תכנית לימודים במדעי המחשב

פרק בחירה ביחידה חמישית
אלגוריתמים

לחטיבה העליונה

בכל המגזרים

חברי הצוות שהכינו את התכנית לאישור ועדת המקצוע:

ד״ר ראובן חוטובלי (פיתח את הפרקים 1-8)

פרופ׳ מיכל ארמוני (פיתחה את הפרקים 1-8)

פרופ׳ שלומי דולב (פיתח את הפרקים 9-11)

מר גל בר-און (פיתח את הפרקים 1-11)

אלגוריתמים – פרק בחירה בתכנית הלימודים במדעי המחשב לתיכון

תכנית הלימודים במדעי המחשב נועדה לחשוף את התלמידים ליסודות הדיסציפלינה ולעקרונותיה (Gal-Ezer, Beeri, Harel, and Yehudai, 1995), תוך שילוב מתמיד בהתנסות ויישום. התלמידים מכירים את התהליך של פתרון בעיות אלגוריתמיות, החל מניתוח בעיה, דרך מציאת פתרון אלגוריתמי עבורה ועד מימוש הפתרון בשפת תכנות. שני פרקי החובה הראשונים ("יסודות מדעי המחשב") עורכים לתלמיד היכרות עם מושגים אלגוריתמיים בסיסיים, פיתוח אלגוריתמים ויישומם ע"י תכנות. פרק החובה השלישי עוסק במושגים מתקדמים יותר ובפרט מעמיק במבני נתונים. גם במהלכו פותרים התלמידים בעיות אלגוריתמיות ומיישמים אותם ע"י תכנות. הפתרונות הם מורכבים יותר ונעזרים במבני נתונים מסוגים שונים. כבר תוך כדי פרקי החובה נחשפים התלמידים לבעיות אלגוריתמיות יסודיות (כגון מיון וחיפוש) ואלגוריתמים קלאסיים עבורם. פרק הבחירה "אלגוריתמים" מתמקד בחלקו הראשון של תהליך פתרון בעיות אלגוריתמיות – ניתוח בעיה נתונה ותכנון פתרון אלגוריתמי עבורה. לצורך כך התלמידים לומדים אלגוריתמים קלאסיים מורכבים יותר מאשר אלו שפגשו בפרקי החובה, את עקרונותיהם והרעיונות הגלומים בהם. מאחר שהמיקוד הוא בתכנון אלגוריתמים תהליך הלימוד של פרק זה אינו כולל יישום (תכנות). הפרק הזה יחד עם פרק הבחירה המקביל לו ("מודלים חישוביים") מהווים את הפן התיאורטי בתכנית הלימודים, כפי שהומלץ ע"י הוגיה, ועורכים לתלמידים היכרות עם העשייה התיאורטית במדעי המחשב ומאפייניה.

קווים מנחים:

1. ההוראה הינה מבוססת בעיות (problem-based). כלומר, כל מושג ובפרט כל אלגוריתם נלמד בהקשר, תוך כדי פתרון בעיה אלגוריתמית אליה הוא רלבנטי. אם כך, הגישה משלבת שלוש גישות הוראה – למידה מבוססת בעיות, למידה ע"י עשייה ולמידה בהקשר, כל אחת מהן ידועה כמקדמת למידה משמעותית. יתרה מזאת, הוראה משקפת עיסוק אותנטי במדעי המחשב, כתחום העוסק בפתרון בעיות אלגוריתמיות. אם כך, כל פרק פותח בבעיה בסיסית שסביבה נבנה הפרק. התכנית שלהלן כוללת הצעה לבעיה כזאת בכל פרק אך ניתן כמובן להשתמש בבעיות מתאימות אחרות, לפי בחירתם וכיד דמיונם של המורים.
2. בהתאם לכך, התלמידים לא רק משתמשים באלגוריתמים נתונים, אלא גם מפתחים אלגוריתמים על בסיס האלגוריתמים הנלמדים. לכן, בכל פרק חשוב לתת בעיות נוספות שלצורך פתרונן ייעשה שימוש באלגוריתמים שנלמדו בו – כלשונם (כלומר, כקופסאות שחורות) או ע"י הכנסת שינויים והתאמות באלגוריתמים שנלמדו.
3. חלקים בלתי נפרדים מפתרון בעיה אלגוריתמית הם הוכחת נכונות הפתרון וניתוח הסיבוכיות. התלמידים ינתחו את סיבוכיות הפתרונות שלהם אך לא תמיד יידרשו לתת הוכחה מלאה לנכונותם משום שבמקרים רבים ההוכחות מורכבות ומחייבות כלים שאינם מוכרים לתלמידים (כמו אינדוקציה מבנית). לכן, כדאי לנצל הזדמנויות בהן הוכחת הנכונות מתאימה לרמת הקושי של התכנית כדי להדגים הוכחת נכונות מלאה.
4. בנוסף להיכרות עם אלגוריתמים חשובים התלמידים יכירו אסטרטגיות אלגוריתמיות שונות (רדוקציה, אסטרטגיה חמדנית, תכנון דינמי). גם אלו יילמדו בהקשר ותמיד לצורך פתרון בעיה עבורה הן רלבנטיות.

5. החוט המקשר בין האלגוריתמים המוצגים בקורס הוא נתונים – ייצוג, קידוד והצפנה. בהתאם לכך התלמידים יעסקו בחלקו הראשון של הפרק בבעיות שניתן לייצג אותן ואת מרחב הנתונים שלהן ע״י גרפים, לאחר מכן יעסקו באלגוריתם לקידוד נתונים ולבסוף באלגוריתמים העוסקים בהצפנת נתונים.
6. לאורך חומר הלימוד יש רעיונות חוזרים, שמופיעים בהקשרים שונים ובצורות שונות. חשוב מאוד ליצור קשר מפורש בין ההופעות השונות של אותו רעיון. בכל פעם שהוא מופיע שוב להתייחס לכך במפורש ולהזכיר את משמעותו. למשל – הרעיון של הפשטה (אבסטרקציה) של נתונים או הרעיון של אסטרטגיה אלגוריתמית לפתרון בעיות. ההתייחסות המפורשת לרעיון ולמופעיו השונים תאפשר הפנמה משמעותית של הרעיון והכללה שלו וכתוצאה מכך שימוש בו גם בהקשרים שונים מאלו המפורשים בחומר הלימוד.
7. כדאי לשלב בעיות מעניינות ורלבנטיות לתלמידים, מתחומים שונים.

