

**שם בית ספר**: עירוני י"ד

**נושא העבודה**: לימוד הצפנת עמודות

**שם תלמיד**: טלי עמרם

**תז תלמיד**: 325014777

**שם מנחה**: מיכאל צ'רנובילסקי

**הפרויקט בוצע במסגרת התכנית "מדעי המחשב, אקדמיה ותעשיה", מכון דוידסון לחינוך מדעי, מכון ויצמן למדע.**

**תאריך הגשה:**

Table of Contents

[מבוא 3](#_Toc40656252)

[מבנה הפרוייקט 8](#_Toc40656253)

[מדריך למשתמש 16](#_Toc40656254)

[מדריך למפתח 23](#_Toc40656255)

[ריפלקציה 24](#_Toc40656256)

[ביבליוגרפיה 25](#_Toc40656257)

# מבוא

המערכת שפיתחתי מקבלת משפט מהמשתמש, ומצפינה אותו בעזרת הצפנת עמודות (rectangular transposition Encryption and decryption). ההצפנה תתבצע בצורה וויזואלית ונוחה כך שהמשתמשים יוכלו ללמוד כיצד שיטת ההצפנה עובדת וללמוד את יסודות ההצפנה. המשפט המוצפן נשלח ממשתמש אחד לשני. המשתמש השני מקבל את ההודעה המוצפנת והמחשב מפענח את ההודעה ומציג זאת בצורה ויזואלית על המסך. הלימוד מתבצע דרך משחק בין המשתמשים של שליחת ההודעות.

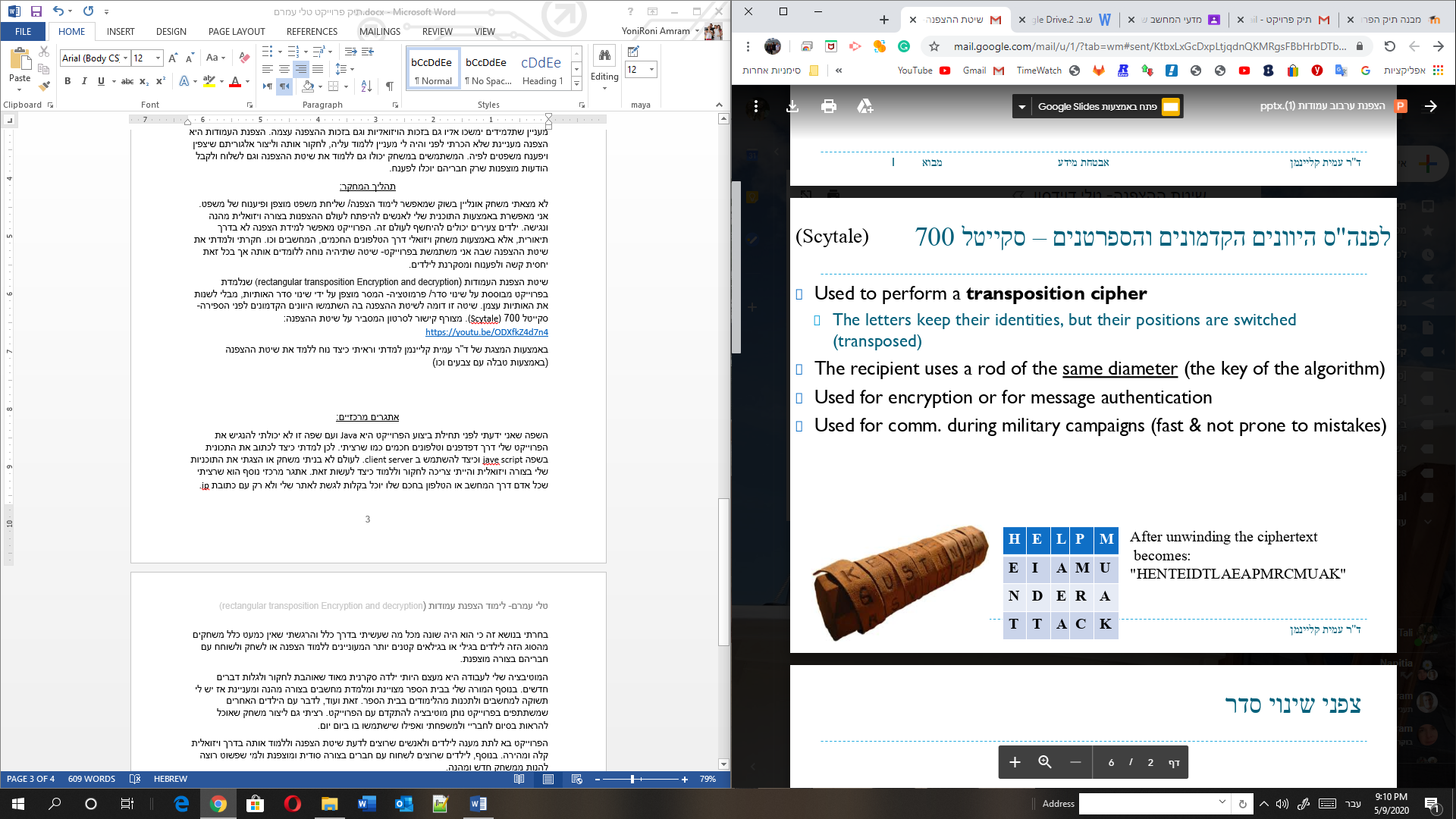
בפרק המבוא אתאר את הרציונל לפרוייקט. האתגרים העיקריים שאיתם התמודדתי מבחינת אלגוריתם, שפות תכנות וסביבות עבודה. לאחר מכן אתאר את התכנון של המערכת. בהמשך אתאר מדריך למשתמש ולמפתח ולסיום אתאר מה למדתי מביצוע הפרויקט.

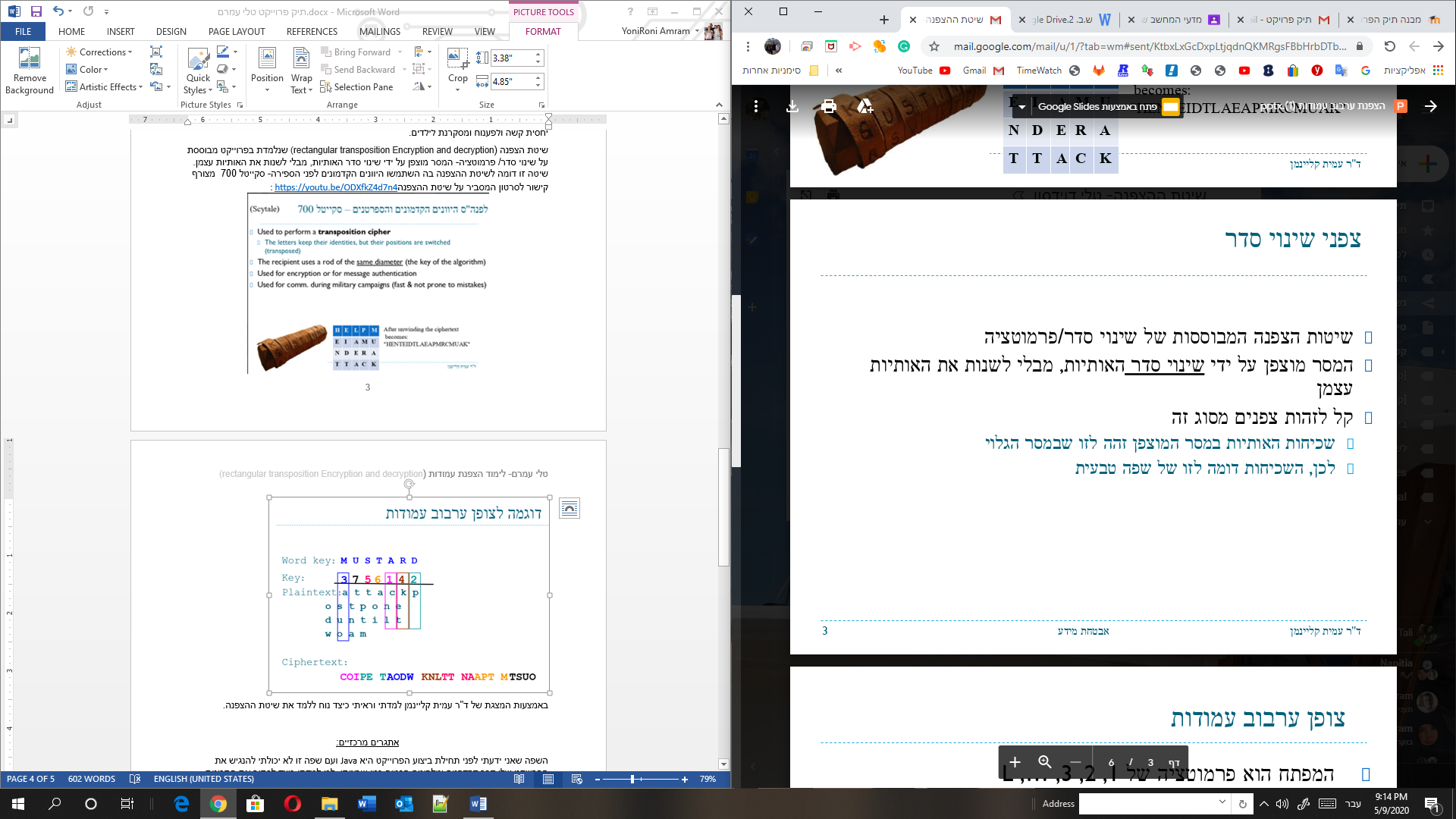
הרקע לפרוייקט:

