

פרוטוקול לפרוייקט שש-בש – נדב כהן

הוראות: השרת יכניס משתמשים למערכת, ויאפשר למשתמשים לקיים משחקי שש-בש.

1. נושא השירות: פרוטוקול לפרוייקט שש-בש.

2. סוגי ההודעות:

מספר	קוד	כיוון	מהות	הערות ותיאור
1	GTKEY	לקוח -> שרת שרת -> לקוח	שליחת מפתח הצפנה אל הצד השני.	גם השרת וגם הלקוח משתמשים בפעולה זו בעת הקמת שיטת ההצפנה.
2	SGNUP	לקוח -> שרת	להירשם	הלקוח פונה אל השרת בבקשת רישום ושמירת פרטי הלקוח במסד הנתונים.
3	CONCT	לקוח -> שרת	להתחבר	הלקוח פונה אל השרת בבקשת התחברות.
4	SCODE	לקוח -> שרת	לשלוח קוד לאימייל	הלקוח פונה אל השרת על מנת שישלח לו קוד במייל. (בשביל יצירת סיסמא חדשה).
5	VRFCY	לקוח -> שרת	לאשר קוד שנשלח	הלקוח פונה אל השרת על מנת שישאר שהקוד שהקליד נכון. (בשביל יצירת סיסמא חדשה).
6	UPDTE	לקוח -> שרת	לעדכן סיסמא	הלקוח פונה אל השרת על מנת שיעדכן את סיסמתו במסד הנתונים.
7	ANSOK	שרת -> לקוח	הודעת אישור בעת תהליך ההצפנה	תגובת אישור כללית של השרת לגבי בקשה שהלקוח ביקש בתהליך ההצפנה.
8	AVAIL	לקוח -> שרת	האם שיטת ההצפנה זמינה	הלקוח פונה אל השרת בשביל לשאול האם השרת תומך בשיטת ההצפנה שהלקוח בחר.
9	CRTKY	לקוח -> שרת	הלקוח מבקש מהשרת ליצור מפתחות RSA, פנימי וחיצוני.	ההודעה שנשלחת כוללת רק את הבקשה ללא שום מידע נוסף.
10	CRTDH	לקוח -> שרת	הלקוח שולח לשרת את "הפרמטרים" מהם שניהם יצרו מפתחות להצפנה.	הלקוח שולח את הבסיס המשותף ליצירת המפתחות בשני הצדדים.
11	WHRSV	לקוח -> המחשבים ב-LAN (Broadcast)	הלקוח שולח הודעת Broadcast על מנת למצוא את הכתובת של השרת שעליו להתחבר אליו	הלקוח שולח את ההודעה לכתובת 255.255.255.255 וכך ההודעה מגיעה לכל מחשב ב-subnet.

פרוטוקול לפרוייקט שש-בש – נדב כהן

מספר	קוד	כיוון	מהות	הערות ותיאור
12	SRVAT	שרת *UDP -< לקוח	שרת (UDP) מחזיר ללקוח את הכתובת של השרת שהלקוח צריך להתחבר אליו	השרת מקבל את הכתובת של הלקוח ושולח לו את הכתובת באופן פרטי
13	READY	לקוח -< שרת	לקוח אומר לשרת שהוא מוכן למשחק	ללא.
14	CANCL	לקוח -< שרת	לקוח מבטל את זה שהוא מוכן למשחק	ללא.
15	LOGED	שרת -< לקוח	הודעת אישור לכניסת לקוח	ללא.
16	SIGNED	שרת -< לקוח	הודעת אישור ללקוח על ההרשמה	ללא.
17	VRFYD	שרת -< לקוח	הודעת אישור ללקוח על הקוד שכתב (במטרה לקבוע סיסמא חדשה)	ללא.
18	SENTM	שרת -< לקוח	הודעת אישור ללקוח על כך שאימייל לקביעת סיסמא חדשה נשלח	ללא.
19	UPDTD	שרת -< לקוח	הודעת אישור ללקוח על כך שסיסמתו עודכנה	ללא.
20	LISTD	שרת -< לקוח	הודעת אישור ללקוח על כך שהלקוח מעוניין להתחיל משחק	ללא.
21	CACLD	שרת -< לקוח	הודעת אישור ללקוח על כוונתו לביטול התחלת משחק	ללא.
22	EXTLG	שרת -< לקוח	הודעת אישור ללקוח על יציאה מהמערכת	ללא.
23	LGOUT	לקוח -< שרת	הלקוח מעוניין לצאת מהמערכת	ללא.
24	FUNCT	שרת -< לקוח לקוח -< שרת	שליחת הודעות הקשורות למשחק.	רשימת תת נושאים של הודעה זו מפורטת בהמשך. כמו כן, השגיאות שנשלחות במהלך המשחק נמצאות תחת רשימת השגיאות.