חלוקת השעות

פרק	הנושא	שעות התנסות	שעות עיוניות	סה״כ שעות
1	היכרות עם גרפים	1	2	3
2	ייצוג של גרפים	1	3	4
3	מסלולים קצרים ביותר ממקור יחיד	2	6	8
4	מסלולים קצרים ביותר בגרף עם משקלות אי-שליליים	2	6	8
5	סריקה לעומק	3	6	9
6	מיון טופולוגי	1	2	3
7	עץ פורש מינימלי	2	4	6
8	קידוד ודחיסת נתונים	2	4	6
9	**הצפנה עם מפתח סימטרי**	4	9	13
10	מערכת הצפנה עם מפתח אסימטרי	6	10	16
11	בניית אמון באמצעות מפתח פומבי (PKI) וחתימה דיגיטלית	2	5	7
	בחנים ומבחנים	4	3	7
	סה״כ שעות	30	60	90

פרק 1: היכרות עם גרפים (3 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות במילים שלו מהו גרף מכוון , לא מכוון וממושקל.
2. התלמיד יסביר מהם: דרגת כניסה, דרגת יציאה, דרגה, מסלול ומעגל.
3. התלמיד יסביר וייתן דוגמה אחת לפחות את המושגים האלה: בעבור גרף לא מכוון- רכיב קשיר ; גרף קשיר ובעבור גרף מכוון- ומהו רק"ח ; גרף קשיר היטב.
4. התלמיד יסביר וייתן דוגמה אחת לפחות מהו גרף שלם, גרף דו צדדי ותת גרף.
5. התלמיד יסביר וייתן דוגמה אחת לפחות מהו הקשר בין סכום הדרגות של קדקודי הגרף לבין מספר הקשתות בגרף.
6. התלמיד יסביר וייתן דוגמה אחת לפחות מהם התנאים על מנת שגרף יהיה עץ.

<u>בעיה בסיסית</u>: את מבנה הנתונים המופשט של גרף ומושגים בסיסיים הקשורים אליו ניתן להציג בעזרת בעיה של אנשים המגיעים למסיבה ולוחצים זה את ידו של זה ויש לחשב את מספר לחיצות הידיים בתנאים שונים של הבעיה.

הבעיה הבסיסית הזאת מאפשרת להגדיר את המושגים הבסיסיים של **צמתים** (אנשים), **קשתות** (לחיצות ידיים) **ודרגה של צומת** (מספר הידיים שלחץ אדם). בעזרת וריאציות על הבעיה הראשונית אפשר להגדיר מושגים נוספים (גרף מכוון ולא מכוון, גרף שלם וגרף לא שלם).

<u>בעיה בסיסית נוספת</u>: בעיית הגשרים של אוילר (Euler) והווריאציה שלה כציור שניתן לצייר ביד אחת בלי להרים את העט מהדף.

בעיה זאת יכולה לשמש כדי להדגים את המושגים של מסלול, מסלול פשוט, מסלול מעגלי ומסלול מעגלי פשוט.

נקודות חשובות להוראה ודיון:

- הבעיה הראשונה היא בעיית חישוב מתמטית ולא בעיה אלגוריתמית, אבל היא נותנת הקשר להיכרות עם המושגים הבסיסיים של גרף.
- הבעיה השנייה היא בעיה אלגוריתמית. מאחר שאינה פשוטה מתאים לפתור אותה במליאה, כלומר, תוך כדי דיון שבו בשלב ראשון תובן הבעיה ואז יפותח אלגוריתם (בכתיבה כללית).

מושגים: גרף, צמתים, קשתות, גרף מכוון, גרף לא מכוון, דרגה של צומת, גרף מלא. מסלול. מסלול מעגלי.

פרק 2: ייצוג של גרפים (4 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות לפעולות הבסיסיות על גרף (הוספת קשת, הוספת קשת משוקללת, הסרת קשת, הסרת קשת משוקללת, בדיקת קיום של קשת, יצירת גרף ריק, הוספת קדקוד, הסרת קדקוד).
2. התלמיד יסביר וייתן דוגמה אחת לפחות לייצוג של גרף באמצעות מטריצה ריבועית.
3. התלמיד יסביר וייתן דוגמה אחת לפחות לייצוג של גרף באמצעות רשימות שכנות.
4. התלמיד יפתח פתרון אלגוריתמי מילולי למימוש הפעולות הבאות לידי ביטוי בסעיף 1, כאשר גרף מיוצג באמצעות מטריצה ריבועית ויחשב את סיבוכיות זמני הריצה שלהן.
5. התלמיד יפתח פתרון אלגוריתמי למימוש הפעולות הבאות לידי ביטוי בסעיף 1, כאשר גרף מיוצג באמצעות רשימות שכנות ויחשב את סיבוכיות זמני הריצה שלהן.
6. התלמיד יפתח בגישה מודולרית פתרונות אלגוריתמיים המשתמשים בייצוגים שונים של גרף
7. התלמיד יפתח פתרונות אלגוריתמיים בעבור הבעיות שלהלן:
   חישוב דרגת כניסה, דרגת יציאה, דרגה של קדקודי הגרף, כאשר משתמשים בייצוגים שונים של גרף ויחשב את סיבוכיות זמני הריצה שלהן.
8. התלמיד יסביר וייתן דוגמה אחת לפחות מהו גרף הפוך ויפתח פתרון אלגוריתמי ליצירת גרף הפוך כאשר משתמשים בייצוגים שונים של גרף ויחשב את סיבוכיות זמני הריצה שלהן.
9. התלמיד ייצור ויסביר מעקב אחר ביצוע אלגוריתמים נתונים הכוללים שימוש בייצוגים שונים של גרף.

<u>בעיה בסיסית</u>: בעיית הגשרים של אוילר שהוצגה בפרק הקודם.

דרך הבעיה של מציאת מסלול אוילר ניתן להבהיר את המשמעות של גרף כמבנה נתונים מופשט ופעולות נדרשות עליו (למשל, מהי רשימת הקשתות של צומת מסוים? מה הדרגה של צומת?), לדון בדרכים לייצוג גרף (עבור בעיית מסלול אוילר עולה באופן טבעי המבנה של **רשימת סמיכויות**) וייצוג מסלול, ובהתאם לכך לנתח את הסיבוכיות של הפתרון.

<u>בעיה בסיסית נוספת</u>: מבט חוזר על בעיות לחיצות הידיים השונות יכול להוביל למבנה של **מטריצת סמיכויות**.

נקודות חשובות להוראה ודיון:

- הנושא מאפשר לחדד את העקרונות של מבנה נתונים מופשט. הפעולות הנדרשות הן זהות אך בכל ייצוג הן ממומשות בצורה אחרת ובסיבוכיות שונה.
- הנושא מאפשר לחזור ולחדד את רמות ההפשטה של ייצוג נתונים. גרף הוא מבנה נתונים מופשט שיכול בתורו להיות ממומש על ידי רשימה מקושרת של רשימות מקושרות, כלומר דרך מבנה נתונים מופשט אחר.
- מפרק זה ואילך עבור כל אלגוריתם שיילמד יש להתייחס לניתוח הסיבוכיות שלו, גם אם זה לא נאמר במפורש בתכנית.