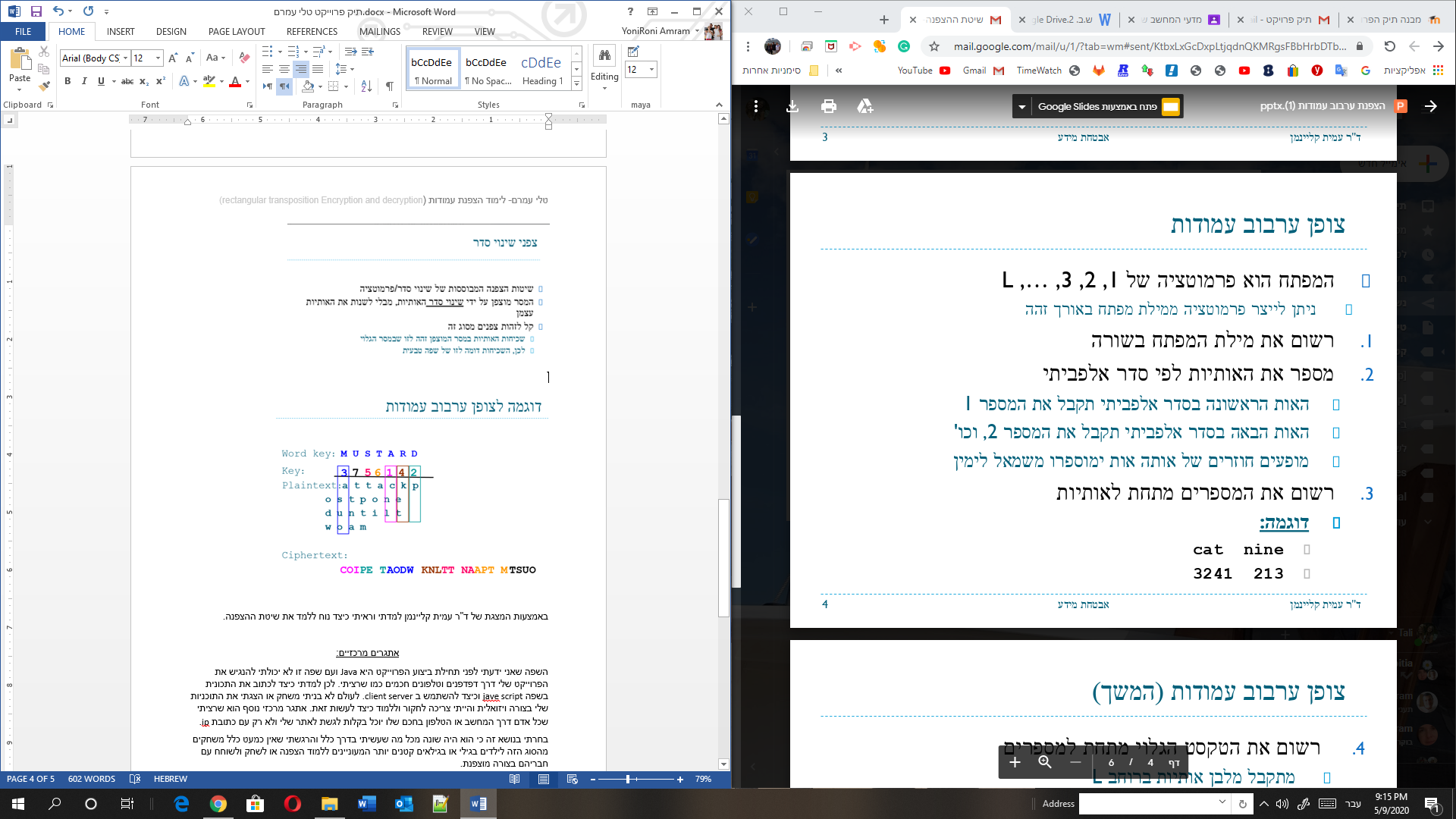
בחרתי לבצע את פרוייקט זה מכיוון שעיניין אותי ללמוד שפה חדשה שמאפשרת הצגה ויזואלית דרך כל דפדפן אפשרי, גם בטלפונים נידיים וגם במחשבים שונים. בבית הספר אני לומדת רק ג'אווה ודברים בסיסייים ורציתי ללמוד שפה שתאפשר לי להכין משחק משלי. כמו כן, רציתי ליצור משחק מעניין שתלמידים ימשכו אליו גם בזכות הויזואליות וגם בזכות ההצפנה עצמה. הצפנת העמודות היא הצפנה מעניינת שלא הכרתי לפני והיה לי מעניין ללמוד עליה, לחקור אותה וליצור אלגוריתם שיצפין ויפענח משפטים לפיה. המשתמשים במשחק יכולו גם ללמוד את שיטת ההצפנה וגם לשלוח ולקבל הודעות מוצפנות שרק חבריהם יוכלו לפענח.

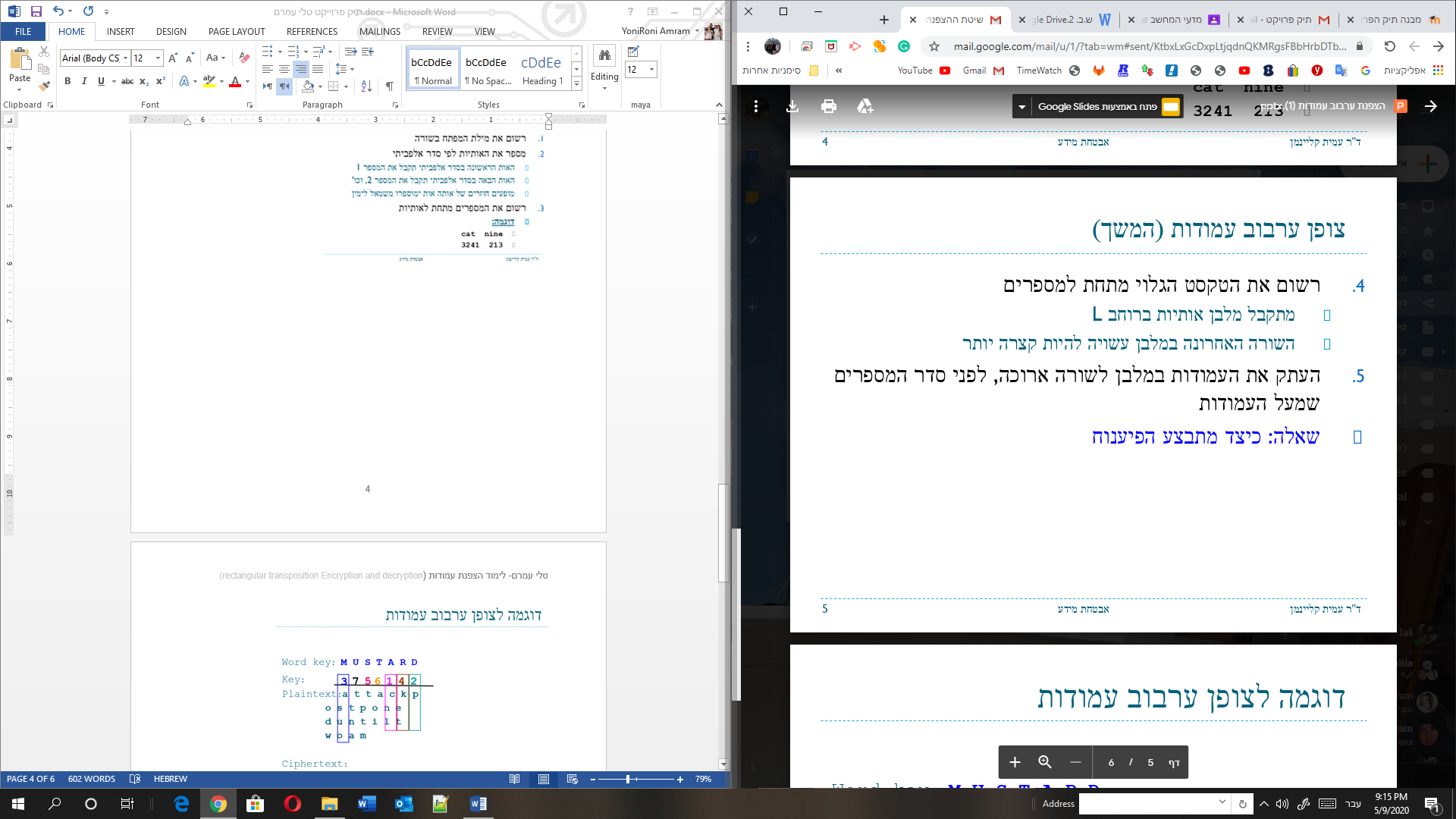
תהליך המחקר:

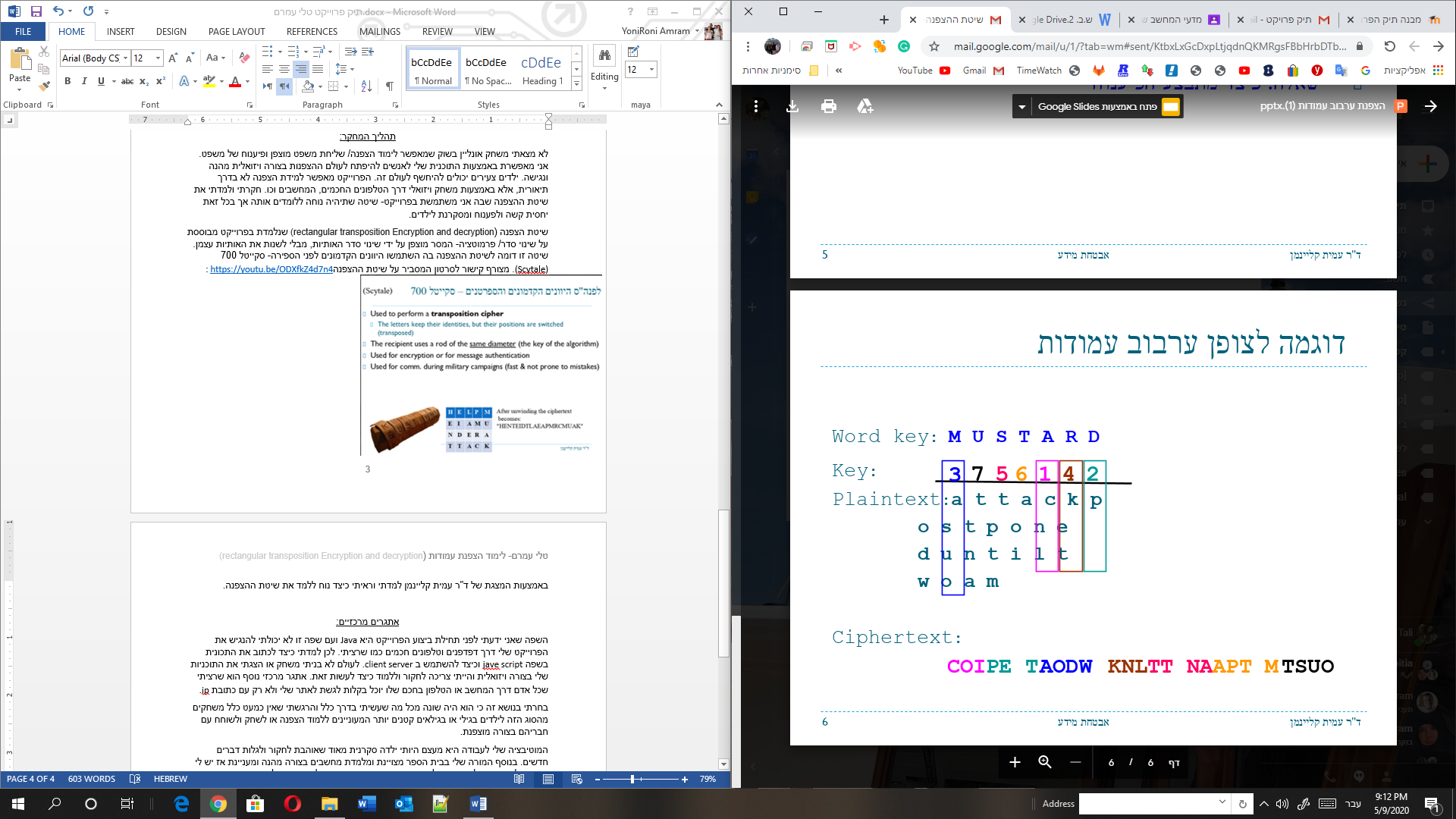
לא מצאתי משחק אונליין בשוק שמאפשר לימוד הצפנה/ שליחת משפט מוצפן ופיענוח של משפט. אני מאפשרת באמצעות התוכנית שלי לאנשים להיפתח לעולם ההצפנות בצורה ויזואלית מהנה ונגישה. ילדים צעירים יכולים להיחשף לעולם זה. הפרוייקט מאפשר למידת הצפנה לא בדרך תיאורית, אלא באמצעות משחק ויזואלי דרך הטלפונים החכמים, המחשבים וכו. חקרתי ולמדתי את שיטת ההצפנה שבה אני משתמשת בפרוייקט- שיטה שתיהיה נוחה ללומדים אותה אך בכל זאת יחסית קשה ולפענוח ומסקרנת לילדים.

שיטת הצפנה (rectangular transposition Encryption and decryption) שנלמדת בפרוייקט מבוססת על שינוי סדר/ פרמוטציה- המסר מוצפן על ידי שינוי סדר האותיות, מבלי לשנות את האותיות עצמן. שיטה זו דומה לשיטת ההצפנה בה השתמשו היוונים הקדמונים לפני הספירה- סקייטל 700 מצורף קישור לסרטון המסביר על שיטת ההצפנה: <https://youtu.be/ODXfkZ4d7n4>









באמצעות המצגת של ד"ר עמית קליינמן למדתי וראיתי כיצד נוח ללמד את שיטת ההצפנה.

אתגרים מרכזיים:

השפה שאני ידעתי לפני תחילת ביצוע הפרוייקט היא Java ועם שפה זו לא יכולתי להנגיש את הפרוייקט שלי דרך דפדפנים וטלפונים חכמים כמו שרציתי. לכן למדתי כיצד לכתוב את התכונית בשפה jave script

לעולם לא בניתי משחק או הצגתי את התוכניות שלי בצורה ויזואלית והייתי צריכה לחקור וללמוד כיצד לעשות זאת.

הייתי צריכה ללמוד כיצד להשתמש ב client server.

אתגר מרכזי נוסף הוא שרציתי שכל אדם דרך המחשב או הטלפון בחכם שלו יוכל בקלות לגשת לאתר שלי ולא רק עם כתובת ip.

בחרתי בנושא זה כי הוא היה שונה מכל מה שעשיתי בדרך כלל והרגשתי שאין כמעט כלל משחקים מהסוג הזה לילדים בגילי או בגילאים קטנים יותר המעוניינים ללמוד הצפנה או לשחק ולשוחח עם חבריהם בצורה מוצפנת. לכן גם הייתי צריכה ללמוד את שיטת ההצפנה שאבחר ללמד ולבדוק האם היא עובדרת רק באנגלית או גם בעברית והאם היא תעניין ילדים ותיהיה מתאימה למשחק שבחרתי לעשות.

המוטיבציה שלי לעבודה היא מעצם היותי ילדה סקרנית מאוד שאוהבת לחקור ולגלות דברים חדשים. בנוסף המורה שלי בבית הספר מצויינת ומלמדת מחשבים בצורה מהנה ומעניינת אז יש לי תשוקה למחשבים ולתכנות מהלימודים בבית הספר. זאת ועוד, לדבר עם הילדים האחרים שמשתתפים בפרוייקט נותן מוטיבציה להתקדם עם הפרוייקט. רציתי גם ליצור משחק שאוכל להראות בסיום לחבריי ולמשפחתי ואפילו שישתמשו בו ביום יום.

