמיר מבסיס בינארי לבסיס הקסאדצימלי ולהפך כאשר טבלת ההמרה לפניו.
- התלמיד יסביר כיצד נשמר מידע טקסטואלי
- התלמיד יסביר כיצד נשמר מידע ויזואלי
- התלמיד יסביר מהו פיקסל ומהי רזולוציה

<u>דרכי הוראה</u>

פרק זה ברובו תיאורטי ונועד להפגיש את התלמיד עם המושגים הבסיסיים שמלווים את מערכות המחשוב אותן הוא פוגש בחיי היום יום.

ניתן להתחיל את הלימוד בהצגת תמונת זיכרון או מפרט של מחשב/טלפון נייד/מחשב לוח המוצע למכירה המדבר על מילה באורך 64 ביט או 32 ביט . הצורך בהבנת המושגים הבסיסים האלו הוא שינחה את מהלך השיעורים. יש להבהיר שכל מערכות המיחשוב הקיימות היום הינן למעשה מערכת אלקטרוניות ספרתיות.

[1] ככלל, הנושאים שמופיעים בסעיף "מטרות ביצועיות" מתארים שאלות אפשריות בבחינות.

לאחר הסבר ראשוני על מבנה הזיכרון יש להדגיש את הצורך בייצוג מידע. המחשב יודע לעבוד עם 0ים ו- 1ים בלבד. למזלנו, אפשר לייצג כל מידע שהוא באמצעות 0ים ו- 1ים וגם לבצע את כל החישובים שאנחנו יודעים לבצע, באמצעות 0ים ו- 1ים.

נתחיל בייצוג מספרים. נראה כיצד ניתן לייצג את המספרים 1..16 באמצעות 0ים ו- 1ים. התלמידים יעבדו עם טבלה. כיוון שלאנשים קשה לעבוד עם מספרים בינאריים אנו מתרגמים את המידע הבינארי למידע הקסאדצימלי (בסיס 16). יש ללמד מעבר בין בסיס בינארי לבסיס הקסאדצימלי ישיר, ללא ההסבר המתמטי המצדיק מעבר זה.

עתה משייצגנו מספרים יש להסביר את כמות המידע שניתן לאחסן בביט (יחידת המידע הקטנה ביותר), בית, מילה, KB (קילו = 1000) , GB, MB.

ייצוג מספרים מסביר לנו איך המחשב קולט נתונים ומעבד אותם. אבל איך הוא מציג את המידע? לשם כך יש להסביר מהו פיקסל, מהי הפרדה (רזולוציה), מה המשמעות של מצלמה בעלת הפרדה של x מגה פיקסל. הרעיון שתמונה מורכבת מפיקסלים אינה זרה לתלמידים. הם משתמשים באפליקציות עריכת תמונה לצורך הפרדת תמונות, הם רואים את הנקודות המרכיבות את התמונה הן בטלפון החכם והן על מסך הטלוויזיה.

<u>דרכי הערכה</u>[2]

דפי עבודה:

- התלמיד ייצור טבלת ערכים עבור מילה באורך 2, באורך 3 ויתאר את תחום המספרים העשרוניים שאפשר לייצג באמצעות מילה באורך זה.
- התלמיד יציג תמונה פשוטה מתוך הייצוג שלה ב BMP \ RLE

בחינה עיונית:

- התלמיד יקבל מחרוזת של ביטים ויחלקה לרביעות בייצוג הקסא דצימאלי.

<u>חלוקת שעות</u>

נושא	שעות
ייצוג מספרים	6
ייצוג טקסט	2
ייצוג תמונות	6
סה"כ שעות:	14

[2] ככלל, "דרכי הערכה" מתייחסות לפעולות פורמליות שהן מעבר להכנת שיעורי בית ובחנים תקופתיים

פרק 2: תקשורת נתונים

<u>יעדים:</u> הכרת מושגי יסוד בתקשורת נתונים, הכרת תהליך יצירת ההתחברות לרשת האינטרנט. הכרת הסימולטור- packet tracer

<u>תכנים</u>

מה זה תקשורת (מבוא קצרצר, לתאר במה עוסק התחום. הסעיף הבא מתייחס לתכנית הלימודים)

- רוצים להעביר 0 ו-1 ממקום למקום. איך עושים את זה במהירות וביעילות ?

