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 |
| CONN | התחברות | סוג הצפנה |  |
| EXCH | החלפת מתפתחות |  |  |
| LOGN | התחברות | שם משתמש | סיסמא |
| SEND | שליחת הודעה | שם משתמש יעד | הודעה |
| BROD | שלחית ברודקאסט | הודעה |  |
|  |  |  |  |
|  |  |  |  |

CONN סוג הצפנה:

0: ללא הצפנה

1: aes

2: rsa

פרוטוקול EXCH

לקוח שולח לשרת EXCH  
השרת שולח ללקוח משתנים גלובלים

אחריEXCH כל הודעה שנשלחת משני הצדדים תהיה מוצפנת כאשר נבחרה הצפנה