הפרוייקט בא לתת מענה לילדים ולאנשים שרוצים לדעת שיטת הצפנה וללמוד אותה בדרך ויזואלית קלה ומהירה. בנוסף, לילדים שרוצים לשחוח עם חברים בצורה סודית ומוצפנת ולמי שפשוט רוצה להנות ממשחק חדש ומהנה.

הצגת פתרונות לבעיה:

כדי ללמוד את השפה שבה השתמשתי, חקרתי וחיפשתי מידע רב על השפה jave script והצלחתי ללמוד כיצד לתכנת בעזרתה. מצאתי ספריות שונות ומגוונות באינטרנט כמו p5js שעזרו לי לתכנת בצורה גרפית ונוחה את המשחק. לפני כן, לא הכרתי את הסיפריות שנמצאות באינטרנט ולא בניתי אתר כלשהו משל עצמי. התהליך היה לי מסקרן, קשה ומספק.

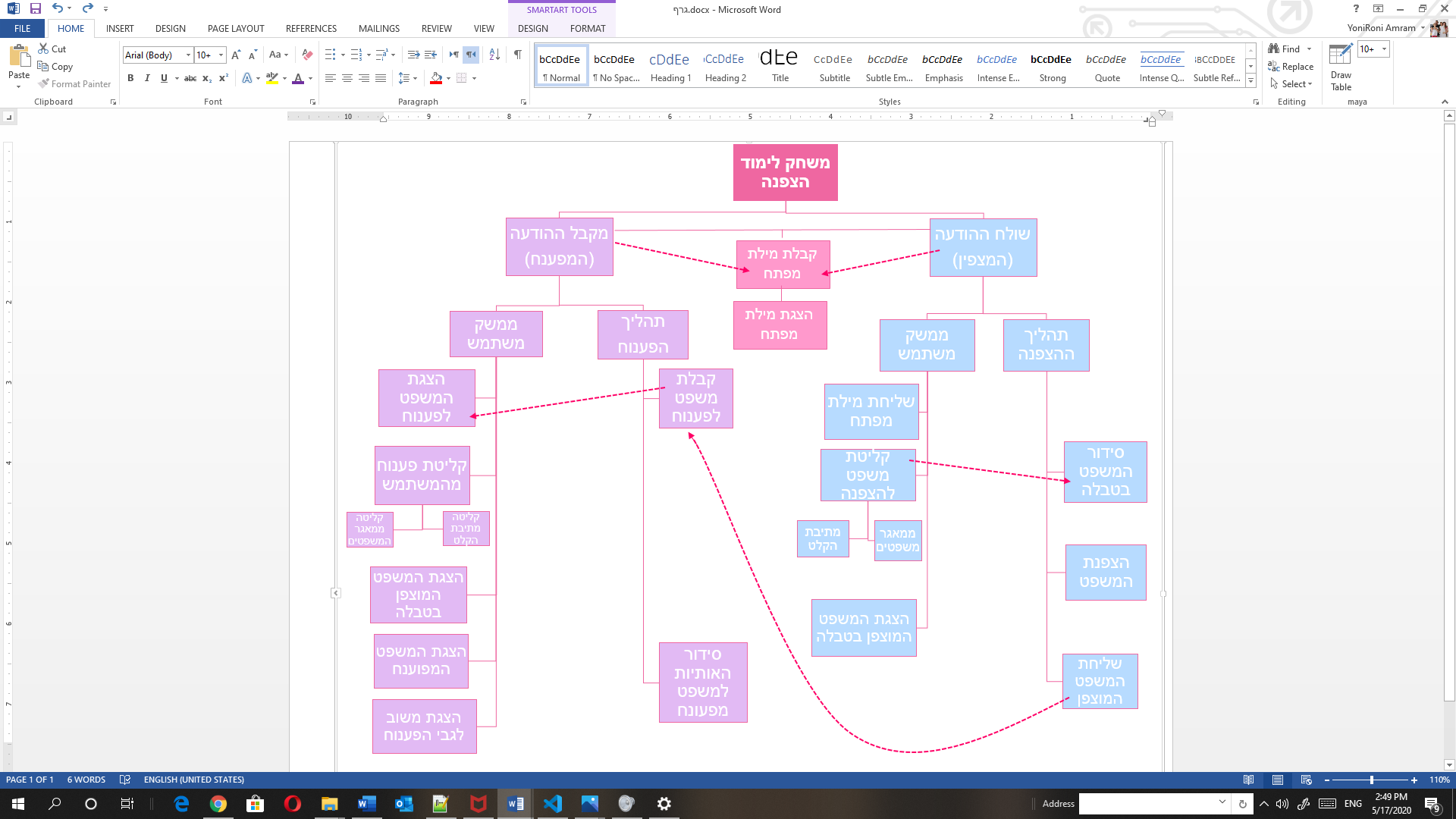
כדי ללמוד client server השתמשתי באינטרנט, ביוטיוב ובמנחה וחקרתי כיצד ניתן לשלוח את המסרים ומילות הקוד שלי ממשתמש אחד לשני באמצעות server. סדרת הסרטונים המצורפים עזרו לי להבין כיצד אני רוצה שהתוכנית שלי תעבוד: <https://www.youtube.com/watch?v=bjULmG8fqc8> <https://www.youtube.com/watch?v=2hhEOGXcCvg> <https://www.youtube.com/watch?v=HZWmrt3Jy10> <https://www.youtube.com/watch?v=i6eP1Lw4gZk&t=616s> .בעזרת סרטונים אלו למדתי להשתמש בטכנולוגיה של node js למימוש client server בשפת java script. למדתי גם כיצד לשלוט בצבעים, בצורות וגרפיקה שבתוכנית שלי דבר שהלהיב אותי מאוד.

בנוסף, בגלל שרציתי שכל אחד ואחת יוכלו בקלות לגשת לאתר שלי ולא רק עם כתובת ip קניתי סרבר בענן בdigitalOcean ובgoDaddy קניתי Domain name, כך ברשימת taliamram.com בכל דפדפן, ניתן למצוא בקלות ובזריזות את המשחר ולשחק בו גם מהטלפוניפ הכחמים וגם ממחשבים.

נתתי לחבריי להתנסות בשיטת ההצפנה ולשכנים שלי כדי לבדוק האם היא מעניינת אותם והאם היא מסקרנת מספיק וראיתי שהם מאוד מתלהבים מהשיטה ואפילו לימדו את חבריהם את השיטה גם כן. ראיתי שיש קהל שישמח לשחק שמבשחק שאבנה.