מושגים: רשימת סמיכויות. מטריצת סמיכויות.

פרק 3: מסלולים קצרים ביותר ממקור יחיד (8 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות מהו **אורך** מסלול ומהו מסלול קצר ביותר.
2. התלמיד יסביר וייתן דוגמה אחת לפחות לאופן מציאת המסלול הקצר ביותר באמצעות האלגוריתם BFS .
3. התלמיד יסביר וייתן דוגמה אחת לפחות לסיבוכיות זמן הריצה של BFS כאשר גרף מיוצג באמצעות רשימות שכנות.
4. התלמיד יסביר וייתן דוגמה אחת לפחות לעץ פורש BFS .
5. התלמיד יסביר וייתן דוגמה אחת לפחות כיצד לקבוע אם בגרף נתון קיים מעגל.
6. התלמיד יסביר וייתן דוגמה אחת לפחות כיצד לקבוע אם גרף נתון לא מכוון הוא גרף קשיר או לא קשיר.
7. התלמיד יתכנן וירשום אלגוריתם הפותר בעיה נתונה תוך שימוש ב- BFS כקופסה שחורה.
8. התלמיד ישתמש בטיפוסי נתונים מופשטים (מחסנית / תור / רשימה) הנלמדים במבנה נתונים לצורך פתרון בעיות הקשורות לסריקה לרוחב בגרפים .
9. התלמיד יסביר וייתן דוגמה אחת לפחות מדוע אלגוריתם מסוים הוא נכון.
10. התלמיד יסביר וייתן דוגמה אחת לפחות מהי רדוקציה.
11. התלמיד יפתור בעיה תוך שימוש ב **רדוקציה** ושימוש ב- BFS למציאת מסלולים קצרים ממקור יחיד כקופסה שחורה.

<u>בעיה בסיסית</u>: חקלאי בעל כמה מטעי תפוחים פזורים בשטחים סביבו ודרכים חקלאיות המחברות בין המטעים. החקלאי רוצה לסמן לעצמו עבור כל אחד מהמטעים שברשותו באיזו דרך יוכל להגיע אל המטע כך שיעבור דרך כמה שפחות מטעים בדרכו אל המטע.

פתרון לבעיה הוא האלגוריתם של חיפוש לרוחב (BFS).

האסטרטגיה האלגוריתמית של **רדוקציה** תעלה באופן טבעי בפרק ע"י הצגת בעיות שאפשר לפתור אותן ע"י שימוש במציאת מסלולים קצרים ממקור יחיד כקופסה שחורה. למשל – אצל חקלאי אחר יש הבדלים משמעותיים במרחקים בין המטעים. חלק מהמטעים קרובים יחסית זה לזה, כחצי ק"מ, אך יש מטעים שהמרחק ביניהם כפול מזה, כק"מ. כיצד ימצא החקלאי עבור כל מטע מהי הדרך הקצרה ביותר שמגיעה אל המטע?

נקודות חשובות להוראה ודיון:

- המקרה הפשוט של צומת יעד מסוים יחיד.

- מימוש BFS בעזרת תור (כמבנה נתונים מופשט). זאת דוגמה נוספת למבנה בתוך מבנה.
- המשמעות של BFS כאלגוריתם ל**סריקת גרף** תוך קישור לבעיות סריקה שכבר הכירו בפרקים הקודמים בתכנית הלימודים – סריקת רשימה וסריקת עץ. לדון במטרות של סריקה – לצורך חיפוש איבר, לצורך חישוב מרחקים. אפיון הסריקה כסריקה לרוחב.
- אלגוריתם הסריקה יוצר **עץ פורש** מכוון (קישור למבנה הנתונים של עץ שהכירו ביחידה העוסקת במבני נתונים).
- BFS בגרף מכוון – את המקרה המכוון ניתן להציג דרך בעיה דומה שבה יש דרכים דו-סטריות וחד-סטריות. גם זה פתרון ע״י רדוקציה – רדוקציה לבעיה הבסיסית של BFS בגרף לא מכוון.
- וריאציה על הבעיה המקורית יכולה להוביל להגדרת **קשירות** ושימוש ב-BFS לבדוק קשירות של גרף. למשל: בעונת הגשמים ייתכן שחלק מהדרכים המקשרות בין מטעים חסומות עקב הצפה ויש למצוא כעת את הדרך הקצרה ביותר לכל מטע. האם עדיין אפשר להגיע לכל מטע?
- בנוסף לחשיבות של חשיפה ראשונה לרדוקציה כאל אסטרטגיה אלגוריתמית, אלגוריתמים שמבוססים על רדוקציה מאפשרים להתנסות בהוכחת נכונות של אלגוריתמים כי אלו הוכחות נכונות פשוטות יחסית שמניחות את נכונות האלגוריתם הבסיסי.

מושגים: אורך מסלול, מסלול קצר ביותר, BFS, עץ, עץ פורש של גרף. קשירות של גרף.

אסטרטגיות אלגוריתמיות: רדוקציה

פרק 4: מסלולים קצרים ביותר בגרף עם משקלות אי-שליליים (8 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות ל**משקל** מסלול ומהו מסלול קצר ביותר במשקל.
2. התלמיד יסביר וייתן דוגמה אחת לפחות לאופן מציאת המסלול הקצר ביותר במשקל באמצעות האלגוריתם של דייקסטרה (Dijkstra).
3. התלמיד יסביר וייתן דוגמה אחת לפחות לסיבוכיות זמן הריצה של אלגוריתם דייקסטרה (Dijkstra). כאשר גרף מיוצג באמצעות מטריצת שכנות.
4. התלמיד יסביר וייתן דוגמה אחת לפחות לעץ מסלולים קצרים במשקל.
5. התלמיד יסביר וייתן דוגמה אחת לפחות באיזה מקרה לא ניתן להשתמש באלגוריתם של דייקסטרה .
6. התלמיד יסביר וייתן דוגמה אחת לפחות מהו תור העדיפויות, באיזה אופן משתמש האלגוריתם של דייקסטרה בתור העדיפויות ולמה הכרחי שזה יהיה תור עדיפויות ולא תור רגיל.
7. התלמיד יסביר וייתן דוגמה אחת לפחות לגישה חמדנית ואיך הגישה הזו באה לידי ביטוי באלגוריתם של דייקסטרה.
8. התלמיד יסביר וייתן דוגמה אחת לפחות מהי אסטרטגיית תכנות דינמי ואיך האסטרטגיה הזו באה לידי ביטוי באלגוריתם של דייקסטרה.
9. התלמיד יתכנן אלגוריתם הפותר בעיה נתונה תוך שימוש באלגוריתם של דייקסטרה כקופסה שחורה.
10. התלמיד יסביר וייתן דוגמה אחת לפחות מדוע אלגוריתם מסוים הוא נכון.
11. התלמיד יפתור בעיה תוך שימוש ב **רדוקציה** ושימוש באלגוריתם של דייקסטרה כקופסה שחורה.