פרוטוקול לפרוייקט שש-בש – נדב כהן

בהודעות מסוג FUNCT:

נושא (subject)	כיוון	מהות	תיאור והערות
MATCH	שרת -> לקוח	התחלת המשחק	בהודעות מסוג FUNCT לכל הודעה יש שדות שונים. למשל: <ul style="list-style-type: none"> • Subject • Game over • Opponent • Color • Turn
GAME_STATE	שרת -> לקוח	מצב המשחק	
DICE_RESULT	שרת -> לקוח	תוצאת הקוביות	
HIGHLIGHT	שרת -> לקוח	הדגשת/הצגת המקומות אליהם יכול השחקן להזיז את הכלי (checker)	
CHECKER_MOVE	שרת -> לקוח	מהלך תנועה של כלי	
CHECKER_CAPTURED	שרת -> לקוח	אכילה של כלי	
EXIT	שרת -> לקוח	אישור יציאה מהמשחק	
ROLL_DICE	לקוח -> שרת	גלגול קוביות	
SELECT_PT	לקוח -> שרת	בחירה של כלי	
MOVE_TO	לקוח -> שרת	הזזה של כלי	
EXIT	לקוח -> שרת	הלקוח מעוניין לצאת מהמשחק	

3. מבנה ההודעות:

מודולארי (בחלקים) – לרוב טקסטואלי: באמצעות תווי ASCII. לסוגי ההודעות, GETKY, CRTDH תוכן המידע יהיה בינארי (bytes) ולא טקסטואלי.

לפני הצפנת המידע (שלב הקמת התקשורת):
 הלקוח שולח: "WHRVS" בלבד (5 בתים).
 כתשובה, השרת UDP שולח:

SRVAT		IP		Port
5 בתים	1 בית	גודל משתנה בהתאם לכתובת ה IP של השרת (בין 7 ל 15 בתים)	1 בית	בין 4 ל 5 בתים
קוד ההודעה	סימן מפריד		סימן מפריד	הפורט של השרת

פרוטוקול לפרוייקט שש-בש – נדב כהן

בעת הצפנת המידע בין השרת ללקוח, בהודעות יהיו השדות הבאים:

Size Of Message	Message Code		Message Content
2 בתים	5 בתים	1 בית	גודלו משתנה
גודל ההודעה (לא כולל את אורך השדה הזה)	קוד ההודעה	סימן מפריד	בהתאם לסוג ולתוכן ההודעה.
			תוכן ההודעה
			(לא יעלה על 60,000 בתים: לצורך נוחיות ובהתאם לאורך מקסימלי שניתן לתאר בשני בתים)

במקרה של ההודעה מסוג CRTKY, אין שדה תוכן ולכן גם לא קיים את הסימן המפריד.
Message Content יהיה בבתים במקרים של שליחת מידע (GETKY,CRTDH).

לאחר הצפנת המידע בין השרת ללקוח, בהודעות יהיו השדות הבאים:

Size Of Message	IV	Encrypted Message (לאחר ההצפנה)		
2 בתים גודל ההודעה (לא כולל את אורך השדה הזה)	16 בתים initial vector (לשימוש הצפנת AES)	Message Code		Message Content
		5 בתים קוד ההודעה	1 בית סימן מפריד	גודלו משתנה בהתאם לסוג ולתוכן ההודעה. תוכן ההודעה
		(לא יעלה על 60,000 בתים: לצורך נוחיות ובהתאם לאורך מקסימלי שניתן לתאר בשני בתים)		

הערה: הסימן המפריד (|) לא יופיע בתוכן ההודעה.

בהודעות מסוג UPDTE ,VRFYC ,SGNUP,CONCT
השדות בהתאם מופרדים **בין** | Pipe symbol.

UPDTE	Username/email	Password	Verify Password	
VRFYC	Username/email	Code		
SGNUP	Username	Password	Verify Password	Email
CONCT	Username	Password		

פרוטוקול לפרוייקט שש-בש – נדב כהן

4. צורת המענה של השרת: א-סינכרונית.

יש תלות בין ההודעות:

- הודעות 11,12 נשלחות פעם אחת, ראשית הודעה 11 מהלקוח (WHRV), ולאחר מכן תשובת שרת UDP* בהודעה מספר 12 (SRVAT), לצורך הקמת התקשורת בין השרת ללקוח.

