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

1. **אפיון הפרויקט** – נרצה לבנות מערכת שמדמה צ'אט בין לקוחות, כאשר ההודעות שמועברות בין הלקוחות מוצפנות מקצה לקצה. לאחר בדיקה, הצפנה מקצה לקצה היא נושא באבטחה שיותר ויותר חברות מאמצות ומשתמשות בו – לדוגמה חברות כמו META דרך צ'אט המסנג'ר שלהן או טלגרם. הצורך בהצפנה הזו היא על מנת לאפשר פרטיות ללקוחות. המשמעות של ההצפנה היא שאם לקוח א' שולח הודעה ללקוח ב' וצד שלישי יתפוס את ההודעה באמצע – הוא לא יכול לפענח אותה ובכך נשמרת הפרטיות של הלקוחות. דבר מעניין נוסף הוא שברוב ההצפנות (שאינן מקצה לקצה), ניתן לפענח את ההצפנה ובכך לשחזר מה היה כתוב בהודעות ולהשתמש במידע הזה, אבל הצפנה מקצה לקצה היא הצפנה כזו שבה רק ללקוח השולח וללקוח המקבל יש את מפתח ההצפנה. לכן, החלטנו שאנחנו רוצים למדל את זה וליצור מערכת כזו.
2. **יעדי הפרויקט** – היעדים שהצבנו לעצמנו הם :  
   **2.1.** התמקצעות בשפת תכנות שלא נלמדה בתואר בצורה משמעותית – פיית'ון  
   **2.2.** למידה על הצפנה ומשמעויות שלה  
   **2.3.** ליצור מערכת שעובדת טוב ונראית טוב
3. **אבני דרך ולוח זמנים** – מבחינת אבני דרך, אנחנו רוצים לפרק את העבודה לכמה גורמים:  
   א. בניית הלוגיקה של הצ'אט, לאפשר ללקוח לדבר עם כמה לקוחות אחרים בקבוצה.  
   ב. בניית ההצפנה ובדיקות של המערכת.  
   ג. עיצוב GUI והוספת פיצ'רים למערכת במסגרת הזמן.
4. **אתגרים וקשיים** – האתגר בבניית המערכת הוא ללמוד מספיק **ולהבין** את אופן הפעולה של הצפנה, אילו אופציות יש על מנת להצפין מקצה לקצה ולהעמיד תוצר שעומד ביעדים שלנו.  
   בנוסף שימוש בכלים שלא למדנו עליהם – עיצוב GUI , תכנות בפיית'ון.