<u>בעיה בסיסית</u>: נהג משווק סחורה לכמה חנויות צעצועים שמפוזרות בעיר. יש כבישים באורכים שונים שמחברים בין חנויות. הנהג רוצה למצוא עבור כל חנות מהי הדרך הקצרה להגיע אליה.

פתרון לבעיה הוא האלגוריתם של דייקסטרה (Dijkstra).

זאת הרחבה טבעית של הבעיה שהייתה במרכז הפרק הקודם. במקום מטעים שמפוזרים על שטח קטן יחסית יש חנויות צעצועים במרחקים שונים משמעותית זו מזו. כעת יש חשיבות למרחקים בין החנויות. פחות חשוב דרך כמה חנויות הנהג עובר בדרכן לכל חנות, וחשוב יותר מה אורך הדרך שעליו לנסוע עד הגיעו לכל חנות.

האלגוריתם של דייקסטרה נשען על שתי אסטרטגיות אלגוריתמיות ומאפשר היכרות ראשונה עם שתיהן – הוא **חמדני** (בכל שלב נבחר הצומת שקרוב יותר לצומת המקור) ובנוסף, המסלול הקצר ביותר לכל צומת נבחר ע״י פתרון של תתי-בעיות, חישוב תתי-מסלולים בדרך ושימוש בתתי המסלולים הקצרים יותר, כלומר יש כאן שימוש באסטרטגיה של **תכנות דינמי**.

נקודות חשובות להוראה ולדיון:

- זאת דוגמה שמראה היטב כיצד שינוי קל בתנאי בעיה (אורכים לקשתות) יכול להקשות אותה משמעותית. התנסות בכיתה יכולה להוביל למסקנה ש-BFS כבר אינו מתאים ויש צורך באלגוריתם אחר.
- כבר בפרק הקודם הודגם שימוש במבנה נתונים מופשט פנימי (תור) בתוך האלגוריתם. האלגוריתם של דייקסטרה משתמש גם הוא במבנה נתונים מופשט פנימי, אך מורכב יותר – תור עדיפויות. במה תור עדיפויות דומה לתור רגיל ובמה הוא שונה ממנו? באיזה אופן משתמש האלגוריתם של דייקסטרה בתור העדיפויות ולמה הכרחי שזה יהיה תור עדיפויות ולא תור רגיל?
- בניתוח הסיבוכיות של האלגוריתם של דייקסטרה יש חשיבות רבה לתור העדיפויות ולסיבוכיות הפעולות הנעשות עליו. כיצד תלויה סיבוכיות האלגוריתם בסיבוכיות הפעולות השונות? אפשר לדון בדרכים שונות למימוש תור עדיפויות (למשל, בעזרת רשימה מקושרת) ולסיבוכיות המתקבלת בעזרתן. אבל, מאחר שהדרכים היעילות יותר למימוש תור עדיפויות (ערימה בינארית וערימת פיבונאצ'י) הן מעבר לחומר הלימוד, זאת הזדמנות טובה לחזור ולדון במבנה נתונים מופשט כקופסה שחורה. לצורך ניתוח סיבוכיות האלגוריתם של דייקסטרה מספיק לדעת שקיימת דרך יעילה לממש תור עדיפויות כך שהפעולות שנדרשות באלגוריתם של דייקסטרה יעבדו בסיבוכיות שמוצהרת ע"י הממשק של המבנה.
- מגבלות האלגוריתם: בדומה למעבר מגרף חסר משקלות לגרף עם משקלות אי-שליליים, שינוי נוסף בתנאי הבעיה (אפשרות למשקלות שליליים) ייצור בעיה קשה יותר שלא נפתרת ע"י האלגוריתם של דייקסטרה.
- למעשה, האסטרטגיה החמדנית היא זאת שמכשילה את האלגוריתם של דייקסטרה כשייתכנו משקלות שליליים, והדגמה של זה מסייעת להבהיר את אופיה של האסטרטגיה החמדנית שאינה מסתכלת קדימה ומתי ראייה מוגבלת כזאת אינה מתאימה.
- דיון כללי באסטרטגיות אלגוריתמיות – בשלב הזה התלמידים הכירו כבר שלוש אסטרטגיות אלגוריתמיות חדשות. זה הזמן למבט אחורה, על יחידות קודמות. האם הכירו אסטרטגיות נוספות בפרקים קודמים של תכנית הלימודים, גם אם לא קראו להן כך במפורש? זה המקום להזכיר את האסטרטגיה של "הפרד ומשול" שבאה לידי ביטוי בחיפוש בינארי ובמיון מיזוג.

מושגים: משקלות לקשתות. האלגוריתם של דייקסטרה.

אסטרטגיות אלגוריתמיות: אלגוריתם חמדני, תכנות דינמי.

פרק 5: סריקה לעומק (9 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות לסריקה לעומק תוך שימוש באלגוריתם של DFS .
2. התלמיד יסביר וייתן דוגמה אחת לפחות לסיבוכיות זמן הריצה של האלגוריתם DFS כאשר גרף מיוצג באמצעות מטריצת שכנות.
3. התלמיד יסביר וייתן דוגמה אחת לפחות לעץ פורש DFS .
4. התלמיד יסביר וייתן דוגמה אחת לפחות לכיצד אפשר לאפיין את קשתות הגרף (מכוון/ לא מכוון) ביחס לקשתות העץ הפורש .
5. התלמיד יסביר וייתן דוגמה אחת לפחות לכיצד לקבוע אם בגרף נתון קיים מעגל.
6. התלמיד יסביר וייתן דוגמה אחת לפחות לכיצד לקבוע אם גרף נתון לא מכוון קשיר או לא קשיר.
7. התלמיד יתכנן אלגוריתם הפותר בעיה נתונה תוך שימוש ב- DFS כקופסה שחורה.
8. התלמיד ישתמש בטיפוסי נתונים מופשטים (מחסנית / תור / רשימה) הנלמדים במבנה נתונים לצורך פתרון בעיות הקשורות לסריקה לעומק בגרפים .
9. התלמיד יסביר וייתן דוגמה אחת לפחות מדוע אלגוריתם מסוים הוא נכון.
10. התלמיד יפתור בעיה תוך שימוש ב**רדוקציה** ושימוש ב- DFS כקופסה שחורה.
11. התלמיד יסביר וייתן דוגמה אחת לפחות לכיצד ניתן למצוא רכיבי קשירות חזקה **(רק"חים)** תוך שימוש ב- DFS כקופסה שחורה.
12. התלמיד יסביר וייתן דוגמה אחת לפחות ל**גרף על** וכיצד ניתן למצוא גרף על) תוך שימוש ברכיבי קשירות חזקה (רק"חים).