# מבנה הפרוייקט

Top down level diagram



3

2

1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **היחידה בפרוייקט** | **תפקיד היחידה** | **שם הפעולה** | **תפקיד הפעולה** | **קלט** | **פלט** |
| קבלת והצגת מילת מפתח | קליטת מפתח ההצפנה מאחד מהמשתמשים והצגתו | inputKeyWordBox() | ליצור תיבת קלט למשתמשים | מילת מפתח בעלת 3-7 אותיות באנגלית מהמקלדת/ מהשרת | הצגה גרפית של מילת המפתח ומיון לוגי |
| getKeyword() | קליטת מילת מפתח מאחד המתשמשים |
| updateKeyWord() | פעולה א-סינכרונית פעולה שמתבצעת כאשר מגיעה מילת מפתח מהשרת |
| drawKeyword() | הצגה גרפית |
| sortKeyword() | מיון לוגי לפי abc |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **היחידה בפרוייקט** | **תפקיד היחידה** | **שם הפעולה** | **תפקיד הפעולה** | **קלט** | **פלט** |
| שליחת מילת מפתח | שליחה של מילת המפתח מהמשתמש לשאר המשתמשים | getKeyword() | קולט מילת מפתח ושולח לשאר המשתמשים דרך השרת | מילת מפתח בעלת 3-7 אותיות באנגלית מהמקלדת | שליחה אל השרת |
| קליטת משפט להצפנה | קליטת משפט ממשתמש שישלח כהודעה מוצפנת לשאר המשתמשים | inputSentenceBox() | יצירת תיבת קלט למשתמשים | קליטת משפט בעברית/ באנגלית מהמקלדת או משפט ממאגר משפטים | --- |
| getSentence() | קליטת משפט מתיבת הטקסט |
| inputSentenceDropDownBox() | קליטת משפט ממאגר המשפטים |
| סידור המשפט בטבלה | המשפט שהכניס המשתמש כעט יסודר במערך | processUserStr() | סידור המשפט במערך דו מימדי ללא רווחים | משפט מהמשתמש | --- |
| הצגת המשפט המוצפן בטבלה | המשפט יוצג בצורה גרפית על גבי מסך המשתמש לפי צבעים על מנת להראות את תהליך ההצפנה | drawOrigin() | הצגה גרפית של המשפט מהמערך לפי שיטת ההצפנה ולפי צבעים בכדי שהלימדה תיהיה נוחה | stringToDraw  המשפט של המשתמש ללא רווחים | הצגה גרפית בטבלה |
| הצפנה ושליחת המשפט המוצפן | הצגה גרפית של תהליך ההצפנה ושליחת המשפט המוצפן לשאר המשתמשמים | drawEncryptedOrderd() | הפעולה ראשית מציגה את סדר ההצפנה לפי הabc ולפי צבעים ולאחר מכן מחברת את המשפט המוצפן ושולחת אותו | מערך דו מימדי שבתוכו המשפט ומערך חד מימדי לפי סדר לוגי של מילת המפתח | שליחה אל השרת |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **היחידה בפרוייקט** | **תפקיד היחידה** | **שם הפעולה** | **תפקיד הפעולה** | **קלט** | **פלט** |
| קבלת משפט לפענוח  +  הצגת המשפט לפענוח | קבלת משפט מהמצפין דרך השרת שהמשתמש יצטרך לפענח | decriptMessage() | קבלת המשפט המוצפן והצגתו למשתמשים | משפט מוצפן שנשלח ממשתמש אחר מהשרת | --- |
| קליטת פענוח מהמשתמש | לקלוט פענוח של המשפט המוצפן שהמשתמש ניחש | getSentence() | קבלת ניחוש של המשתמש מתיבת הקלט | משפט שהמשתמש מקליד בתיבת הטקסט/בוחר מהמאגר | --- |
| inputSentenceDropDownBox() | קבלת ניחוש של המשתמש ממאגר המשפטים |
| הצגת המשפט המוצפן הטבלה | להראות למשתמש את תהליך ההצפנה של המשפט המוצפן צעד אחרי צעד בבירור | processUserStr() | מחיקת הרווחים מהמשפט שהכניס המשתמש | משפט שהמשתמש ניחש | הצגת טבלה בצורה גרפית לפי צבעים ולפי שיטת ההצפנה |
| drawDecrypt() | מציג את המשפט המוצפן בטבלה בצורה גרפית לפי צבעים ולפי סדר הabc של מילת הקוד- מראה כיצד לפענח את המשפט המוצפן | המשפט של המשתמש ללא רווחים |
| סידור האותיות למשפט מפוענח | לסדר את המשפט המוצפן ולמשפט מפוענח | draw() |  | המשפט המוצפן מהשרת | --- |
| הצגת המשפט המפוענח | מציג בצורה גרפית את המשפט המפוענח על המסך | draw() |  | המשפט המוצפן מהשרת | הצגת המשפט המוצפן על המסך עם הודעה מתאימה |
| הצגת משוב לגבי הפענוח | ליידע את המשתמש האם צדק בפענוח המשפט או שטעה | draw() | משווה בין המשפט המקורי לפני ההצפנה לבין הפיענוח של המתשמש, אם פיענח בצורה נכונה/לא נכונה תוצג בצורה גרפית הודעה בהתאם | המשפט לפני ההצפנה והמשפט שניחש המשתמש | לפעינוח נכון ההודעה:"very good"  לטעות:"bad guess" |

ארכיטקטורת רשת

בפרוייקט שלי, המערכת כוללת שימוש ברשת בתצורה של שרת לקוח Client-server model. השתמשתי בטכנולוגיית node js <https://nodejs.org/en/>

בכדי שהמשחק יהיה נגיש שכרתי שרת וירטואלי מחברה בשם Digital Ocean, המריץ מכונת לינוקס שעל גביה התקנתי את Node.js העתקתי את הקבצים שלי והרצתי את הסרבר. היות והשרת בעל public address ניתן לגשת אליו מכל דפדפן ובאמצעות כך את המשחק שלי ניתן לשחק מכל מחשב או טלפון חכם.

open account in DigitalOcean (yonironi@gmail.com) //פתחתי משתמש

start new machine "ubuntu Nodejs" // ubuntu התחלתי מכונת לינוקס

we got temporray password , fornew machine public IP 104.248.248.74

user root

change password to T...M..2. //סיסמא

run:

npm install --save express path //היות ואני משתמש ב Node js express התקנתי את האקספרסס

npm install --save socket.io path //כמו כן אני משתמשת בטכנלוגית סוקט מעל נווד ג'יי אס לכן התקנתי אותה גם

בעזרת גיט הורדתי את הקבצים לשרת החדש git pull

cd encrypt/

npm init

הרצתי screen שישמור על הסרבר במצב ריצה גם שאני מתנתקת מהשרת

npm start

( node server.js )

בכדי ליעיל את המשחק ולהפוך את המשחק לעוד יותר ידידותי למשתמש וזמין, שכרתי דומיין בשם [www.taliamram.com](http://www.taliamram.com) והיפנתי את הדומיין לכתובת הip של המכונה שרצה בדיגיטל אושן.

תיאור ההצפנות

מכיוון שהמשחק שלי מיועד לילדים בגילי, רציתי שההצפנה שבה אשתמש תיהיה מעניינת ומאתגרת אך גם לא קשה מדי. משהו שנערים יראו בו קושי אך גם לא יהיה מתסכל או מסובך להבין את שיטת ההצפנה והפענוח. לכן ביחד עם ד"ר עמית קליינמן בחרתי את שיטת הצפנת העמודות rectangular transposition Encryption and decryption. רציתי שבמשחק שלי תיהיה מעורבת מחשבה מצד המתשמשים. בנוסף, אחד מהתחביבים הגדולים שלי הוא עיצוב ואומנות לכן רציתי לעשות הצפנה שאוכל להראות אותה בצורה גרפית מעניינת ומושכת לעין.

השיטה מבוססת על שינוי סדר/ פרמוטציה- המסר מוצפן על ידי שינוי סדר האותיות, מבלי לשנות את האותיות עצמן. בשיטה זו למפענח ההודעה ולמצפין ההודעה יש את אותה מילת מפתח שרק באמצעותה ניתן לפענח את ההודעה.

לדוגמא נקח את המילה M A N G O. נמספר כל אות במילת המפתח לפי סדר הabc ונצבע כל אות כדי לעזור להבין את השיטה בצורה קלה יותר.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5O | 2G | 4N | 1A | 3M |

כעת נציב את האותיות של המשפט אותו אנו רוצים להצפין לפי סדר המשפט ללא רווחים ובמקומות הריקים שנותרו בטבלה נכניס x y z (משפט לדוגמא- have a great day)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5O | 2G | 4N | 1A | 3M |
| a | e | v | a | h |
| t | a | e | r | g |
| y | x | y | a | d |

המשפט המוצפן יהיה בנוי כך- האותיות בתור שמתחת לאות A(תור 1) ולאחר מכן האותיות בתור G (2) וכן הלאה...

המשפט המוצפן- **araeaxhgdveyaty**

בכדי לפענח את המשפט, נקח את מספר האותיות במשפט המוצפן, נחלק במספר האותיות במילת המפתח ונציב לפי הabc בתורים שבטבלה את מספר האותיות המתאים.

קישור לסרטון המסביר על שיטת ההצפנה https://youtu.be/ODXfkZ4d7n4

הראתי לחברים ובני דודים בגילי את שיטת ההצפנה לפני תחילת הפרוייקט וההתלהבות שלהם מכך שהצליחו לפענח משפט שהצפנתי הייתה עצומה! כך ידעתי ששיטה זו תסקרן ילדים לשחק במשחק.

