**שיטת ההצפנה:** משתמשים שרוצים לשלוח אחד לשני הודעה צריכים להחליף בינהם מפתח סימטרי.

כדי לעשות זאת, כל אחד מהם יג'נרט זוג מפתחות אסימטריים: ציבורי ופרטי.

המשתמשת שרוצה להתחיל את הצ'אט (נניח אליס) יוצרת מפתח סימטרי ומבקשת מהשרת את המפתח הציבורי של מי שהיא רוצה לשלוח לו את ההודעה (נניח בוב).

היא מצפינה את המפתח הסימטרי עם המפתח הציבורי של בוב, ושולחת לשרת את המפתח המוצפן.

השרת שולח לבוב את המפתח המוצפן ובוב מפענח אותו ושומר אצלו.

לאחר מכן כדי לוודא את זהותה של אליס, בוב מבקש מהשרת את המפתח הציבורי שלה ומצפין את המפתח הסימטרי איתו. הוא שולח את המפתח המוצפן לשרת, ששולח אותו לאליס.

אליס מפענחת את המפתח וכעת הם יכולים להתחיל את השיחה.

כל הודעה שנשלחת בין אליס לבוב ובחזרה מוצפנת בעזרת המפתח הסימטרי, שהשרת לא יודע.

לכן זוהי הצפנת E2EE.

**תהליך הרישום הראשוני:** הלקוח שולח לשרת מספר טלפון מוצפן עם המפתח הציבורי של השרת.

השרת בודק האם מספר הטלפון קיים כבר, אם כן הוא יחזיר שגיאה.

אחרת, הוא יחזיר OK.

הלקוח יג'נרט איזשהו secret ויצפין אותו עם המפתח הציבורי של השרת.

הלקוח ישלח את הsecret המוצפן לשרת.

השרת יחזיר OK, תשלח לי TOTP.

השרת והלקוח יחשבו את הTOTP והלקוח ישלח לשרת את הTOTP שיצא לו.

השרת יבדוק האם הם שווים. אם כן, השרת יאשר את הרישום.

אחרת השרת יחזיר שגיאה.

**אופן יצירת והחלפת המפתחות:** כל לקוח יג'נרט מפתח ציבורי ומפתח פרטי, המפתח הציבורי יישמר בשרת והמפתח הפרטי אצל הלקוח.

לשרת יש מפתח ציבורי גם כן, שהוא קבוע ומובנה באפליקציית הלקוח, ומפתח פרטי שנשמר אצל השרת.

לצורך שליחת הודעות ישתמשו במפתח סימטרי, שמועבר למקבל על ידי הצפנה עם המפתח הציבורי של המקבל.

בטיחות החלפתם היא ממש ממש גבוהה.

**שלמות במובן הרחב**:

TODO:

**מה שומרים בשרת:** לכל לקוח יש מספר טלפון, מפתח ציבורי וsecret עבור הTOTP.

טבלת הודעות: מי שלח את ההודעה, באיזה שעה ואת התוכן המוצפן שלה.