<u>בעיה בסיסית</u>: יציאה ממבוך. את המבוך אפשר לייצג ע"י גרף – הצטלבויות ושבילים שעוברים ביניהן. יש הצטלבויות שיוצאים מהן שבילים רבים, ויש שבילים ללא מוצא, שאם מגיעים לקצותיהם צריך להסתובב אחורה ולחזור להצטלבות האחרונה שיצאנו ממנה, והליכה לא זהירה עלולה להוביל לסיבוב חסר תוחלת במעגל ולאי-יציאה מהמבוך.

הפתרון – עיקרון היד הימנית. התרגום של העיקרון לאלגוריתם חד-משמעי ולייצוג של מבוך ע"י גרף מוביל לאלגוריתם של חיפוש לעומק (DFS).

נקודות חשובות להוראה ולדיון:

- זאת דוגמה לכך שאפשר למצוא פתרון (עיקרון היד הימנית) בעולם הבעיה, לפני שנעשה מידול לעולם של מדעי המחשב. המידול לבעיה אלגוריתמית בתורת הגרפים מאפשר להגיע לניסוח מדויק של הפתרון כולל ניתוח סיבוכיות.
- סריקה לעומק (DFS) מול סריקה לרוחב (BFS).

- סריקה לעומק בגרף לא קשיר.
- מדוע רקורסיה היא טבעית עבור סריקה לעומק?
- העץ הפורש שנוצר בסריקה לעומק, בהשוואה לעץ הפורש שנוצר בסריקה לרוחב.
  כיצד אפשר לאפיין את קשתות הגרף (מכוון/ לא מכוון) ביחס לקשתות העץ הפורש?
- כיצד אפשר למצוא רכיבי קשירות חזקה (רק״חים) תוך שימוש ב- DFS ובגרף הפוך ומהם למצוא את גרף על.

מושגים: DFS.

פרק 6: מיון טופולוגי (3 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות למיון טופולוגי וכיצד ניתן להשיג מיון כזה תוך שימוש באלגוריתם DFS .
2. התלמיד ישתמש באחד מפתרונותיו לפחות בטיפוסי נתונים מופשטים (מחסנית / תור / רשימה) הנלמדים במבנה נתונים לצורך מיון טופולוגי.
3. התלמיד יסביר וייתן דוגמה אחת לפחות לסיבוכיות זמן הריצה של אלגוריתם מיון טופולוגי כאשר גרף מיוצג באמצעות מטריצת שכנות.
4. התלמיד יסביר וייתן דוגמה אחת לפחות איך ניתן לקבוע אם בגרף נתון קיים מעגל תוך שימוש במיון טופולוגי.
5. התלמיד יסביר וייתן דוגמאות על אילו גרפים ניתן להפעיל את האלגוריתם- מיון טופולוגי.
6. התלמיד יתכנן וירשום אלגוריתם הפותר בעיה נתונה תוך שימוש במיון טופולוגי כקופסה שחורה.
7. התלמיד יסביר וייתן דוגמה אחת לפחות כיצד אלגוריתם נתון המשתמש במיון טופולוגי כקופסה שחורה.

<u>בעיה בסיסית</u>: ההורים נסעו לשבוע, וכל מטלות הבית הן באחריותכם. ויש הרבה... אתם מכינים רשימה של כל המטלות שעליכם לבצע. למשל – להשקות את העציצים, לעשות קניות, לטייל עם הכלב, לבשל, לכבס, לשאוב אבק, לקפל כביסה, לשטוף את הרצפה, לאסוף את כל הבגדים המלוכלכים שזרוקים על הרצפה בחדר שלכם, ועוד כמה וכמה.

אחרי שהכנתם את הרשימה אתם רוצים לארגן סדר משימות שתפעלו לפיו. יש מטלות שהסדר ביניהן לא חשוב. למשל, לא משנה אם קודם תכבסו או קודם תשטפו את הרצפה. אבל במקרים רבים הסדר חשוב מאוד. למשל – את הבגדים המלוכלכים צריך לאסוף מהרצפה לפני ששוטפים אותה וגם לפני שמכבסים. קודם צריך לכבס ורק אחר כך לקפל כביסה. קודם צריך לעשות קניות ורק אחר כך לבשל. קביעת סדר המטלות הכללי צריכה להתחשב באילוצי הסדר האלו.

זאת בעיית מיון טופולוגי ואפשר לפתור אותה ע״י אלגוריתם למיון טופולוגי שמבוסס על DFS.

נקודות חשובות להוראה ולדיון:

- האם תמיד ניתן לבצע מיון טופולוגי (מה קורה בגרף שמכיל מעגל?)?
- הישענות על אלגוריתם קיים (DFS לגרף מכוון) כדי לפתור בעיה שונה.

מושגים: מיון טופולוגי.

פרק 7: עץ פורש מינימלי (6 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות לעץ פורש מינימלי.
2. התלמיד יסביר וייתן דוגמה אחת לפחות עבור האסטרטגיה של האלגוריתם של קרוסקל (Kruskal).
3. התלמיד יסביר וייתן דוגמה אחת לפחות לסיבוכיות זמן הריצה של האלגוריתם של קרוסקל.
   בניתוח הסיבוכיות של האלגוריתם של קרוסקל יש חשיבות שהתלמיד יידע להסביר כיצד תלויה סיבוכיות האלגוריתם בסיבוכיות הפעולות השונות?
   מאחר שהדרכים היעילות יותר למימוש הפעולות האלו הן מעבר לחומר הלימוד התלמיד יידע להסביר שניתן להשיג סיבוכיות הטובה ביותר בעבור האלגוריתם קרוסקל תוך שימוש במבנה נתונים מופשט כקופסה שחורה.
4. התלמיד יסביר וייתן דוגמה אחת לפחות להבדל בין עץ פורש מינימלי לבין עץ המסלולים הקצרים שהתקבלו לפי BFS או לפי דייקסטרה.
5. התלמיד יתכנן וירשום אלגוריתם הפותר בעיה נתונה תוך שימוש באלגוריתם של קרוסקל כקופסה שחורה.
6. התלמיד יפתור בעיה תוך שימוש ב**רדוקציה** ושימוש באלגוריתם של קרוסקל כקופסה שחורה.
7. התלמיד יסביר וייתן דוגמה אחת לפחות כיצד הגישה חמדנית באה לידי ביטוי באלגוריתם של קרוסקל ומדוע גישה זו מניבה פתרון אופטימלי למציאת עץ פורש מינימלי.

