# תכנית הלימודים קריפטוגרפיה – פרק בחירה בתכנית הלימודים במדעי המחשב לתיכון

חברי הצוות שהכינו את ההצעה:

פרופ' שלומי דולב

מר גל בר-און

## פריסת שעות

| | חלוקת השעות לפרק | מעבדה | כיתה | סה"כ |
|---|---|---|---|---|
| א | מבוא להצפנה סימטרית, צפנים נאיביים ושבירתם | 8 | 9 | 17 |
| ב | הצפנה עם מפתח סימטרי | 6 | 14 | 20 |
| ג | פונקציית גיבוב וגיבוב קריפטוגרפי | 3 | 10 | 13 |
| ד | מערכת הצפנה עם מפתח אסימטרי | 6 | 19 | 25 |
| ה | בניית אמון באמצעות מפתח פומבי (PKI) וחתימה דיגיטלית | 5 | 10 | 15 |
| | סה"כ שעות | 30 | 60 | 90 |

תוכן עניינים (הקלקה על מספר העמוד + לחצן Ctrl ביחד, תקפיץ לעמוד המתאים)



# פרק א: מבוא להצפנה סימטרית, צפנים נאיביים ושבירתם (17 שעות)

## הקדמה

בעיית הצפנה קלאסית, בין אליס ובוב, תלווה אותנו בפרקים הקרובים. נתחיל בהצפנת הודעות שעוברות בין אליס לבוב כאשר אייב מאזינה, באמצעות מפתח סימטרי .

בפרק זה נכיר צפנים היסטוריים המבוססים על אלגוריתם צופן נאיבי (ניתן לשבירה בקלות). נכון, צפנים אלו כבר אינם בשימוש, אך היכרות עם אלגוריתמי צופן נאיביים יעזרו לתלמיד להבין את אופי הבעיה, דרך החשיבה וההגיון מאחורי יצירת צופן ופיענוחו. בנוסף, נוכל ליצור, בקלות יחסית, אלגוריתם עבור התקפות שישברו את הצופן ויחשפו את מפתח ההצפנה.

בפרק העוקב נלמד כיצד להצפין ולהעביר הודעות בין אליס לבוב באמצעות אלגוריתם מבוסס מפתח סימטרי. מפתח סימטרי נקבע מראש ובעל בטיחות מושלמת וסמנטית, כך שאייב המאזינה, לא תצליח לשבור את הצופן לעולם.

בפרקים הבאים, נלמד כיצד ניתן ליצור מפתח סימטרי מבלי להיפגש מראש ("במסיבת מפתחות") בעזרת סכמת הצפנה אסימטרית שבה לכל אחד יש מפתח ציבורי ומפתח פרטי, בעזרתם יוצרים מפתח סימטרי.

לבסוף, נתמודד עם תופעת ההתחזות של אייב להיות אלייס על ידי שליחת המפתח הציבורי שלה לבוב במקום זה של אליס. לצורך זה ניעזר 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.

## מטרות ביצועיות

1. התלמיד יבחין בין הישויות המעוניינות לתקשר באופן מאובטח והיריבים עימם מתמודדים.
2. התלמיד יסביר מהו מפתח הצופן, כמו גם את החשיבות שישמר בסוד רק בין שני הצדדים המתקשרים.
3. התלמיד יסביר מהם האלגוריתמים המרכזיים במערכת צופן.
4. התלמיד יכתוב אלגוריתם המיישם הצפנה ופענוח קיסר באמצעות גלגל הזזה.
5. התלמיד יכתוב אלגוריתם צופן ופענוח המבוסס על שינוי מקום סדר האותיות בהתאם לגודל המפתח והטקסט.
6. התלמיד ישבור את צופן "שינוי מקום סדר אותיות" באמצעות אלגוריתם כוח-גס ויחשב את סיבוכיותו.
7. התלמיד יסביר ויתן דוגמא אחת לצופן החלפה החסין מפני התקפת כוח-גס.
8. התלמיד יעשה שימוש בטבלת מיפוי אותיות לצורך שבירת צופן החלפה.
9. התלמיד יסביר ויתן דוגמא אחת לפחות לצופן וויז'נר פולי-אלפביתי בעל מפתח מרובה אותיות וחסין מפני התקפת כוח-גס פשוטה.
10. התלמיד ינתח טקסט באמצעות טבלת תדירות אותיות בשפה האנגלית.
11. התלמיד יסביר ויתן דוגמא אחת למציאת אורך המפתח באמצעות אלגוריתם קסיסקי (Kasiski) באמצעות הסתברות החזרה בגודל מרווח המפתח.
12. התלמיד יסביר ויתן דוגמא אחת לשבירת צופן וויז'נר באמצעות אלגוריתם קסיסקי (Kasiski) והתקפת ניתוח תדירויות.

