**פרויקט אפליקציית מסרים**

**פרוטוקול http**

הודעות:

פורמט:

- <שם הודעה>, <סוג הודעה> (<פרמטרים של ההודעה>) (<מה יש בהודעה שהצד השני מחזיר>)

הודעות מהלקוח לשרת:

- הרשמה, post ( שם משתמש, אימייל, סיסמה, מפתח ציבורי של המשתמש)(אם ההרשמה הצליחה).

- התחברות, post (שם משתמש, סיסמה) (אם ההתחברות הצליחה, הסשיין).

- שינוי מפתוח ציבורי של הלקוח, post (סשיין, מפתח ציבורי חדש, חתימה על ההודעה בעזרת המפתח הפרטי החדש) (אם השינוי הצליח).

- יצירת צ'אט עם משתמש, post (שם המשתמש שאיתו יוצרים צ'אט) (אם הצליח, מפתח סימטרי שיצר המשתמש השני מוצפן על ידי המפתח הציבורי של המשתמש הראשון).

- שליחת הודעה למשתמש, post (שם משתמש שאילו שולחים את ההודעה, ההודעה מוצפנת על ידי המפתח הסימטרי של הצ'אט).