**פרויקט אפליקציית מסרים**

**פרוטוקול http**

הודעות:

**חשוב!!!: כל ההודעות יהיו חתומות על ידי המפתח הציבורי של השרת, וגם כל ההודעות יהיו מוצפנות על ידי מפצח סימטרי שהשרת והלקוח יחליפו בינהם.**

פורמט:

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

הודעות מהלקוח לשרת:

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

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

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

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

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