מה מעניין אותנו:

- איך מנתבים את המידע? (מי ממיליוני המחשבים צריך לקבל אותו)
- איך מחלקים אותו ואיך אורזים אותו?
- איך יודעים שנפלו שגיאות ואיך מתקנים אותן?
- איך מאבטחים את המערכת – שלא יכנסו מזיקים (ילמד בפרק הגנת סייבר)
- איך מסתירים את המידע? (ילמד בפרק הצפנת)

פתרונות בנפנוף ידיים:

- פרוטוקול – מוסכמות. המחשבים ברשת יודעים איך מחלקים, איך אורזים, איך מנתבים, איך מתקנים שגיאות ואיך מסתירים מידע. כל מוסכמה כזו היא פרוטוקול.

העברת חבילת מידע מנקודה לנקודה. ההוראה תתבצע תוך הדגמה ב- packet tracer ותוך שימוש והכרת המושגים הבאים:

- IP address, MAC address
- DNS
- ראוטר (נתב), switch, Hub
- DHCP
- Default Gateway
- ping, tracert

<u>מטרות ביצועיות</u>

- התלמיד ידע להסביר איך מנתבים את המידע?
- התלמיד ידע להסביר מהו פרוטוקול
- התלמיד ידע על אפשריות המעקב אחר מידע ברשת
- התלמיד יתאר מעבר מידע באמצעות תוכנת PacketTracet מלקוח אל לקוח תוך מעבר ברשת פנימית:
  - hub , Switch

- התלמיד יתאר מעבר מידע באמצעות תוכנת PacketTracet מלקוח אל לקוח תוך מעבר ברשת פנימית לחיצונית:
  - Switch
  - נתב
- התלמיד יסביר תהליך שליחה וקבלה של הודעה.
- התלמיד יסביר מהי כתובת IP ומהי כתובת MAC
- התלמיד ידע להשתמש בהוראות: ipconfig \all, ping, tracert

<u>דרכי הוראה</u>

את רוב הלימודים לפרק זה ראוי לבצע במעבדה.

הוראת הפרק תתחיל בהסבר כללי מהי תקשורת, מה הנושאים בהם עוסקים בתקשורת ומה מתוכם מעניין אותנו (ניתוב מידע, חלוקת המידע, תיקון שגיאות, אבטחה והסתרה).

יש להציג מהו פרוטוקול באופן כללי כמוסכמה לשיחה. יש להציג פרוטוקולים פשוטים. רצוי לתת לתלמידים להתנסות בהפעלת פרוטוקולים כאשר התלמידים הם מחשבים המנסים לשלוח מידע על פי הפרוטוקול. ניתן לדון גם ביתרונות ובחסרונות של הפרוטוקול.

הדגמת שליחת הודעות תעשה תוך הדגמה ב- packet tracer.

תחילה המורה ידגים את הורדת התכנה מהאינטרנט, התקנתה והתלמידים יתנסו בתהליך זה. במידה ולא ניתן להתקין עם התלמידים ונדרשת התקנה לפני השעור, יש להסביר לתלמידים את תהליך ההתקנה, כך שיוכלו להתקין את התכנה בבית.

תוך מעבר על בניית רשת אינטרנט פשוטה ביותר, המורה יסביר את תפקידי כל אחד מהמרכיבים ברשת. נתינת כתובת IP. אין להיכנס ל- classes או לדרך בה נבנה המספר. יש להבהיר בנקודה זו את ההבדל בתפקידי כתובת IP ו-Port אצל הלקוח. ראוי להסביר זאת באמצעות פתיחת כמה דפדפנים שלכולם אותו מספר IP אך לכל אחד מהם מספר פורט שונה.

הנתב יקבל את תשומת הלב המקסימלית בתאור המעבר של הנתונים.

<u>דרכי הערכה</u>

דפי עבודה:

- מעקב אחר פרוטוקולים

בחינה במעבדה:

- התלמיד יבנה רשת פשוטה פנימית וחיצונית ויעביר חבילת מידע הלוך ושוב תוך תאור המרכיבים והתהליך.