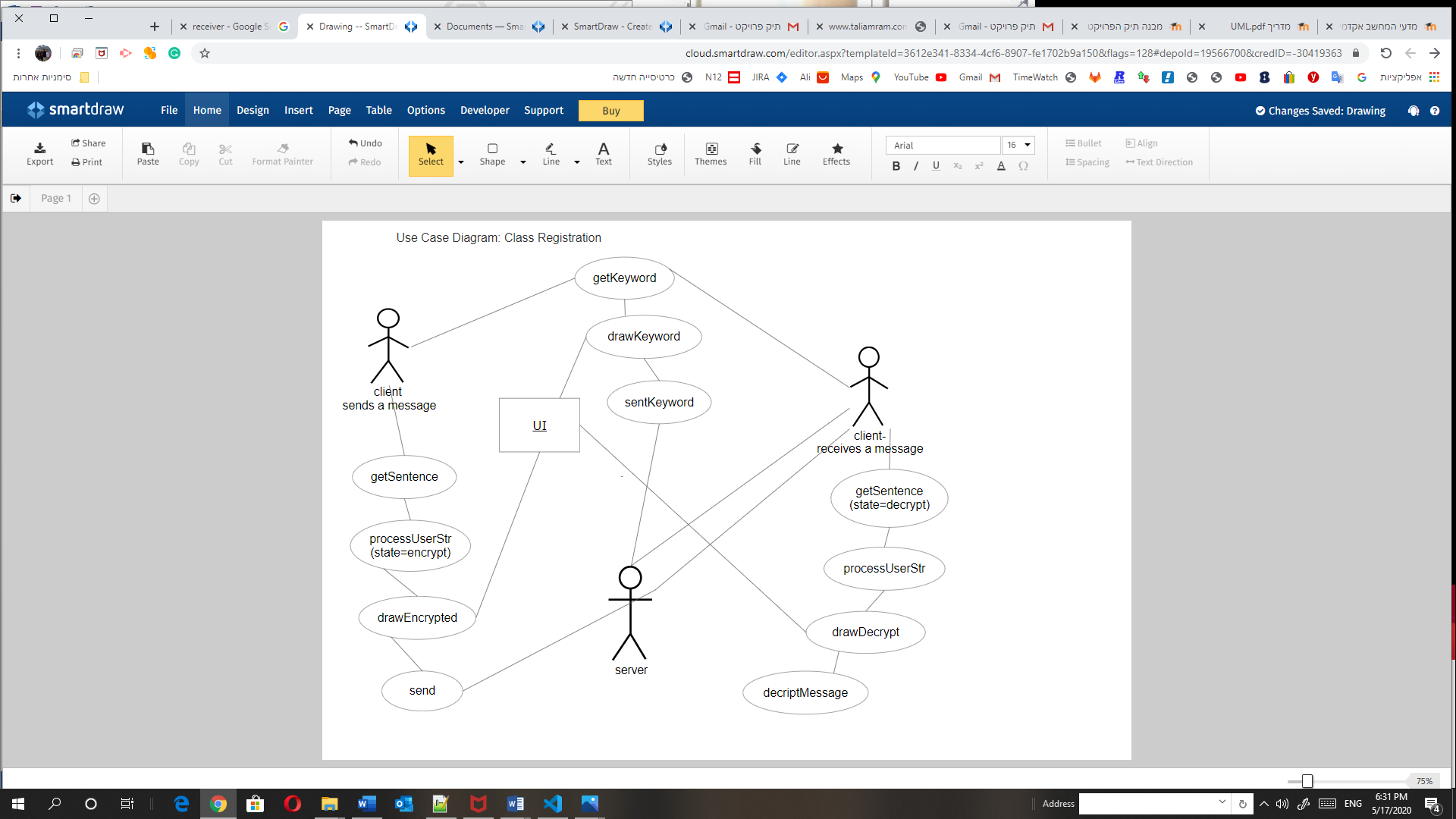
תיאור אלגורתמים עיקריים

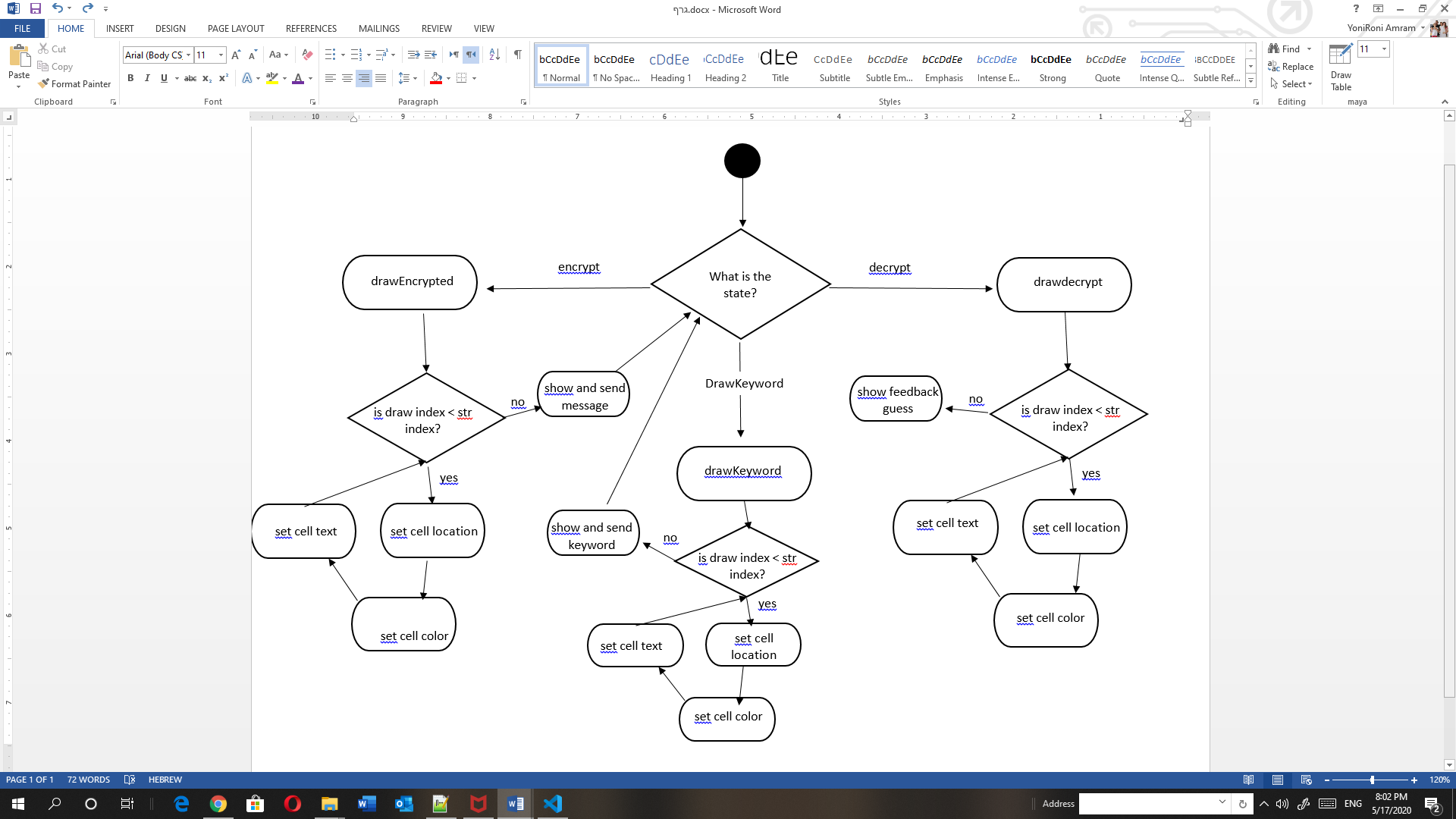
אלגוריתם פענוח המשפט בטבלה- יצירת הטבלה לפי צבעים ולפי סדר לוגי של מילת הקוד שנבחרה על ידי אחד מהמשתמשים. המערכת מראה בצורה גרפית על המסך את הטבלה לפי צבעים, לפי זמן מוקצב ולפי הabc של מילת הקוד ומכניסה לפי תורים ובלי רווחים את האותיות הנדרשות מהמשפט. אלגוריתם זה גם מפענח את המשפט המוצפן וגם מראה ומלמד בצורה ויזואלית כיצד המשתמש היה צריך לפענח את המשפט שנשלח אליו. המשפט נשלח לכל המשתמשים.

אלגוריתם סידור המשפט המקורי בטבלה- מסדר את הקלט של המשתמש בטבלה מסודרת לפי צבעים לפי שורות בלי רווחים. מציג אותה בצורה גרפית על מסך המשתמש. כל ההצפנה ולימדתה מבוססת על הטבלה הזו ועל הצגה גרפית של טבלת העמודות.

אלגוריתם מילת המפתח- כל המשתמשים יכולים להכניס מילת מפתח לתיבת הקלט על המסך באמצעות המקלדת. מילת המפתח שנבחרה נשלחת לכל המשתמשים במשחק באמצעות שרת-לקוח. לאחר מכן אחד מהמשתמשים מכניס משפט שיוצפן לפי מילת המפתח שנבחרה.

