תכנון פרוטוקטול

התחברות:

1.CONN הלקוח שולח לשרת האם קיימת הצפנה ואם כן מה היא.(משתמשים בדיפי )

2. EXCH החלפת מפתחות כאשר קיימת הצפנה

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| קוד הודעה | משמעות | פרמטר 1 | פרמטר 2 | כיוון |
| CONN | התחברות | סוג הצפנה |  | שרת ללקוח |
| EXCH | החלפת מתפתחות |  |  | שרת ללקוח |
| LOGN | התחברות | שם משתמש | סיסמא | שרת ללקוח |
| SEND | שליחת הודעה | שם משתמש יעד | הודעה בבסיס64 | לקוח לשרת |
| BROD | שלחית ברודקאסט | הודעה | הודעה בבסיס64 | שני הכייונים |
| NEWU | להודיע שנכנס משתמש חדש | שם משתמש |  | שרת ללקוח |
| REMU | להודיע שיצא משתמש | שם משתמש |  | שרת ללקוח |
| RECV | קבלת הודעה ממשתמש | שם השולח | ההודעה | שרת ללקוח |

CONN סוג הצפנה:

"none”: ללא הצפנה

“aes”: aes

“rsa”: rsa

פרוטוקול EXCH

לקוח שולח לשרת EXCH  
השרת שולח ללקוח משתנים גלובלים  
ונשלחת הודעה אחת מכל צד עם מספר לפי הפרוטוקול של דיפי( A ו B)

אחריEXCH כל הודעה שנשלחת משני הצדדים תהיה מוצפנת לפי ההצפנה שנבחרה