

**נושא : מנגנון הגנה תיקיות**

**שם התלמיד: יונתן חרמץ**

**ת"ז: 207017146**

**בית הספר: תיכון חדש הרצליה**

**שמות המורים: מיכאל צ'רנובילסקי**

**מועד הגשה:14.11.15**

1. **הקדמה**
   1. **מטרה-**

המטרה המרכזית של המוצר היא למנוע מגורם זר לקבל גישה לתיקיות רגישות הנמצאות במחשב.בעזרתהמוצר, המשתמש יוכל להגן על תיקיות חשובות ופרטיות במחשב שלו, או תיקייה משותפת שקיימת בכמה מחשבים.

* 1. **המוצר-**

השרת שמחובר למספר לקוחות מחובר גם לבסיס נתונים אשר נמצאים בו פרטי שם משתמש וסיסמה אשר שיכים לכל אחד מהלקוחות. בעת ניסיון כניסה לתיקייה רגישה, המערכת תבקש מהמשתמש לאמת את נתוני הגישה שלו. במקרה והנתונים שהוזנו לא נכונים או המשתמש התמהמה יתר על המידה בעת הכנסת הנתונים- התיקייה הרגישה תוצפן והמחשב יפסיק להגיב למשתמש.

הצפנת התיקיות תתבצע על ידי מפתח אשר יתקבל מהשרת, ופיצוח התיקייה והמשך פעולת המחשב יתבצעו רק לאחר אישור מהשרת. אותה פעולה של הצפנת התיקייה ואי תגובת המחשב תתבע גם בכל שאר הלקוחות של השרת אשר ברשותם אותה תיקייה רגישה או נמצאים ברשת משותפת עם המחשב שבו התרחש ניסיון הפריצה- בכדי למנוע פריצה של המחשב דרך מחשב אחר הנמצא באותה רשת.

* 1. **קישור למסמכים קודמים-**

[מסמך אפיון](file:///C:\Users\User\Downloads\הצעת%20פרוייקט%20סייבר%20יונתן%20חרמץ%20(1).docx)

* 1. **הגדרות-**

GUI– ממשק גרפי

PIPE– צינור תקשורת בין תוכנות בתוך המחשב. לא ניתן להשתמש בצינור לתקשורת ברשת.

1. **ארכיטקטורת המערכת**
   1. **מבט על**

מודול תקשורת- אחראי על כל התקשורת בין השרת ללקוחות.

מודול הצפנת מידע- אחראי על הצפנה סימטרית של כל המידע העובר בתקשורת שבין השרת ללקוח.

**שרת:**

מודול תקשורת- אחראי על כל התקשורת בין השרת ללקוחות.

מודול הצפנת מידע- אחראי על הצפנה סימטרית של כל המידע העובר בתקשורת שבין השרת ללקוח.

מודול יצירת מפתחות הצפנה- אחראי על יצירת מפתחות הצפנה לשם הצפנה אי-סימטרית של התיקיות הרגישות במחשב הלקוח.

מודול ניהול מאגר נתונים-אחראי על הכנסת משתמש למאגר הנתונים בעת הרשמה ועל אימות נתוני המשתמש בעת ההרשמה עם מאגר הנתונים.

מודול נגישות למאגר נתונים- אחראי על הוספת נתונים למאגר, שאילתות וקישור עם מודול ניהול המאגר.

**לקוח:**

מודול תקשורת- אחראי על כל התקשורת בין השרת ללקוחות.