חלוקת שעות

נושא	התנסות	עיונית	סה״כ שעות
מהי תקשורת		3	3
פרוטוקולים	1	1	2
התקנת התוכנה והסברים	1		1
מעבר מידע ברשת	2	2	4
נתבים ומפסקים	4	2	6
סה״כ שעות:	8	8	16

פרק 3: העברת מידע מוצפן ברשת

<u>יעדים</u>: הצורך בהעברת מידע מוצפן ושיטות להצפנה.

<u>תכנים</u>

- היסטוריה
  - למה צריך הצפנה
  - צופן אתב"ש , אלב"מ
  - צופן קיסר
  - צופן ערבול
  - צופן שיחלוף ללא חוקיות
- הצפנה סימטרית
  - חוזק ההצפנה
  - DES (רעיון בלבד)
  - שיטות לפיצוח
    - כח גס (Brute Force)
    - סטטיסטיקות לשוניות
  - פנקס חד פעמי One Time Pad
  - חסרונות ההצפנה הסימטרית:
    - בעיית הפצת המפתחות
    - החלפת המפתחות
- הצפנה א-סימטרית
  - פונקציה חד כיוונית
  - שיטת דיפי-הלמן להסכמה על מפתח סודי משותף
  - מפתח ציבורי \ פרטי (רעיון בלבד)

<u>מטרות ביצועיות</u>

- התלמיד יסביר מהו מידע מוצפן ומהו חוזק ההצפנה .
- התלמיד ייתן דוגמה מעשית לצורך בהצפנה
- התלמיד יתאר דוגמה של הצפנה סימטרית.
- התלמיד יכתב אלגוריתם מבוסס כח גס לפענוח מסר מוצפן בהצפנה סימטרית
- התלמיד יתאר דוגמה של הצפנה אסימטרית.

- התלמיד יצפין, יפענח וישבור צופן אתב"ש, צופן קיסר וצופן ערבול
- התלמיד ידע לתרגם אלגוריתם הצפנה לפסאודו קוד.
- התלמיד ידע להצפין לפי פסאודו קוד נתון.

<u>דרכי הוראה</u>

אפשר להתחיל את הפרק בסיפורים מההיסטוריה על השימוש בהצפנות. לדוגמה, סיפורה של מרי, מלכת הסקוטים אשר הוצאה להורג לאחר שהצופן בו השתמשה בהתכתבויות עם קבוצת אצילים שקשרו קשר נגד מלכת אנגליה, נפרץ.

את סוגי ההצפנות השונים אפשר ללמד באמצעות משחקים. יש להתחיל עם הצפנות סימטריות (בעלות מפתח אחד להצפנה ופיענוח) כדוגמת צופן קיסר, צופן החלפה וצופן ערבול. יש להכין מסרים מוצפנים, לחלק את הכיתה לקבוצות ולבקש שיפענחו את המסר.

את ההצפנות הסימטריות ניתן לתאר באמצעות פסאודו קוד ואם למדו javaScript אפשר לכתוב מימוש במחשב.

יש להשתמש בציון אלגוריתם DES ובפיצוחו על ידי אלגוריתם כוח גס, להסבר על מגבלות החישוב. כוח גס הוא אלגוריתם נאיבי המנסה את כל המפתחות האפשריים (למעשה מספיק מחצית המפתחות) עד לפיצוח הקוד. כיוון שמדובר במספרים מאד גדולים נדרשת סריקה של לפחות 2^{55} מפתחו בממוצע עד לפיצוח הקוד. עד 1998 נדרשה חומרה ייחודית ויקרה לצורך הפיצוח, שנמשך מספר ימים. ב- 2008 פורסם שרת שכל מטרתו הייתה לפצח DES וזה לקח לו פחות מיום. כיום משתמשים במעבדים 'מתנדבים' ברשת וניתן לפצח את הקוד במספר שעות. כלומר כח המחשוב מקטין את זמן הפיצוח, אבל ניתן להגדיל את אורך הקוד, ובמקום להתבסס למשל על מספרים בני 300 ספרות, להתבסס על מספרים בני 600 ספרות. דבר זה יגדיל מאד את זמן החישוב הנדרש ויעלה אותו שוב למספר שנים, דבר ההופך את הפענוח ללא רלוונטי.