<u>בעיה בסיסית</u>: נחזור מעט בהיסטוריה לשלב שבו התרבות המערבית עברה מתחבורה שאינה ממונעת לתחבורה ממונעת. יש ערים ודרכים המחברות ביניהן ומתאימות לכרכרות סוסים. אבל עם המצאת המכוניות והתרחבות השימוש בהן, יש לסלול חלק מהדרכים כך שיתאימו לנסיעה ברכב. הדרישה הבסיסית היא שיהיה ניתן להגיע לכל עיר ועיר, אך מאחר שהחומר והעבודה הנדרשים לסלילת כבישים הם יקרים המטרה היא לסלול כמה שפחות קילומטרים.

הבעיה תיפתר ע״י האלגוריתם של קרוסקל (Kruskal).

נקודות חשובות להוראה ולדיון:

- ההבדל בין הדרישות בבעיות של מסלולים קצרים ביותר לדרישות הבעיה של עץ פורש מינימלי. האם העץ הפורש שמיוצר ע״י BFS בגרף שבו לכל הקשתות משקל זהה הוא בהכרח עץ פורש מינימלי? מה ההבדל בין מציאת עץ פורש מינימלי למציאת מסלולים קצרים ביותר בגרף עם משקלות אי-שליליים?
- הפתרון מדגים שוב שימוש באסטרטגיה חמדנית.

מושגים: עץ פורש מינימלי.

פרק 8: קידוד ודחיסת נתונים (6 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמה אחת לפחות לקידוד ומהו , קוד תחיליות.
2. התלמיד יסביר וייתן דוגמה אחת לפחות לאסטרטגיה של האלגוריתם של הופמן.
3. התלמיד יסביר וייתן דוגמה אחת לפחות לסיבוכיות זמן הריצה של האלגוריתם של הופמן.
4. התלמיד יסביר וייתן דוגמה אחת לפחות לקשר בין מספר העלים לבין מספר הצמתים שיש בעץ הופמן.
5. התלמיד יתכנן וירשום אלגוריתם הפותר בעיה נתונה תוך שימוש באלגוריתם של הופמן כקופסה שחורה.
6. התלמיד יסביר וייתן דוגמה אחת לפחות לגישה חמדנית אשר באה לידי ביטוי באלגוריתם של הופמן ומדוע גישה זו מניבה פתרון אופטימלי למציאת קידוד שאורכו מינימלי.

<u>בעיה בסיסית</u>: לצורך גיבוי של טקסט מאוד חשוב אנחנו מעוניינים לשמור אותו בצורה בינארית, ע״י כך שנקודד כל אות לרצף של ביטים. אבל על הקוד שניצור לקיים כמה תנאים – ראשית, יהיה אפשר לפענח את הקידוד באופן חד משמעי, כלומר, תמיד נדע לשחזר מתוך הקוד את הטקסט המקורי. שנית, אורך הטקסט לאחר הקידוד יהיה קצר ככל שניתן. שלישית, ביצוע הקידוד והפענוח יהיו פשוטים ככל שניתן. כדי שהקידודים שניצור יהיו קצרים ככל שניתן אנחנו נעזרים בידע שנחקר ונאסף על השפה בה הספר כתוב – נתונה לנו השכיחות של כל אות בשפה בתוך טקסטים הכתובים בשפה. כך למשל, בעברית לאותיות א׳, ה׳, י׳, ו׳ שכיחות גבוהה מאוד. לעומת זאת לאות צ׳ שכיחות נמוכה יחסית.

הבעיה תיפתר ע״י האלגוריתם לבניית קוד הופמן.

נקודות חשובות להוראה ולדיון:

- בניגוד לבעיות שנדונו בפרקים קודמים בעיית הקידוד שמוצגת כאן נראית רחוקה מגרפים ובכל זאת מסתבר שהשימוש בגרפים (בפרט, בעצים) מועיל לפתרונה.
- עוד דוגמה לשימוש באסטרטגיה חמדנית.
- העץ הנוצר הוא מעניין משום שבניגוד למרבית העצים שהתלמידים נתקלו בהם בלימודי מדעי המחשב כל המידע המשמעותי בעץ שמור אך ורק בעלים.

מושגים: קוד דחיסה, קוד הופמן, קוד תחיליות.

פרק 9: הצפנה עם מפתח סימטרי (13 שעות)

הקדמה למבוא להצפנה עבור המורים. בפרקים הבאים נתחיל בהצפנת הודעות העוברות באינטרנט בין אליס לבוב כאשר אייב מאזינה, בהתחלה באמצעות מפתח סימטרי, מפתח שסוכם בין אליס לבוב (למשל במסיבת מפתחות) מבלי שנחשף לאייב. בפרק העוקב נראה כיצד ניתן ליצור מפתח סימטרי מבלי להיפגש מראש (במסיבת מפתחות) בעזרת סכמת הצפנה אסימטרית שבה לכל אחד יש מפתח ציבורי ומפתח פרטי שבעזרתם יוצרים מפתח סימטרי. לבסוף נתמודד עם התחזות של אייב להיות אלייס על ידי שליחת המפתח הציבורי שלה לבוב במקום זה של אלייס. ההתמודדות תיעזר בחתימה דיגיטלית של גורם מוסמך על אישור שבו גם פרטי הזהות של בוב וגם המפתח הציבורי שלו מופיעים יחדיו. החתימה הדיגיטלית תעשה בעזרת המפתח הפרטי של הגורם המוסמך, כך שבעזרת המפתח הציבורי של הגורם המוסמך שידוע לכל אפשר לוודא את הקשר בין המפתח הציבורי של בוב לפרטי זהותו.

<u>מטרות ביצועיות</u>:

1. התלמיד יתנסה ויממש בצופן החלפה אחד לפחות כמו היל וויז'נר.
2. התלמיד יפתח משוואת הסתברות דיסקרטית.
3. התלמיד יעשה שימוש בפונקציית XOR.
4. התלמיד יצפין ויפענח הודעות המיוצגות בביטים ולבצע מעבר מביטים לאותיות באמצעות קוד ASCII.
5. התלמיד יסביר וייתן דוגמה לצופן סימטרי.
6. התלמיד יפתח צופן OTP ולהוכיח בטיחות מושלמת שלו.
7. התלמיד יעשה שימוש ב OTP באמצעות צופן זרם ופונקציה פסאדו ראנדום PRG.
8. התלמיד יסביר וייתן דוגמא אחת לפחות ליצירת פונקציה PRG בלתי צפויה.
9. התלמיד יבחין בין PRG חלשה לחזקה ולהדגים את אלגוריתם פון ניומן.
10. התלמיד יסביר וייתן דוגמא אחת לפחות עבור OTP חלשה, ולהדגים כיצד ניתן לשבור את הצופן המוחלש שנוצר.
11. התלמיד יסביר וייתן דוגמא אחת לפחות ליצירת אלגוריתם צופן ערבול באמצעות PRG, תוך הכפלת אורך המסר והוספת ריפוד ביטים.
12. התלמיד יסביר וייתן דוגמא אחת לפחות למערכת הצפנה מוחשית ופרקטית מהעולם האמיתי.