## דגשים ודרכי הוראה

- המאפיינים הרצויים במערכת הצפנה סימטרית ועמידותה בפני שבירת הצופן וגילוי המפתח הסודי.
- ייצוג מערכת הצפנה המורכבת מזוג אלגוריתמים, אלגוריתם הצפנה המסומן על ידי E ואלגוריתם פענוח D.
- בניית פונקציה המיישמת צופן קיסר, שהוא בעצם צופן החלפה באורך והסטה קבוע. מומלץ לקיים דיון על חולשת הצופן. המפתח אינו אקראי כך שאם תוקף יודע כיצד פועלת תכנית ההצפנה, הוא יכול לפענח את ההודעה בקלות.
- שיפור צופן קיסר באמצעות צופן טרנספוזיציה, בעל אפשרויות רבות למפתח (הסודי), מכיוון שמספר המפתחות האפשריים תלוי באורך המסר.
- כתיבת אלגוריתם בשיטת כוח-גס לשבירת צופן טרנספוזיציה (קיימות אלפי אפשרויות של מפתחות). המפתח הנכון יהיה זה המגלה משפטי אנגלית תקינים אותם נבדוק באמצעות מבנה נתונים של מילון.
- בניית מערכת הצפנה מבוססת צופן החלפה. המפתח לצופן ההחלפה בגודל 26 אותיות אלף-בית בסדר אקראי. צופן זה מאפשר טווח עצום של מפתחות אפשריים ולכן עמיד בפני התקפת כוח גס.
- תוקף המעוניין לשבור מערכת צופן החלפה נאלץ להשתמש בשיטות מתוחכמות יותר מהתקפת כוח-גס. את אלגוריתם ההתקפה נבנה באמצעות ערכי מילון, על מנת למפות את אותיות הפענוח האפשריות של הצופן תוך צמצום אפשרויות הפענוח הנכונות.
- שיפור צופן מונו-אלפביתי באמצעות צופן וויז'נר פולי-אלפביתי המיישם קשר יחיד-לרבים בין תו-טקסט לתו-צופן. כעת כל תו אלפביתי מתוך הטקסט ממופה לתווים שונים בטקסט צופן.
- מומלץ לדון ביכולתנו לייצג את התדירות באחוזים עבור מספר פעמים שהאירוע מתרחש. צופן וויז'נר מאפשר לחשוף את תדירות חזרת האותיות ועל סמך טבלת התדירויות בשפה האנגלית נוכל להבין (בהסתברות מסוימת) את מיפוי הצופן.
- באמצעות אלגוריתם קסיסקי(Kasiski) נגלה את אורך המפתח בצופן וויז'נר. האלגוריתם מנסה להתאים את התפלגות תדירות המילים באנגלית בהתאמה לגודל מפתח מסוים. כאשר ההסתברות הגדולה ביותר להתאמת התפלגות התדירויות, תתרחש כאשר הגענו לאורך המפתח שהצפין את הטקסט.

## פרק ב: הצפנה עם מפתח סימטרי (20 שעות)

בעיה בסיסית: 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 יכול 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.

### מושגים

- פנקס חד פעמי
- מפתח סודי
- פונקציה פסאודו אקראית יוצרת
- סיביות בינאריות, טבלת ASCII
- פונקציית XOR
- אלגוריתם ערבול כחלופה ל AES
- טיפול וערבול סיביות

### מטרות ביצועיות

1. התלמיד יתנסה 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 מהו צופן סימטרי.
6. התלמיד יפתח צופן OTPויראה את הבטיחות מושלמת שלו.
7. התלמיד יעשה שימוש ב OTP באמצעות צופן זרם ופונקציה פסאודו-רנדום.PRG
8. התלמיד יסביר ויתן דוגמא אחת לפחות ליצירת פונקציה PRG בלתי צפויה .
9. התלמיד יבחין בין PRG חלשה לחזקה וידגים את אלגוריתם פון ניומן .
10. התלמיד יסביר ויתן דוגמא אחת לפחות עבור OTP חלשה, וידגים כיצד ניתן לשבור את הצופן המוחלש שנוצר.
11. התלמיד יסביר ויתן דוגמא אחת לפחות ליצירת אלגוריתם צופן ערבול באמצעות PRG, תוך הכפלת אורך המסר והוספת ריפוד ביטים.
12. התלמיד יסביר ויתן דוגמא אחת לפחות למערכת הצפנה מעשית ופרקטית מהעולם האמיתי.