- הודעות שקשורות להצפנה: CRTKY,AVAIL,GETKY,CRTDH
אותן הלקוח והשרת שולחים רק בזמן תהליך בחירת סוג ההצפנה.

- הודעות מסוג FUNCT: נשלחות רק בעת משחק.
כלומר לאחר שהלקוח קיבל הודעה מסוג זה, כאשר הנושא שלה הוא MATCH
ההודעה האחרונה שתישלח מסוג זה היא הודעת FUNCT שתשלח מהשרת, כאשר הנושא שלה הוא EXIT.

- הודעות הקשורות למערכת הכניסה (הודעות 7-2, 23-13) לא ישלחו בעת מצב משחק.

5. רשימת שגיאות:

מספר	קוד	כיוון	מהות	הערות ותיאור
1	ERR01	שרת -> לקוח	שגיאה כללית בעת התקשורת/ עיבוד בקשת המשתמש.	לצד ההודעה מידע נלווה.
2	ERR02	שרת -> לקוח	השרת לא תומך בשיטת ההצפנה שהלקוח ביקש	לצד ההודעה מידע נלווה.
3	ERR03	שרת -> לקוח	התחברות לא הצליחה	לצד ההודעה מידע נלווה.
4	ERR04	שרת -> לקוח	בעיה בעת שליחת הקוד לאימייל (לקביעת סיסמא חדשה)	לצד ההודעה מידע נלווה.
5	ERR05	שרת -> לקוח	בעיה בעת שליחת האימייל (ובתוכו הקוד בתהליך קביעת הסיסמא החדשה)	לצד ההודעה מידע נלווה.

פרוטוקול לפרוייקט שש-בש – נדב כהן

מספר	קוד	כיוון	מהות	הערות ותיאור
6	ERR06	שרת -> לקוח	הקוד שהלקוח שלח לא נכון	לצד ההודעה מידע נלווה.
7	ERR07	שרת -> לקוח	בעיה ברישום משתמש, הסיסמאות שהוזנו לא זהות	לצד ההודעה מידע נלווה.
8	ERR08	שרת -> לקוח	בעיה ברישום משתמש, לפחות סיסמא אחת ריקה	לצד ההודעה מידע נלווה.
9	ERR09	שרת -> לקוח	בעיה עם חידוש הסיסמא	לצד ההודעה מידע נלווה.
10	ERR10	שרת -> לקוח	בעיה ברישום המשתמש, לא ניתן להוסיף את המשתמש	לצד ההודעה מידע נלווה.
11	ERR11	שרת -> לקוח	השרת קיבל מידע בבתים, שלא הצליח לפרסר אותם	לצד ההודעה מידע נלווה.
<p align="center">הודעות שגיאה שמספרן 50 ומעלה קשורות לבעיות הקשורות למשחק. הודעות אלה נכללות תחת הנושא FUNCT, אך הן הודעות שגיאה.</p>				
12	ERR50	שרת -> לקוח	לא תור הלקוח לשחק	לצד ההודעה מידע נלווה.
13	ERR51	שרת -> לקוח	הקוביות כבר גולגלו	לצד ההודעה מידע נלווה.
14	ERR52	שרת -> לקוח	צריך להזיז קודם את הכלים שנאכלו	לצד ההודעה מידע נלווה.
15	ERR53	שרת -> לקוח	לחיצה במיקום לא נכון	לצד ההודעה מידע נלווה.
16	ERR54	שרת -> לקוח	אין כלי במיקום שנלחץ	לצד ההודעה מידע נלווה.
17	ERR55	שרת -> לקוח	אין מהלכים לכלי שנבחר	לצד ההודעה מידע נלווה.
18	ERR56	שרת -> לקוח	הכלי חייב להיכנס לבית של היריב	לצד ההודעה מידע נלווה.
19	ERR57	שרת -> לקוח	המרחק לא מתאים לביצוע המהלך	לצד ההודעה מידע נלווה.
20	ERR58	שרת -> לקוח	היעד חסום בידי היריב	לצד ההודעה מידע נלווה.
21	ERR59	שרת -> לקוח	לא ניתן להוציא כלים מהלוח (bear off) לפני שכל הכלים נמצאים בבית	לצד ההודעה מידע נלווה.
22	ERR60	שרת -> לקוח	לא ניתן להוציא כלי מנקודה זו	לצד ההודעה מידע נלווה.

מבנה השגיאות זהה למבנה ההודעות המוצפנות. מבנה ERR02 זהה למבנה ההודעות שלא מוצפנות.