<u>בעיה בסיסית</u>: בוב מעוניין לשלוח אימייל לאליס ברשת האינטרנט המאפשרת לצותת באופן גלוי. כלומר אם לאיב יש גישה לרשת האינטרנט היא תוכל ליירט את ההודעה ולקרוא אותה באופן מיידי. כיצד בוב יוכל לשלוח מסרים לאליס מבלי שאיב תוכל להבין אותם, גם כשהיא נחשפת לתוכנם?

הפתרון ע״י אלגוריתם הצפנה סימטרית המבוסס על מפתח סודי, שידוע לשני הצדדים בלבד, בוב ואליס.

נקודות חשובות להוראה ולדיון:

- המאפיינים הרצויים ממערכת הצפנה סימטרית ועמידותה בפני שבירת הצופן וגילוי המפתח הסודי. התייחסות לעקרון קירכהוף, כך שמאפייני האלגוריתם הינם פומביים בעוד מפתח ההצפנה סודי.
- פענוח והצפנה של הודעה במושגים של סיביות (bits). מעבר מסיביות לתווויות באמצעות קוד ASCII.
- בניית מערכת הצפנה מושלמת מבוססת על פנקס חד פעמי שאינה תלויה בכוח החישוב של היריב. המפתח נבחר מהדף הבלתי מנוצל המתאים שהוא החלק הבא של הפנקס החד פעמי. המקום של הפנקס החד פעמי שמשתמשים בו אינו סודי, התוכן סודי. ההצפנה באמצעות פונקציית XOR.
- הצורך במפתח שאורכו כאורך המסר המיועד להצפנה, הוא חיסרון בולט שהופך שליחת מסרים ארוכים לבעייתית. על מנת לייעל את העיקרון שבו עובד הפנקס החד פעמי, נשמור מפתח קצר במקום פנקס קודים ארוך, נשתמש באלגוריתם פסאדו אקראי (למשל זה של פון נוימן) ליצירת פנקס חד פעמי מהמפתח הקצר (שבהקשר זה נקרא seed). החלפת הפנקס החד פעמי בפנקס שמיוצר באמצעות מפתח קצר ופונקציה פסאודו-אקראית מייעלת משמעותית את תהליך ההצפנה והפענוח אך בו בזמן הופכת את הבטיחות להיות תלויה באורך המפתח ובאפשרות לנחש את ערכו. עדין אם המפתח בגודל ארוך מספיק (נניח באורך של 256 סיביות) ייקח למחשב הרבה זמן לנחש את המפתח הנכון.
- דרך אחרת מאוד נפוצה (AES) לשימוש במפתח קצר כדי להצפין הודעות היא להשתמש באלגוריתם ערבול בעל פרוטוקול פומבי בעוד שסדר הערבול הוא פרטי ותלוי במפתח שידוע רק לבעלי המפתח הסודי.

מושגים: פנקס חד פעמי, מפתח סודי, פונקציה פסאודו אקראית יוצרת, סיביות בינאריות וקוד ASCII, פונקציית XOR, אלגוריתם ערבול כחלופה ל AES, טיפול בסיביות וערבולן.

פרק 10: מערכת הצפנה עם מפתח אסימטרי (16 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יבחין בין מערכת כללית להצפנה בעזרת מפתח פומבי והדרישות ממנה לבין RSA כדרך להשיג מערכת הצפנה בעזרת מפתח פומבי.
2. התלמיד יישם עקרונות מתמטיים בסייסים: גורם משותף, פירוק לגורמים, מספרים ראשוניים.
3. התלמיד יבצע חישובים בשדה מודולרי מעל חיבור, כפל, חזקה.
4. התלמיד יבצע חישובי חזקות מעל חזקה בינארית ללא מחשבון ולפתח משוואות מעל שדה מודולרי.
5. התלמיד יפתח את משוואת פי של אויילר וחישובי חזקה מעל פונקציית פי בשדה מודולרי.
6. התלמיד יבחין וירשום את עקרונות משוואה פי של אויילר מעל מספרים ראשוניים.
7. התלמיד יפתח את אלגוריתם אוקלידס למציאת הגורם המשותף הגדול ביותר בין שני מספרים.
8. התלמיד יפתח קומבינציית לינארית למציאת הגורם המשותף הגדול ביותר בין מספרים ראשוניים באמצעות אלגוריתם אוקלידס המורחב.
9. התלמיד יפתח את משוואת הצפנת והפענוח RSA באמצעות העקרונות המתמטיים שנלמדו בסעיפים הקודמים.
10. התלמיד ייצר מפתח משותף באמצעות אלגוריתם אסימטרי.
11. התלמיד יחליף מפתחות בין שני צדדים דרך צד שלישי.
12. התלמיד יחליף מפתוח בין שני צדדים ללא צד שלישי.
13. התלמיד יבחין וירשום את חולשות המערכת הקריפטוגרפית ליצירת מפתח בטוח.
14. התלמיד יחשב את הצעדים הדרושים לפיצוח שיטת ההצפנה RSA במידה ויצירת המפתח נעשתה באופן שגוי.
15. התלמיד יפתח את הצעדים הנדרשים מהאלגוריתם כדי להבטיח בטיחות חישובית.

<u>בעיה בסיסית</u>: בוב מבקש לשלוח לחברתו אליס טבעת זהב. ליד ביתו של בוב יש סניף של חברת משלוחים, שכל עובדיה גנבים. הם פותחים כל חבילה, גונבים את תכולתה ושולחים אותה ריקה ליעדה. בוב כבר שמע שמועות על בעיית אמינות המשלוחים בחברה אבל אין לו כרגע אפשרות להגיע למקום אחר. כיצד יוכלו בוב ואליס להתגבר על בעיית האמינות של החברה ולוודא שהטבעת תגיע בשלום ליעדה?

הפתרון הסיפורי של הבעיה יתבסס על הגנת הקופסה באמצעות המנעול הפומבי והמפתח הפרטי של אליס, פתרון שימומש דרך מערכת ההצפנה RSA .

נקודות חשובות להוראה ולדיון:

- להבחין בין מערכת כללית להצפנה בעזרת מפתח פומבי והדרישות ממנה לבין RSA כדרך להשיג מערכת הצפנה בעזרת מפתח פומבי.
- האתגר בהשגת חד-כיווניות.
- כדי להציג את RSA יש צורך בעריכת היכרות מסוימת עם נושאים בתורת המספרים וביניהם חשבון מודולרי (פעולות חשבון בסיסיות מודולו n ואלגוריתם העלאה בחזקה מודולו n). מעבר לתועלת שבהרחבת הידע מודגם כאן הקשר החשוב בין הצפנה מודרנית כתחום יישומי ובין תורת המספרים כתחום במתמטיקה תיאורטית. עם זאת, אין העמקה בחומר המתמטי מעבר לנדרש כדי להבין את RSA ופעולתו. בפרט, אין התייחסות לחבורות.
- דיון על הרעיון בבחירת מספרים אקראיים לפי רעיון הסיבוב המעגלי
- מהם הצעדים הדרושים לפיצוח שיטת ההצפנה RSA? הבנת הצעדים האלו תוביל למה שנדרש מהאלגוריתם כדי להבטיח בטיחות חישובית.