## דגשים ודרכי הוראה

- 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, אך התוכן סודי. להדגיש כי ההצפנה באמצעות פונקציית XOR.
- יש לדון בסוגיה שהצורך 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 פסאודו אקראי (למשל זה של פון נוימן) ליצירת פנקס חד פעמי מהמפתח הקצר (בהקשר זה נקרא החלפת seed). הפנקס החד פעמי שמיוצר באמצעות מפתח קצר נוסף על פונקציה פסאודו-אקראית מייעלת משמעותית את תהליך ההצפנה והפענוח אך בו בזמן הופכת את הבטיחות להיות תלויה באורך המפתח ובאפשרות לנחש את ערכו. יחד עם זאת, אם המפתח ארוך מספיק (נניח באורך של 256 סיביות) ייקח למחשב הרבה זמן לנחש את המפתח הנכון.
- יש להציג דרך אחרת, מאוד נפוצה, (AES) לשימוש במפתח קצר כדי להצפין הודעות : להשתמש באלגוריתם ערבול בעל פרוטוקול פומבי בעוד שסדר הערבול הוא פרטי ותלוי במפתח שידוע רק לבעלי המפתח הסודי.

## פרק ג: פונקציית גיבוב וגיבוב קריפטוגרפי (13 שעות)

<u>בעיה בסיסית</u>: בוב מעוניין להעביר סכום כסף מסוים, בהעברה בנקאית, אל אליס. את קובץ אישור הפעולה הבנקאית, בוב שולח דרך רשת האינטרנט (לא מאובטחת) לאליס. אליס מעוניינת לאמת את תקינות קובץ אישור הפעולה (הבנקאית) שבוב ביצע ושלח לה. ידוע כי במהלך העברת קובץ ברשת, פרטים יכולים ללכת לאיבוד או להשתנות. זאת עקב מעבר תקול של הנתונים ברשת או מאידך, יריב זדוני המאזין לרשת מנסה לחבל בתקינות הקובץ. כיצד אליס תוודא את תקינות קובץ האישור שנשלח מבוב?

הבעיה נפתרת ע״י פונקציית גיבוב (Hashing) קריפטוגרפית. בוב יפרסם את תוצאת גיבוב (עבור הפעולה הבנקאית שביצע) בנפרד לשליחת הקובץ לאליס (יפרסם במקום פומבי ונגיש, למשל באתר האינטרנט). אליס תבצע את אימות הפעולה, ע״י השוואת ערך הגיבוב המפורסם, אל מול תוצאת הגיבוב המתקבלת מהפעלת פונקציית הגיבוב הקריפטוגרפי על קובץ אישור הפעולה שקיבלה מבוב.

### מושגים

- פונקציית גיבוב
- פונקציה פסאודו אקראית
- תמצות הודעה
- פונקציית גיבוב קריפטוגרפית
- SHA
- פונקציה חד כיוונית
- התנגשויות
- עקרון שובך היונים
- seed, XOR
- בלוקציין וכריית בלוק

### מטרות ביצועיות

1. התלמיד יסביר מהי פונקציה חד כיוונית.
2. התלמיד יבנה פונקציית גיבוב המתמצתת הודעה גדולה כך שההסתברות ששתי הודעות יתנגשו קטנה.
3. התלמיד ידגים פשטות בחישוב פלט של פונקציה חד כיוונית.
4. התלמיד ידגים את הקושי בשחזור הקלט בהינתן פלט של פונקציה חד-כיוונית.
5. התלמיד יתן דוגמא אחת לפחות כיצד חיפוש ממצה אינו מצליח לשחזר קלט של פונקציית גיבוב חד-כיוונית באופן לא יעיל.
6. התלמיד יסביר את עקרון שובך היונים.
7. התלמיד יסביר וייתן דוגמא אחת לפחות מדוע חשוב למנוע התנגשות בפונקציית גיבוב.
8. התלמיד יסביר ויתן דוגמא ליצירת מערכת אותנטיקציה באמצעות פונקציית גיבוב.
9. התלמיד ייצור מפתח סודי סימטרי פונקציית הגיבוב.

