**תיעוד עבודה – מיני פרויקט במערכות הגנה ברשת**

1. **מטרת הכלי** – הכלי שאנחנו בונים הוא צ'אט קבוצתי מוצפן מקצה לקצה, במודל server-client.  
   הserver מחזיק את הצ'אט וניתן להתחבר אליו ממספר clients במקביל. ההצפנה היא מסוג RSA.  
   הכלי שלנו אכן עונה למטרה, הוא מצפין את ההודעות מקצה לקצה כך שלא ניתן לתפוס את ההודעות בדרך ולפענח אותן ונותנת ממשק נוח למשתמש שנבנה בעזרת ספריית Tkinter. הכלי עונה למטרה, תחת הגבלות מסוימות של ארכיטקטורת ההצפנה.
2. **בעיות שנתקלנו בהן** – נתקלנו במספר בעיות, רובן קשורות לארכיטקטורת ההצפנה :  
   **2.1.** ארכיטקטורת ההצפנה של RSA קובעת כי כל צד בתקשורת מחולל מפתח ציבורי ומפתח פרטי.  
   ההצפנה היא א-סימטרית ולמדנו כי זו דורשת שההצפנה והפענוח ישתמשו במפתחות שונים. ההצפנה נעשית ע"י שימוש במפתח הציבורי, לכן יש צורך שכל משתמש יחזיק את כלל המפתחות הציבוריים של המשתמשים אליהם הוא מעוניין לשלוח הודעה (במקרה השימוש שלנו, זה אומר לכלל המשתמשים). ניסינו להבין מה תהיה דרך טובה להעביר למשתמש מסוים את כלל המפתחות הציבוריים ונוכחנו לדעת שזו אחת מבעיות הליבה של הארכיטקטורה של RSA.   
   **2.2.** בעיה נוספת שצמחה מארכיטקטורת הRSA היא אורך ההודעה שניתן לשלוח כך שהיא תהיה מוצפנת. לRSA מגבלות על מספר הבייטים המקודדים בפעולת ההצפנה. לכן, השימוש בצ'אט הוא תחת הגבלת אורך ההודעה. בדומה לאפליקציות שאנו משתמשים בהן כמו WhatsApp שגם בה קיימת הגבלה על אורך ההודעה, במידה והמשתמש מקליד הודעה ארוכה מדי, הוא יתבקש לפצל את ההודעה או לקצר את אורכה.  
   **2.3.** הצ'אט שלנו אמור להוות מודל של הצפנה מקצה לקצה. בניסיון להתמודד עם בעיה 2.1 שציינו לעיל, ניסינו לשלב הצפנה סימטרית בעבודה (הצפנת AES) כך שמפתח ההצפנה הסימטרי יוצפן ע"י הRSA. גילינו שזו הדרך לגשת להצפנה של טקסטים ארוכים אך הסתבכנו עם המימוש. לאחר דיון עם דורון, הוחלט כי נחולל עבור הserver מפתחות וכל ההודעות יוצפנו תחילה עם המפתח של הserver, יפוענחו וישלחו לכל client לפי המפתח האישי שלו שהשרת מחזיק. כלומר, ההודעה עוברת פענוח בדרך שמהווה סתירה לעקרון ההצפנה מקצה לקצה, אך זו נחשבת כ"נקודת כשל" כפי שדורון הסביר לנו, נקודה שהטיפול בה מצריך פתרונות מורכבים שעד היום לא ידועים להם פתרונות יעילים מאוד.  
   **2.4.** קבענו לעצמנו יעד לבנות GUI נוח למשתמש. בחרנו להשתמש בספריה בסיסית של פייתון Tkinter ובמהרה נוכחנו לדעת שהקישוריות בין הIO לבין התצוגה בחלון הצ'אט מצריכה תזמון בין קבלת המידע או שליחתו לבין הצגתו וניהול של מה מוצג למשתמש. היינו צריכים לנהל זאת באמצעות ת'רדים נפרדים עבור הGUI ועבור התקשורת ולדעת לחלק את העבודה ביניהם בצורה שלא תפגע בעבודה של האחר.
3. **חוזקות וחולשות של הכלי**:  
   3.1. **חוזקות   
   א.** ממשק נוח למשתמש – בחירת שם לצ'אט ומשם שימוש פשוט ע"י שליחת הודעות.  
   **ב.** הצפנת ההודעות – לא ניתן לתפוס ההודעות ולבצע פעולות MitM של עריכת ההודעה או קריאתה.  
   **ג.** למשתמש אין גישה למערכת עצמה – היא קופסה שחורה ולכן אי אפשר להשפיע על ההצפנה או לחבל בה.  
   3.2. **חולשות  
   א.** ההצפנה מקצה לקצה אינה "טהורה" – הסרבר מפענח את ההודעה ומצפין אותה מחדש.  
   **ב.** המערכת אינה סקאלבילית, הסרבר מחזיק ת'רד עבור כל לקוח.  
   **ג.** אורך ההודעה מוגבל עקב מגבלות הצפנת RSA.
4. **תאור עבודת הכלי** – ראשית, מקימים את הסרבר כך שיהווה נקודת התחברות עבור הלקוחות שמעוניינים לשוחח בצ'אט.  
   לאחר מכן, לקוחות יכולים להתחיל להתחבר. בעת ההתחברות כל לקוח צריך לבחור שם משתמש שמייצג אותו בצ'אט. מאחורי הקלעים, כאשר הלקוח בוחר את הnickname מתבצעת החלפת מפתחות ציבוריים בינו לבין הserver. באופן טבעי השרת צריך לשמור מיפוי של שמות המשתמשים למפתחות הציבוריים על מנת להיות מסוגל להעביר הודעות מוצפנות למשתמשים והמשתמשים צריכים את המפתח הציבורי של השרת על מנת לבצע את השלב הראשון של התקשורת המוצפנת (העברת ההודעה לשרת, מוצפנת עם המפתח שלו). כפי שתיארנו, לקוח A שולח הודעה לקבוצת הצ'אט וזו מועברת דרך השרת (מפעונחת ומוצפנת מחדש) לכלל המשתמשים שמחוברים באותה נקודת זמן. שאר עבודת הכלי הוא עבודת הGUI שמציגה התראות והודעות בחלון הצ'אט.  
   הוספנו מספר פיצ'רים כמו:

* לקוחות יכולים להתנתק ע"י לחיצה על כפתור הX בחלון הצ'אט והם מוסרים מהרשימות שמחזיק השרת.
* השרת יכול לכבות את עצמו ע"י הקשת q בטרמינל ומתבצע graceful shutdown של המשתמשים הפעילים בצ'אט שרק לאחריו השרת מכבה את עצמו.
* ניסינו לדמות הרגשה אמיתית של צ'אט כך שכפתור הENTER ישלח את ההודעה כפי שאנחנו רגילים וShift + Enter ירד שורה.
* כל סוג הודעה מאופיין אחרת:  
  - הודעה מסוג notification שמתבצעת על ידי broadcast מהשרת נצבעת בכחול.  
  - הודעה שנשלחת מלקוח מסוימת מוגדרת עבור אותו לקוח outgoing, תיצבע בחלון שלו באפור ובחלונות של שאר המשתמשים תוגדר כincoming ותיצבע בירוק.
* הקליינט מקבל notification בחלון הצ'אט כשהוא מקיש הודעה ארוכה מדי עבור הצפנת הRSA.
* בעת ההתחברות, ניתן לבחור להשתמש בין Host, Port דיפולטיביים לinput של המשתמש (מניחים כי המשתמש לא מקיש דברים רנדומאליים).