פרוטוקול לפרוייקט שש-בש – נדב כהן

6. דוגמאות להודעות בתקשורת:
לצורך נוחות, אציג את ההודעות לפי התבנית הבאה:

Size Of Message	Message Code	Message Content
גודל ההודעה (לא כולל את אורך השדה הזה)	קוד ההודעה	סימן מפריד תוכן ההודעה

(התבנית לא מיועדת להודעות הקמת התקשורת. הודעות מוצפנות יוצגו כפי שהן לאחר ההצפנה. גודל ההודעה יהיה גודל ההודעה המוצפנת (ללא iv).)
דוגמאות להודעות בתקשורת:

מספר	דוגמא
1	WHRSV
2	SRVAT 10.100.102.58 55655
3	\0x00\0x09AVAIL RSA
4	\0x00\0x09ANSOK yes
5	\0x00\0x05CRTKY
6	\0x01\0xC3GETKY -----BEGIN PUBLIC KEY----- MIIBIjANBgqhki G9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6wLgxm6ZCeQtzjl5f0rF i/WcJtWvP1 mNonHD8dfYHoN7Wd6AwMtDFYUbs5Rdool7LS2beGfIPaq5QwaBzoxl v/uHd xDwXFBf4Xu96M4fKSPKkBbnqRiV1bNhAeM4te2FDjS8HJhkBUxOChPMFrsc S 8JIZY5bvDtj/0tKea7Jz37lmk/gaxn9a8Dr+iMBqB1zpOjwPwLTXOWhMpnDp9K1 8ES/aU4Sf8PBAyWQm/UfgpbHhjmF0UxZkuCkLQpuDriNjJaxZ1NwQdVzeudgz L00 xOaqLvnAo/fFX87YDw8ynCu4CONkgDH6ffQkm9OJDFxl3P0YBzZBCVimE d0wmI9Y XQIDAQAB -----END PUBLIC KEY-----
7 (ייצוג hex)	\0x02\0x06GETKY d0691bc5a3b550137512862d41751c8de09868 585e7bab32cd9b578ae5d45de999a3f7263d2355c56cf95acd653d40357efd14 b2c40760689a505370eff8ee6ed9187930e3f91c575002fc00fecdd424c6b259c 3b6d381d1c1fc2437c23b410eb8335201f63eca42b34af554fe52a300e113373 3acb847d83396f9cf00ccbe0734bf6cdfefbd6658bf9d2f451ba8ec9da914baf5 4b0dee36c5538e23e6da69d80044c325e22156533b3dd63648f40f52778b0eb 358d8413e5af7d2c52d4deaf0b338a3080558646b4f04780f36723b3b3bece3 17507d62a90ad750e32232ac21104a89e2ab8bd61470411a5a53eec0c41456 767569a4433afcd9c31e8267d5
8	\0x00\0x09ANSOK yes
9	\0x00\0x14CONCT player3 ANDREW
10	\0x00\0x17ERR03 Connection Failed
11	\0x00\0x13VRFYC ANDREW 133144
12	\0x00\0x18ERR01 An error occurred.
13	\0x00\0x13VRFYC ANDREW 133155
14	\0x00\0x16VRFYD Code is Correct!
15	\0x00\0x1DSENTM Email sent successfully

פרוטוקול לפרוייקט שש-בש – נדב כהן

דוגמא	מספר
\0x00\0x0CSCODE ANDREW	16
\0x00\0x23ERR06 Error with verification code!	17
\0x00\0x15CONCT ANDREW mishmish	18
\0x00\0x18LOGED Connection Succeed	19
\0x00\0x0BREADY start	20
\0x00\0x08LISTD ok	21
\0x00\0x30FUNCT subject=MATCH color=White opponent=player3	22
\0x00\0x23FUNCT subject=GAME_STATE turn=White	23
\0x00\0x23FUNCT subject=ROLL_DICE color=White	24
\0x00\0x27FUNCT subject=DICE_RESULT num1=1 num2=1	25
\0x00\0x23FUNCT subject=GAME_STATE turn=White	26
\0x00\0x28FUNCT subject=SELECT_PT color=White pt=6	27
\0x00\0x25FUNCT subject=HIGHLIGHT pt=6 points=5	28
\0x00\0x33FUNCT subject=MOVE_TO color=White from_pt=6 to_pt=5	29
\0x00\0x60FUNCT subject=GAME_STATE info=Three consecutive doubles - Yellow wins! turn=White game_over=True	30
\0x00\0x0CLGOUT logout	31
\0x00\0x08EXTLG ok	32