10. התלמיד יסביר ויתן דוגמא אחת לפחות מדוע לא ניתן לשנות הודעה שהונפק עבורה מפתח סודי באמצעות פונקציית גיבוב.
11. התלמיד יסביר ויתן דוגמא אחת לפחות לשימוש בפונקציית גיבוב במערכת בלוקצ'יין.
12. התלמיד יסביר ויתן דוגמא אחת לפחות כיצד מושגת חתימה במערכת בלוקצ'יין (באמצעות פונקציית גיבוב) ומדוע אינה ניתנת לשינוי. התלמיד ידגים כיצד שינוי בחתימה יגרום לביטול שרשרת הבלוקים החל מהבלוק העוקב.
13. התלמיד יהיה מסוגל להסביר כיצד עקרון החד כיווניות בפונקציית גיבוב בא לידי ביטוי בעת כריית בלוק חדש במערכת בלוקצ'יין.

אסטרטגיות אלגוריתמיות: בניית פונקציית גיבוב, חיפוש ממצה, חד-כיווניות, אימות הודעות.

## דגשים ודרכי הוראה

- הדרישות מפונקציית גיבוב לעומת הדרישות מפונקציית גיבוב קריפטוגרפית.
- הבנת הרעיון כי פונקציה חד כיוונית בעלת סיבוכיות נמוכה לחישוב ובעלת סיבוכיות גבוהה לשחזור פלט לקלט.
- הבנה כי חיפוש ממצה(Exhaustive search ) כאסטרטגיה אלגוריתמית כללית, לא יעילה. יש לדון בהשלכות הקריפטוגרפיות שלה כהתקפת כוח-גס (Brute force).
- בניית פונקציית גיבוב תתאפשר באמצעות ההודעה עליה נבצע את האימות כ seed עבור פונקציית הפסאדו-אקראית שנלמדה בפרק הקודם. חלק מהרצף המתקבל ישמש כתוצאת הגיבוב .
- נשים לב שלא כל פונקציה פסאודו-אקראית מיישמת חד כיווניות. על מנת ליישם פונקציה גיבוב קריפטוגרפית כדוגמת SHA, נרצה להשתמש בפונקציית פסאודו חד כיוונית.
- כיצד נתמודד עם הודעות ארוכות בתהליך הגיבוב? הפתרון מושג באמצעות חלוקת ההודעה והפעלת פונקציית XOR בין חלקי ההודעה. נשתמש בתוצאת הגיבוב של החלק הראשון ונפעיל XOR על החלק השני. פלט זה ישמש כ seed שממנו ניצור גיבוב של שני החלקים. התהליך יחזור באופן איטרטיבי על יתר חלקי ההודעה.
- נשים דגש על מצב בעייתי כאשר seed התחלתי כולו אפסים. במקרה זה, רצף הפסאדו אקראי ישאר תמיד אפס. הפתרון מושג באמצעות קביעת seed התחלתי קבוע שונה מאפס. זאת על מנת לשמר את זהות הפעולות החל מהגיבוב הראשון.
- כיצד ניתן לכרות בלוקים במערכת בלוקצ'יין? חתימת הבלוק חייבת לעמוד בדרישות מסוימות, לדוגמא להסתיים ב 10 אפסים. כיצד נשיג זאת אם אסור לשנות שום טרנזקציה בבלוק וקיימת חתימת גיבוב ייחודית לכל קלט. על מנת להשיג את השינוי הנדרש מבלי לשנות את המידע נכניס nonce עליו יתבצע השינוי על מנת להשיג חתימה שעומדת בדרישות הבלוק.

## פרק ד: מערכת הצפנה עם מפתח אסימטרי (25 שעות)

<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, תוך שימוש במערכת ההצפנה RSA .

### 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 $\Pi$ של אוילר
- RSA.

### מטרות ביצועיות

1. התלמיד יבחין בין מערכת כללית להצפנה בעזרת מפתח פומבי והדרישות ממנה לעומת RSA כדרך להשיג מערכת הצפנה בעזרת מפתח פומבי.
2. התלמיד יפגין מיומנות בעקרונות מתמטיים בסיסיים: 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 ויפתח משוואות מעל שדה מודולרי.
5. התלמיד יפתח את משוואת $\Pi$ של אויילר וחישובי חזקה מעל פונקציית $\Pi$ בשדה מודולרי.
6. התלמיד יבחין בעקרונות משוואה $\Pi$ של אויילר מעל מספרים ראשוניים.
7. התלמיד יפתח את אלגוריתם אוקלידס למציאת הגורם המשותף הגדול ביותר בין שני מספרים.
8. התלמיד יפתח קומבינציות לינאריות למציאת הגורם המשותף הגדול ביותר בין מספרים ראשוניים באמצעות אלגוריתם אוקלידס המורחב.
9. התלמיד יפתח את משוואת הצפנה ופענוחRSA באמצעות העקרונות המתמטיים שנלמדו בסעיפים הקודמים .