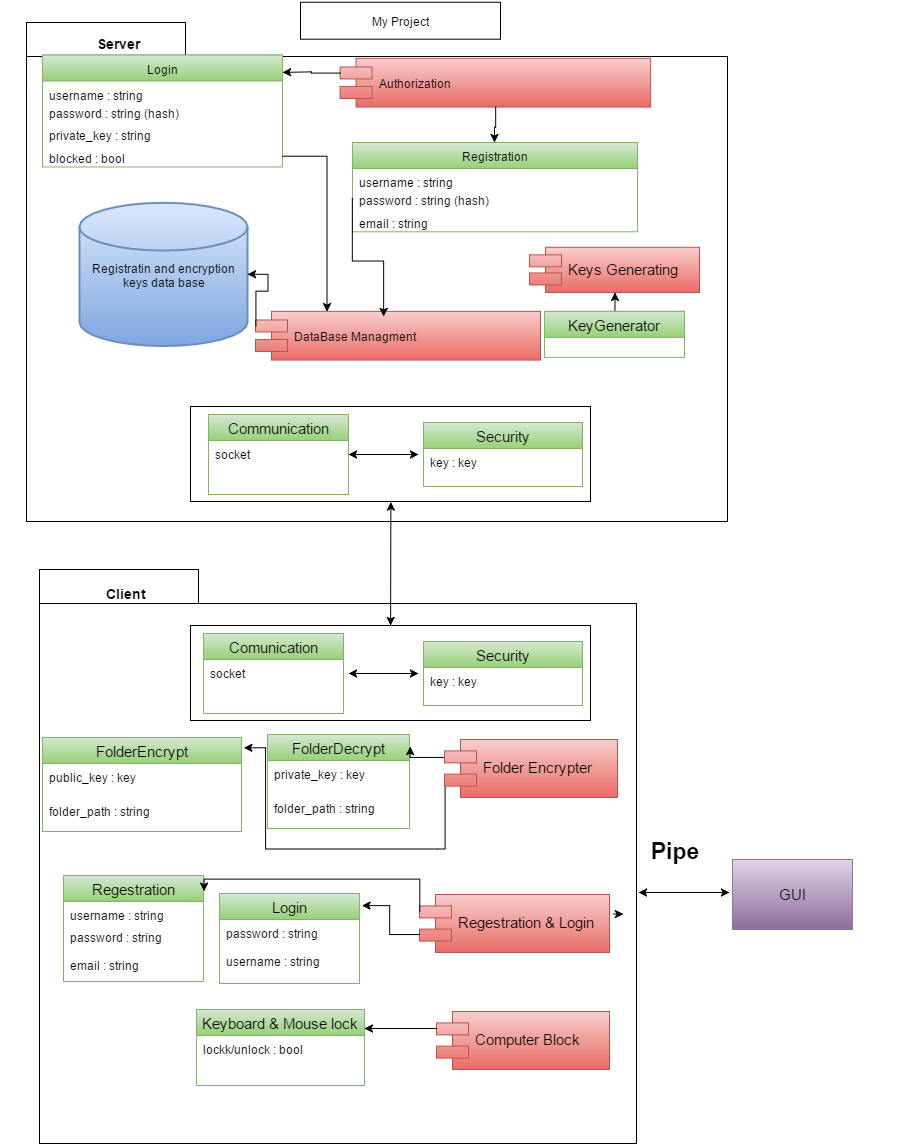
מודול הצפנת מידע- אחראי על הצפנה סימטרית של כל המידע העובר בתקשורת שבין השרת ללקוח.

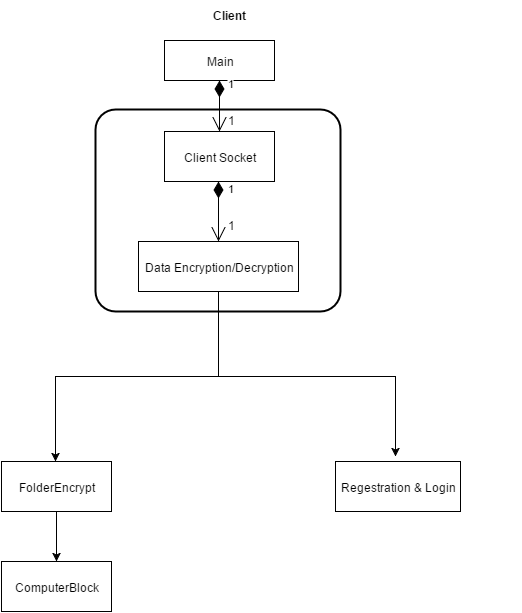
מודול הרשמה התחברות- אחראי על תהליכי ההרשמה וההתחברות של הלקוח למערכת.