אלגוריתם מכונת מצבים- הפעולות והאלגוריתמים פועלים בצורה סינכרונית. כאשר פעולה מסויימת נקראת היא מבצעת את הפעולה הנדרשת תלוי במצב מכונת המצבים. מצב- שולח ההודעה המוצפנת או מצב- מקבל ההודעה לפענוח. כאשר המצב הוא מצב של הצפנה, האלגוריתם קורא לפעולות שייציגו את המשפט בטבלה המתאימה וישלחו את המשפט המוצפן. כאשר המצב הוא מצב מפענח (קבלת הודעה מוצפנת) האלגוריתם יציג את המשפט המוצפן ויחכה לקליטה של פענוח מהמשתמש, לאחר מכן יציג את הפענוח הנכון בעזרת אותה טבלת עמודות לפי צבעים ולפי תורים (לפי abc של מילת המפתח) ויתן משוב למשתמש אם צדק בפענוח המשפט או טעה.



Activity diagram

Class Diagram

התוכנית לא בנוייה ממחלקות כיוון שלא היה צורך בכך.

התוכנית משתמשת בספרייה בשם p5.js, אשר מספקת לי תשתית של פונקציות כמו :

Setup- נקראת פעם אחת בתוכנית לאחר עלייתה, ובה אני דאגתי לתכל את התוכנית שלי, למשל יצירת הקנבס, הגדרת מספר הפעמים שאנו קוראים ל Draw(כלומר קצב המשחק) וקוראת ליצירת מילת מפתח. היא גם פותחת socket עם הserver ומאזינה לקבלת הודעות socket.

Draw- פונקציה מחזורית ובה, אנו מציירים את טבלאת הצפנת העמודות הן עבור המצפין והן עבור המפענח.

הסברים בטבלה של פונקציות ופעולות חשובות:

|  |  |
| --- | --- |
| server.js | פונקציות/פעולות חשובות: |
| שימוש בטכנולוגית node JS express | var express = require ('express') |
| צירית אובייקט מסוג אקספרס שיוצר את הסרבר באופן מהיר ואוטמטי | var app= express() |
| האזנה לפורט 3000 (הקוד בדיגיטל אושן מאזין לפורט 80) | var server= app.listen(3000) |
| הפנייה לתת ספרייה public המכילה את קובץ האייץ טי אמ אל והגאווה סקריפט | app.use(express.static('public')) |
| שימוש בספרייה | var socket =require('socket.io'); |
| האזנה לסוקט | var io = socket(server) |
| הפעולה שתתבצע כל פעם שיש חיבור של משתמש חדש | io.sockets.on('connection', newTaliConnection) |
| פעולה שנקראת כאשר יש חיבור של משתמש | function newTaliConnection (socket) |
| פעולה שנקראת בכדי לשלוח לכל המשתמשים את ההודעה המוצפנת | function stringMsg (data) |
| פעולה שנקראת בכדי לשלוח לכל המשתמשים את מילת הקוד | function updateKeyWord(data) |

|  |  |
| --- | --- |
| textedit.js | פונקציות/פעולות חשובות: |
| נקרא פעם אחת בתחילת התוכנית על ידי p5JS  יוצרים קנבס, מתאחלים משתנים | function setup() |
| נקרא על ידי p5Js כל פעם שהתוכנית במצה loop איקס פעמים בשנייה  אחראית על מכונת המצבים בתוכנית | function draw() |
| לאחר קבלת הודעה מהשרת פעולה זו הופכת את המסך של המשתמש לורוד ומשנה את המצב במכונת המצבים למצב המציג את מילת המפתח שנקלטה | function updateKeyWord(data) |
| לאחר קבלת המשפט המוצפן מהשרת פונקציה זו מתריאה על קבלת הודעה ומשנה את הדגל למצב מקבל ההודעה | function decriptMessage (data) |
| מצייר לפי צבעים את מילת הקוד | function drawKeyword (stringToDraw) |
| מצייר את המשפט המקורי בטבלה מסודרת לפי הא-ב של מילת המפתח | function drawOrigin (stringToDraw) |
| מציג בטבלה בצורה גרפית לפי צבעים ולפי סדר התורים לפי הא-ב את הצפנת המשפט | function drawDecrypt (stringToDraw) |
| פעולה שנקראת כאשר יש חיבור של משתמש | function newTaliConnection (socket) |
| פעולה שנקראת בכדי לשלוח לכל המשתמשים את ההודעה המוצפנת | function stringMsg (data) |
| פעולה שנקראת בכדי לשלוח לכל המשתמשים את מילת הקוד | function updateKeyWord(data) |
| מציג את המשפטים בשורות לפי הסדר הלוגי של העמודות -לב ההצפנה | function drawEncryptedOrdered () |
| מציג על גבי מילת הקוד את סדר הא-ב להצפנה קלה יותר | function drawKeywordNum () |
| יצירת מערך שישמור את סדר הא-ב במילת המפתח | function sortKeyWord () |
| יצירת כפתור ותיבת קלט למילת הקוד | function inputKeywordBox () |
| לאחר קבלת קלט של מילת קוד הפעולה עוברת למצב הראשון במכונת המצבים, שולחת את מילת הקלט לשאר המשתמשים ומשנה את צבע המסך של השולח לירוק | function getKeyword () |
| יצירת תיבת טקסט להכנסת משפט להצפנה וכפתור | function inputSentenceBox () |
| טיפול במשפט מתיבת הקלט או של המצפין או של המפענח תלוי במצב במכונת המצבים | function getSentece () |
| יצירת אפשרות בחירת משפט ממאגר משפטים או של המצפין או של המפענח תלוי במצב במכונת המצבים | function inputSentenceDropDownBox() |
| כאשר נבחר משפט ממכונת המצבים | function SelectEvent() |
| עושה שני תפקידים- תלוי אם המשתמש הוא שולח ההודעה או מקבל ההודעה | function processUserStr() |

טכנולוגיות

שפת התכנות היא java script בשימוש בסיפריית p5.js .

דפדפןchrome מאפשר כלים עבור מפתחים, שם יש אפשרות לעקוב אחרי התוכנית, לשים נקודות עצירה(break points) ולהריץ את התוכנית צעד אחר צעד.

לצורך הצגת הודעות קופצות במהלך התוכנית השתמשתי בספרייה מעל Java Script שנקראת sweetalert.

בנוסף השתמשתי לצורך הכתיבה וההרצה בvisual studio code וכן בNotepad++ או בsublime.

לצורך client-server השתמשתי בטכנולגיית node js (express).

בכדי שיהיה אפשר לגשת למשחק דרך שרת שנמצא בpublic IP ולא רק במחשב האישי שלי, פתחתי חשבון בDigitalOcean ובו העלתי שרת (לינוקס) שהעתקתי אליו את קבצי התוכנית והרצתי בו את הסרבר בעזרת node js. כתובת השרת הינה 104.248.248.74 והשרת מאזין על פורט 80.

בנוסף בכדי שיהיה אפשר לגשת לשרת על ידי כתובת URL ולא בהקלדת כתובת IP שכרתי דומיין מאתר בשם goDaddy שנקרא: [www.taliamram.con](http://www.taliamram.con)

כך הגישה למשחק מתאפשרת כעט מכל מחשב או טלפון חכם בקלות ובמהירות.

כדי לנהל את הקבצים והשינויים, וכדי שיהיה לי האפשרות לחזור לאחורה, לראות את השינויים שעשיתי לאורך זמן, השתמשתי בתוכנת ניהול קבצים git.