10. התלמיד ייצר מפתח משותף באמצעות אלגוריתם אסימטרי.
11. התלמיד יחליף מפתוח בין שני צדדים דרך צד שלישי.
12. התלמיד יחליף מפתוח בין שני צדדים ללא צד שלישי.
13. התלמיד יבחין בחולשות מערכת קריפטוגרפית 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.
16. התלמיד יהיה מסוגל להסביר את הרעיון בבסיס הוכחה באפס מידע ( Zero knowledge proofs) כך שבעל המפתח הפרטי (מוכיח) יכול לשכנע את הצד השני (המוודא) התאמה למפתח הציבורי מבלי לחשוף את המפתח הפרטי.

## דגשים ודרכי הוראה

- יש לדון בכיתה בהבחנה 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 בנוסף גם אלגוריתם העלאה בחזקה מודולו n). מעבר לתועלת בהרחבת הידע מודגם כאן הקשר החשוב בין הצפנה מודרנית כתחום יישומי ובין תורת המספרים כתחום במתמטיקה תיאורטית. עם זאת, אין צורך להעמיק בחומר המתמטי מעבר לנדרש כדי להבין את RSA ופעולתו. בפרט, אין לבצע התייחסות לחבורות.
- מומלץ לקיים 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 .

## פרק ה: בניית אמון באמצעות מפתח פומבי (**PKI**) וחתימה דיגיטלית (15 שעות)

<u>בעיה בסיסית</u>: בפרק הקודם ראינו שכל אחד יכול להצפין באמצעות המפתח הפומבי של RSA. ננסה להתמודד עם הנסיבות לפיהם בוב רוצה לשלוח הודעה מוצפנת לאליס, אך יקבל מפתח פומבי שלא שייך לה אלא לאיב המעוניינת לדעת את תוכן ההודעה שבוב מעונין להעביר לאליס? 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 נפתרת ע"י בניית רשת אמון להנפקת תעודה בעלת חתימה דיגיטלית המאמתת את זהותה של אליס כבעלת המפתח הפומבי שלה.

### מושגים

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

### מטרות ביצועיות

1. התלמיד יסביר ויתן דוגמא אחת לפחות להתקפה מסוג "התקפת האדם שבתווך" עבור מערכת הצפנה אסימטרית ובפרט מערכת המבוססת על אלגוריתם RSA.
2. התלמיד יסביר ויתן דוגמא אחת לפחות כיצד ניתן לפתור את "התקפת האדם שבתווך" באמצעות חתימה דיגיטלית.
3. התלמיד יסביר ויתן דוגמא אחת לפחות מדוע החותם על התעודה אינו יכול (בקלות) להכחיש את העובדה שחתם עליה.
4. התלמיד יתכנן וירשום סכמת חתימה דיגיטלית מבוססת על שלושה אלגוריתמים: Gen, Sing, Vrfy. התלמיד יציג את קלטי ופלטי האלגוריתמים ויסביר באילו מצבים החתימה נשברת.
5. התלמיד יסביר ויתן דוגמא אחת לפחות ליצירת חתימה באמצעות אלגוריתם RSA שנלמד בפרק הקודם תוך התייחסות לחולשות של חתימה על מסר ספציפי מול חתימה על מסרים רנדומליים. התלמיד יסביר מהן החולשות באלגוריתם כאשר תוקף מנסה לייצר חתימה חדשה משתי חתימות קודמות.
6. התלמיד יסביר ויתן דוגמא אחת לפחות לבניית תשתית PKI. התלמיד יגדיר את הישויות בתשתית למימוש בחתימות כמפתח מאובטח.

7. התלמיד יסביר ויתן 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 ויתן דוגמא אחת לפחות לתהליך אימות 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.

## דגשים ודרכי הוראה

- 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 הדרושים לביצוע תהליך האימות מול הגוף המאמת מבחינת המאומת והמאמת. תוכן תעודת האימות, הצורך בפרטי הזהות של הישות שעבורה הופקה התעודה והמפתח הציבורי של הישות. נדון בצורך 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 מסמך, 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 המשויך לזהות. המפתח הציבורי של הגוף המאמת ידוע לכולם (למשל, נמצא בדפדפן) ומאפשר לבדוק את תקינות החתימה על התעודה.
- דיון בקשר בין החתימה הדיגיטלית (המאמתת את השולח) ומפתח ההצפנה הפומבי. ראשית השולח יוודא את האימות באמצעות המפתח הציבורי הידוע ברבים של הגוף המאמת. רק אז יעשה שימוש במפתח המאומת (הציבורי) של הנמען להצפנת ההודעה. התהליך 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.