לאחר דיון קצר בכשלים של צפנים סימטריים יש להציג את רעיון המפתח הציבורי. ההצפנה מבוססת על שתי פונקציות: פענוח והצפנה. לכל משתמש שני מפתחות: האחד ציבורי וגלוי לכולם והשני פרטי. הרעיון מבוסס על כך שהפעלת שני המפתחות בזה אחר זה על מחרוזת מחזיר את המחרוזת למקור, אך ידיעת המפתח הציבורי לבדו אינה מאפשרת גילוי המפתח הפרטי ולכן לא ניתן לפענח את המסר.

בהצגת רעיון ההצפנה הא-סימטרית המבוססת על רעיון המפתח הציבורי, יש להסביר ברמה מתמטית המתאימה לידע הקודם של התלמידים. התלמידים למדו חזקות ו- modulus ועל כן יכולים לחשב פענוח והצפנה של מסרים פשוטים עם מפתחות פשוטים. אם זאת אין להכנס להוכחת נכונות האלגוריתם.

האלגוריתם מתבסס על הרעיון הבא:

1. לכל משתתף יש מפתח ציבורי הגלוי לכולם ומפתח פרטי הנשמר בסוד.
2. אליס רוצה להעביר מידע חסוי לבוב
3. אליס כותבת את ההודעה, מניחה את ההודעה בקופסה ונועלת עם המפתח הציבורי של בוב.
4. בוב מקבל את הקופסה שנעולה במפתח הציבורי שלו. בוב פותח את הקופסה באמצעות המפתח הפרטי שלו (רק הוא יכול לפתוח)

5. בוב קורא הודעה שעליה כתוב: "אני אליס...."

את האלגוריתם הזה אפשר לשחק בכיתה עם מפתחות פשוטים ולהסביר כי האלגוריתם מתבסס על הקושי לפרק מספר לגורמים.

יש לציין שעד היום לא מצאו אלגוריתם יעיל לפירוק לגורמים וגם לא יודעים אם יש כזה או אין כזה. (רק אם התלמידים נמצאים ברמה המתמטית).

התלמידים למדו בכיתה ז' במתמטיקה פרק על מספרים ראשוניים, כולל בדיקה האם מספר הוא ראשוני על ידי בדיקה האם מתחלק לאחד המספרים בין 2 לשרש המספר.

<u>דרכי הערכה</u>

דפי עבודה:

- עבודה זוגית שבה תלמידים יפתחו תהליך הצפנה ופיענוח סימטריים (שפת הב', שפת ה ג' וכדומה)
- הצפנה \ פענוח עפ"י פסאודו קוד נתון
- תיאור תהליך הצפנה א-סימטרית (שבו חסר שלב שיש להשלים)

<u>מקורות</u>

- הצפנה סימטרית
  - http://meyda.education.gov.il/files/Tochniyot_Limudim/Math/Hatab/Hatzpana1.pdf
- הצפנה אסימטרית
  - http://meyda.education.gov.il/files/Tochniyot_Limudim/Math/Hatab/Hatzpana2.pdf

<u>חלוקת שעות</u>

נושא	התנסות	עיונית	סה"כ שעות
הצפנה סימטרית	4	6	10
הצפנה א-סימטרית	2	2	4
מימוש בפסאודו קוד או JS	4		4
סה"כ שעות:	10	8	18

פרק 4: הגנת סייבר

יעדים: הבנת האיומים ברשת, הצורך בסיסמאות חזקות, הכרת מושגי פריצה בסייבר והתנאים להתרחשות אירוע. הגברת המודעות לאפשרויות הגדרת הפרטיות ברשת. הגברת המודעות לחוסר האנונימיות בסביבת הסייבר ולאפשרויות המעקב אחר מעבר המידע ברשת

תכנים

- DoS/DdoS
- נוזקה (Malware)
- סוס טרויאני (Trojan Horse)
- תולעת מחשבים (Computer Worm)
- וירוס מחשבים (Computer Virus)
- Spyware
- אנונימיות ברשת – יש דבר כזה?
- פרטיות ברשת – יש דבר כזה?
- גניבת זהויות