מושגים: מערכת מפתח פומבי, חשבון מודולו (חיבור, כפל, חזקה, הופכי כפלי), מחלק משותף גדול ביותר (GCD), האלגוריתם של אוקלידס (ללא הוכחת נכונות), מספרים זרים זה לזה, משפט פרמה הקטן (ללא הוכחת נכונות), פונקציית φ של אוילר, RSA.

פרק 11: בניית אמון באמצעות מפתח פומבי (PKI) וחתימה דיגיטלית (7 שעות)

<u>מטרות ביצועיות</u>:

1. התלמיד יסביר וייתן דוגמא אחת לפחות להתקפת "התקפת האדם שבתווך" עבור מערכת צפנה אסימטרית ובפרט מערכת המבוססת על אלגוריתם RSA.
2. התלמיד יסביר וייתן דוגמא אחת לפחות כיצד ניתן לפתור את "התקפת האדם שבתווך" באמצעות חתימה דיגיטלית
3. התלמיד יסביר וייתן דוגמא אחת לפחות מדוע החותם על התעודה אינו יכול (בקלות) להכחיש את העובדה שחתם עליה.
4. התלמיד יתכנן וירשום סכמת חתימה דיגיטלית שמתבססת על שלושה אלגוריתמים: Gen, Sing, Vrfy. התלמיד יציג את קלטי ופלטי האלגוריתמים ויסביר באילו מצבים החתימה נשברת.
5. התלמיד יסביר וייתן דוגמא אחת לפחות ליצירת חתימה באמצעות אלגוריתם RSA שנלמד בפרק הקודם תוך התייחסות לחולשות של חתימה על מסר ספציפי מול חתימה על מסרים רנדומאליים. התלמיד יסביר מהן החולשות באלגוריתם כאשר תוקף מנסה לייצר חתימה חדשה משתי חתימות קודמות.
6. התלמיד יסביר וייתן דוגמא אחת לפחות לבניית תשתית PKI. התלמיד יגדיר את הישויות בתשתית למימוש בחתימות כמפתח מאובטח.
7. התלמיד יסביר וייתן דוגמא אחת לפחות כיצד משתמש הגוף המאמת במפתחות שבידו (עבור ישות מסוימת), על מה הוא חותם, באיזה מפתח משתמש לחתימה וכיצד ניתן לאמת את החתימה (התלמיד יסביר מי מאמת את החתימה ובאיזה שלב).
8. התלמיד יסביר וייתן דוגמא אחת לפחות לתהליך האימות המתבצע מול הגוף המאמת, הן מהצד השולח את ההודעה (זיהוי פיזי וקישור בלתי ניתן להפרדה באמצעות חתימה על מסמך עם המאפיינים הפיזיים ועם המפתח הציבורי) והן מול הצד שמקבל את ההודעה ומאמת אותה באמצעות המפתח הציבורי (הידוע לכל) של הגוף המאמת.

<u>בעיה בסיסית</u>: בפרק הקודם ראינו שכל אחד יכול להצפין באמצעות המפתח הפומבי של RSA. אך מה אם בוב שרוצה לשלוח הודעה מוצפנת לאליס, יקבל מפתח פומבי שלא שייך לה אלא לאיב שמעוניינת לדעת את תוכנה של ההודעה שבוב מייעד עבור אליס? אם בוב ישתמש במפתח הפומבי הזה כדי להצפין את ההודעה איב תוכל לפענח אותה עם המפתח הפרטי שלה. איך בוב ידע שאכן המפתח הפומבי שייך לאליס ולא לאיב?
הבעיה תיפתר ע"י בניית רשת אמון שתנפיק תעודה בעלת חתימה דיגיטלית המאמתת את זהותה של אליס כבעלת המפתח הפומבי שלה.

נקודות חשובות להוראה ולדיון:

- מערכת PKI הינה תשתית המבוססת על הצפנה אסימטרית.

- נדון בהשוואה בין סודיות לבין אימות. אימות אינו מושג מהצפנת ההודעה. ההצפנה פגיעה מפני "התקפת האדם שבתווך".
- אימות וחתימה דיגיטלית בעזרת RSA.
- התהליכים שנדרשים לביצוע תהליך האימות מול הגוף המאמת מבחינת המאומת והמאמת. תוכן תעודת האימות, הצורך בפרטי הזהות של הישות שעבורה הופקה התעודה והמפתח הציבורי של הישות. והצורך בחתימה של התעודה בכללותה, ללא אפשרות להפרדת חלקים, פרטי הזהות והמפתח הציבורי ביחד.
- הגדרת הגוף המאמת המוסמך לחתום (Certificate Authority), שגם לו מפתח פרטי וציבורי. הצורך שהמפתח הציבורי של הגוף המאמת יהיה ידוע ומפורסם ברבים (למשל, כחלק מהפצת הדפדפנים) כדי שאפשר יהיה לפענח את החתימה שלו על המסמך, חתימה שנעשית על ידי הצפנה של תעודת האימות באמצעות המפתח הפרטי של הגוף המוסמך.
- הגוף המאמת בודק שאכן מי שמזדהה בפניו (לעיתים פיזית) הוא בעל המפתח הציבורי, ואז הגוף המאמת חותם באמצעות המפתח הפרטי שלו (על קובץ שמכיל את פרטי הזהות יחד עם המפתח הציבורי שמשויך לזהות. המפתח הציבורי של הגוף המאמת ידוע לכולם (למשל, נמצא בדפדפן) ומאפשר לבדוק את תקינות חתימת התעודה.
- דיון בקשר בין החתימה הדיגיטלית (המאמתת את השולח) למפתח ההצפנה הפומבי. ראשית השולח יוודא את האימות באמצעות המפתח הציבורי הידוע ברבים של הגוף המאמת. רק אז ישתמש במפתח המאומת (הציבורי) של הנמען להצפנת ההודעה. הפרק מחבר בין הישות הפיזית למפתח הציבורי שלה באמצעות הגוף המאמת. לאחר תהליך האימות של המפתח הציבורי של הנמען, ניתן להשתמש ב-RSA ליצירת מפתח סימטרי והצפנה באמצעות המפתח הסימטרי שנוצר.

מושגים: תשתית PKI, סודיות, אימות, MITM, Certificate Authority, חתימה דיגיטלית, מפתח ציבורי, RSA ליצירת מפתחות, אינטרנט, דפדפן, web of trust, SSL.