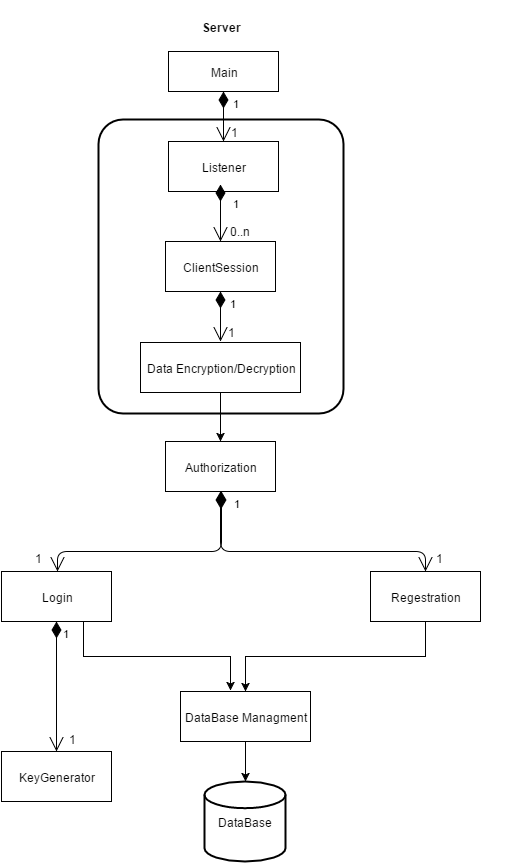
מודול הצפנת ופיצוח תיקיות- אחראי על הצפנת ופיצוח התיקיות בעזרת המפתח שהתקבל מהשרת.

מודול חסימת מחשב- אחראי על חסימת המחשב ומניעה של המשך שימוש של הלקוח הלא מורשה במחשב.

ממשק משתמש גרפי- מאפשר ללקוח להירשם ולהתחבר למערכת בצורה ויזואלית נוחה.

* 1. **פירוט רכיבי המערכת**

****

****

**שרת:**

מחלקת KeyGenerator

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self) | יוצר אובייקט KeyGenerator |
| Key generate(bits) | מקבלת מספר בטים ומחזירה מפתח RSA |

מחלקת S\_ Registration

|  |  |
| --- | --- |
| הפעולה | תיאור |
| string hash(password) | מקבלת סיסמה ומצפינה אותה בhash |
| \_\_init\_\_(self,uname,hashed,email) | יוצרת אובייקט מסוג registration המכיל שם משתמש, סיסמה מוצפנת וכתבות מייל. |

מחלקת S\_Login

|  |  |
| --- | --- |
| הפעולה | תיאור |
| string hash(password) | מקבלת סיסמה ומצפינה אותה בhash |
| \_\_init\_\_(self,uname,hashed,blocked) | יוצרת אובייקט מסוג login המכיל שם משתמש, סיסמה מוצפנת, ודגל המסמל אם המחשב חסום או לא |
| string Error() | מחזירה הודעת שגיאה אם ההתחברות נכשלה. |

מחלקת DB\_managment

|  |  |
| --- | --- |
| הפעולה | תיאור |
| void Add(registration) | מוסיפה משתמש חדש למאגר הנתונים. |
| bool Exist(login) | מחזירה אמת אם נתוני המשתמש שהוזנו בעת התחברות נמצאים במאגר הנתונים ושקר אם לא. |
| bool compare(login, registration) | מקבלת משתנה registration ומחזירה אמת אם נתוני המשתמש זהים לזה של login |

**לקוח:**

מחלקת FolderEncrypt

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self, public\_key, path) | יוצרת אובייקט FolderEncrypt |
| void fileEnc(public\_key, path) | מקבלת מפתח ציבורי וכתובת תיקייה ומצפינה את התיקייה. |

מחלקת FolderDecrypt

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self, private\_key, path) | יוצרת אובייקט FolderDecrypt |
| void fileDec(private\_key,path) | מקבלת מפתח פרטי וכתובת תיקייה ומפצחת את התיקייה. |

מחחלקת Block

|  |  |
| --- | --- |
| הפעולה | תיאור |
| void block(bool toblock) | מקבלת משתנה בוליאני לפיו הפעולה חוסמת או מבטלת חסימה של מחשב. |

מחלקת C\_Login

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self, username, password) | יוצרת אובייקט מסוג Login |

מחלקת C\_Registration

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self, username, password, email) | יוצרת אובייקט מסוג Registration |

**משותף ללקוח ולשרת:**

מחלקת Communication

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self, socket) | יוצר אובייקט מסוג Communication |
| String receive() | מקבלת מידע דרך socket |
| Void send(data) | שולחת מידע דרך socket |

מחלקת Security

|  |  |
| --- | --- |
| הפעולה | תיאור |
| \_\_init\_\_(self,key) | יוצר אובייקט מסוג Security |
| String encrypt(data, key) | מקבלת מידע ומפתח ומצפינה באמצעות המפתח את המידע. |
| String decrypt(enc\_data,key) | מקבלת מידע מוצפן ומפתח ומפצחת באמצעות המפתח את המידע המוצפן. |
| Key Generator() | פעולה שמחזירה מפתח הצפנה. |

1. **עיצוב נתונים ופרוטוקולים**

