תכנון פרוטוקול

**מהו המשחק?**

משחק ריצה דו־ממדי שבו מספר שחקנים יכולים לרוץ במסלול ולשלוח מכשולים אחד לשני. המשחק כולל:

* שליטה בדמות בתנועה ימין/שמאל/קפיצהslide/
* שליחת מכשולים
* ריצה במסלול עד לסיום
* טבלת מובילים לפי זמן סיום

**אבטחת מידע בפרוטוקול**

הפרוטוקול תומך בהצפנה מבוססת RSA ו-AES:

* כל לקוח מייצר מפתח RSA ציבורי-פרטי.
* הוא שולח לשרת את המפתח הציבורי (GSR).
* השרת שולח מפתח AES מוצפן (FRS).
* כל שאר ההודעות מוצפנות ב-AES (CBC mode).
* **מבנה ההודעות**
* הודעות מורכבות מקוד קבוע באורך 3 תווים, ולאחריו ~ ומידע נוסף.
* המפריד הוא תילדה(~)
* שימוש בtcp by size
* אסינכורני

**זרימת תקשורת בסיסית**

1. **התחברות לשרת:**
   * לקוח מנסה להתחבר (connect\_to\_srv)
   * אם הצליח, ממשיך למסך התחברות/הרשמה
2. **הצפנה:**
   * שליחת מפתח RSA (GSR)
   * קבלת מפתח AES (FRS)
   * המשך תקשורת מוצפנת ב-AES
3. **הרשמה / התחברות:**
   * SGU – הרשמה
   * LGN – התחברות
   * קבלת תשובות בהתאם (SUP, LOG)
4. **ניהול חדרים:**
   * MRS – יצירת חדר
   * GRS – קבלת חדרים
   * JRI – הצטרפות לחדר
5. **משחק פעיל:**
   * UPD – עדכון מיקום שחקן
   * UPO – עדכון מיקום מכשול
   * GOP – קבלת מיקומי שחקנים
   * UPP – עדכון לשאר השחקנים על מיקום שחקן
   * UPL – שליחת זמן סיום
   * ULL – שליחת טבלת מובילים
6. **יציאה:**
   * BYE – ניתוק מהשרת

| **קוד** | **כיוון** | **מטרה** |
| --- | --- | --- |
| LGN | שרת → לקוח | בקשת התחברות עם פרטי התחברות מוצפנים (AES) |
| SGU | שרת → לקוח | בקשת הרשמה עם שם משתמש וסיסמה |
| BYE | שרת → לקוח לקוח → שרת | בקשת ניתוק וסגירת נתוני משתמש |
| GSR | שרת → לקוח | בקשה לקבלת מפתח ציבורי של השרת (RSA) |
| FRS | לקוח → שרת | תגובה עם מפתח AES מוצפן באמצעות RSA |
| MRS | שרת → לקוח  לקוח → שרת | יצירת חדר משחק חדש  תוצאות יצירת חדר |
| GRS | שרת → לקוח לקוח → שרת | בקשת רשימת חדרים קיימים (הנתונים נשלחים עם Pickle) |
| JRI | שרת → לקוח לקוח → שרת | הצטרפות לחדר על פי מזהה  תוצאות כניסה לחדר |
| UPD | שרת → לקוח לקוח → שרת | עדכון מיקום שחקן |
| UPP | לקוח → שרת | שליחת מיקומי שחקנים אחרים |
| UPL | שרת → לקוח | שליחת זמן סיום לעדכון טבלת מובילים |
| ULL | לקוח → שרת | תגובה לעדכון טבלת מובילים (ייתכן שגיאת כתיב בקוד) |
| GOP | שרת → לקוח לקוח → שרת | בקשת מידע על מיקומי שחקנים אחרים |
| UPO | שרת → לקוח לקוח → שרת | עדכון מיקום מכשול |
| SUP | לקוח → שרת | תוצאת הרשמה |
| LOG | לקוח → שרת | תוצאת התחברות |
| ERR | לקוח → שרת | שגיאה כללית או בקלט |