מטרות ביצועיות

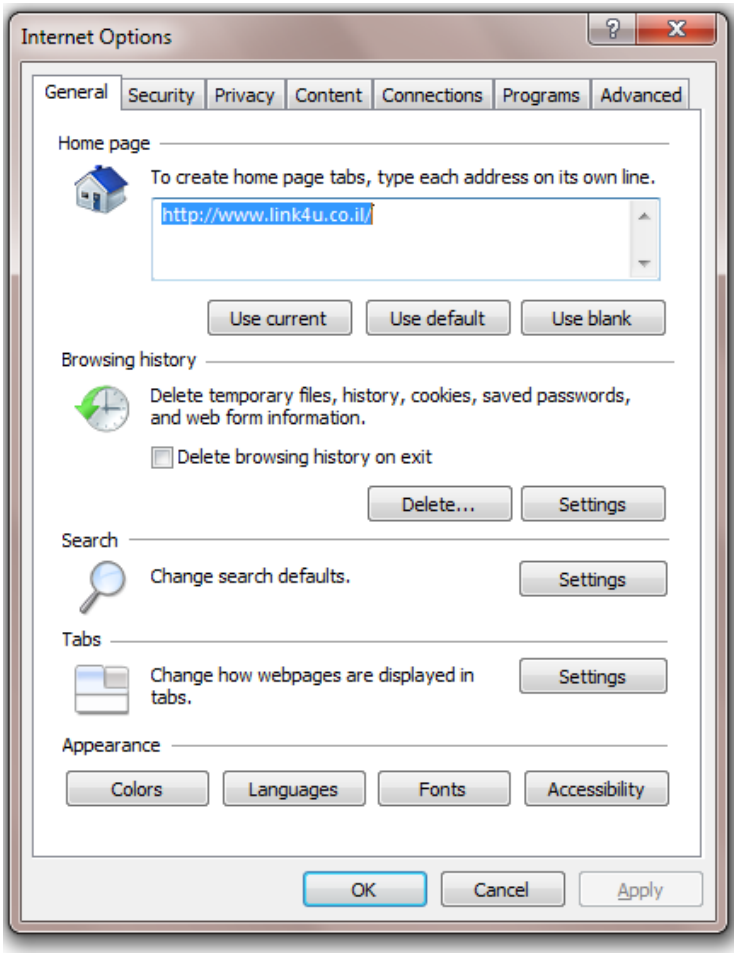
- התלמיד יהיה מודע לחוסר האנונימיות בסביבת הסייבר
- התלמיד ידע על אפשריות המעקב אחר מידע ברשת בדגש על חוסר אנונימיות
- יזהה מרכיבי חוסר פרטיות ברשת.
- התלמיד יתאר סיסמה חזקה והצורך בשמירת סיסמאותיו.
- התלמיד יתאר את ההבדלים בין סוגי התוכנות הגורמות לנזק/מעקב/ואיתור.

דרכי הוראה

התלמידים יכירו במחשב במעבדה ובמחשב בבית את ההגדרות של הרשת הפרטית והחיצונית ויגדירו בעצמם בהתאם למושגים בפני אילו בעיות של פרטיות הם עומדים. ניתן להדגים את המידע הניתן ברשת באמצעות הרשתות החברתיות והיכולת לגנוב זהויות כאשר הסיסמאות חלשות.

רצוי לשחק "21 שאלות" במטרה לגלות סיסמה. לאחר מספר סיבובים התלמידים יגלו כי רצוי לבחור בסיסמה שאינה מקושרת ישירות אליהם.

יש להראות לתלמידים את אפשרויות ההגנה האלו:



להסביר את המושגים ולאפשר לתלמידים לתכנן את שמירת פרטיותם ברשת.

במידה ונשאר זמן בסוף השנה, יש לתת לתלמידים לבחור אירוע סייבר, לנתח אותו ולהציג בכיתה. בניתוח האירוע יכללו: התוקפים, מטרת התקיפה, השפעות התקיפה, דרך התקיפה ודרך ההגנה.