ואת הקבצים עצמם שמרתי בסרבר פתוח ברשת שנקרא github

ובתור השרת השתמשתי בrawgit שיודע להיות שרת לקבצין שנשמרים ב github. כתובת הURL של חשבון הgitHub שלי היא: <https://github.com/taliamram>

# מדריך למשתמש

תרשים מסכים:

מסך פתיחה-

קלט מילת מפתח

מקבל מילת הקוד

שולח מילת הקוד

קלט משפט להצפנה-

מסך ירוק

מקבל המשפט המוצפן

הצגת המשפט המוצפן והמתנה לפענוח מהמשתמש

הצגה גרפית של פענוח המשפט דרך טבלת העמודות לפי צבעים, הצגת המשפט המקורי והודעה קופצת עם משוב

מקבל המשפט המוצפן

הצגת המשפט המוצפן והמתנה לפענוח מהמשתמש

הצגה גרפית של פענוח המשפט דרך טבלת העמודות לפי צבעים, הצגת המשפט המקורי והודעה קופצת עם משוב

שולח המשפט המוצפן

הצגה גרפית של המשפט בטבלה לפי צבעים והצגת המשפט המוצפן

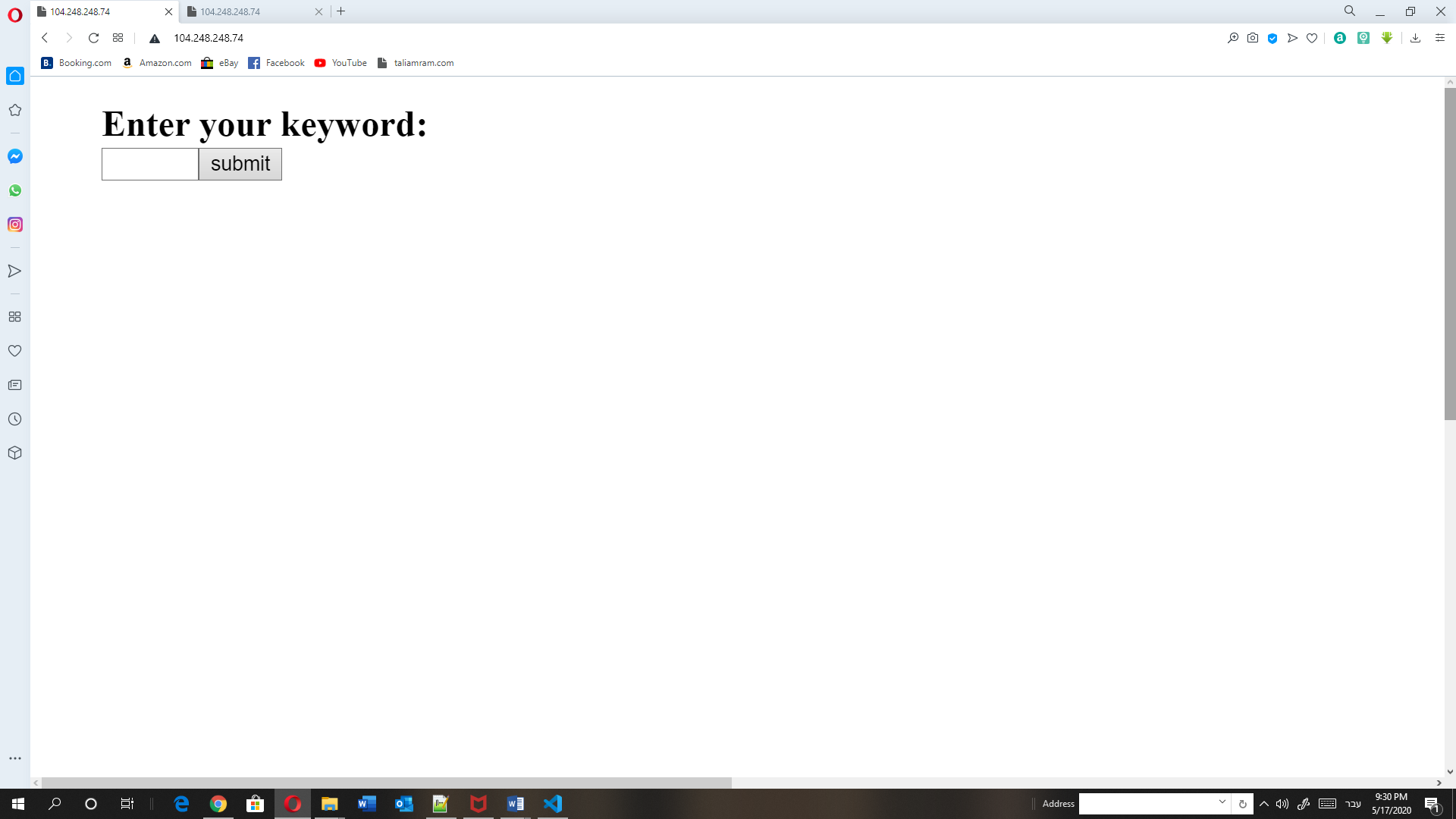
שולח המשפט המוצפן

הצגה גרפית של המשפט בטבלה לפי צבעים והצגת המשפט המוצפן

קלט משפט להצפנה-

מסך ורוד

מסך פתיחה:

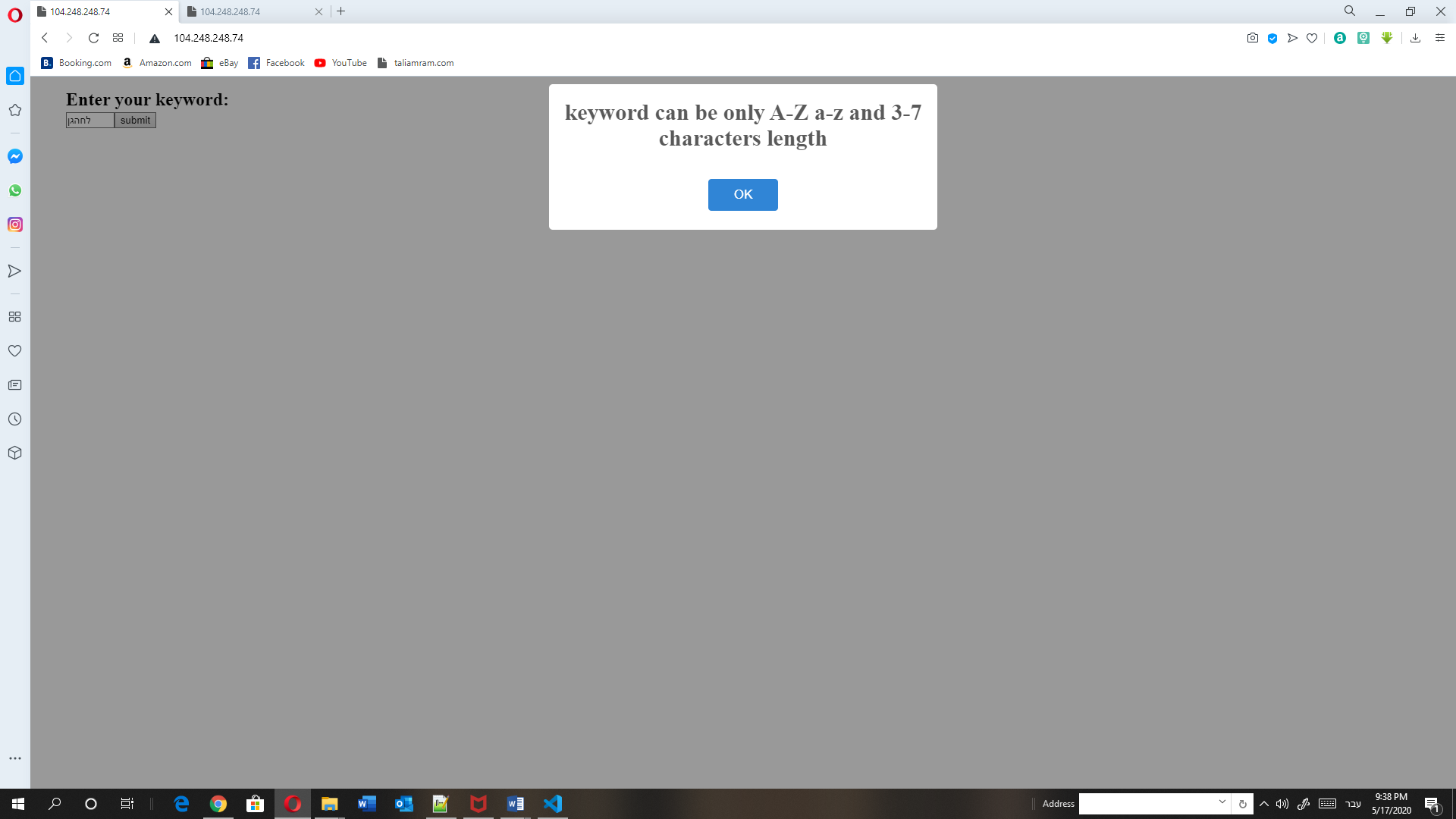


מסך זה הוא מסך הפתיחה של משחק ההצפנה, שבו המשתמש צריך להכניס מילת מפתח לבחירתו, שתשלח לשאר המשתמשים ואיתה יתבצעו ההצפנה והפענוח.

תיבת הטקסט: המשתמש צריך להקליד את מילת המפתח שבחר לצורך ההצפנה לתוך התיבה.

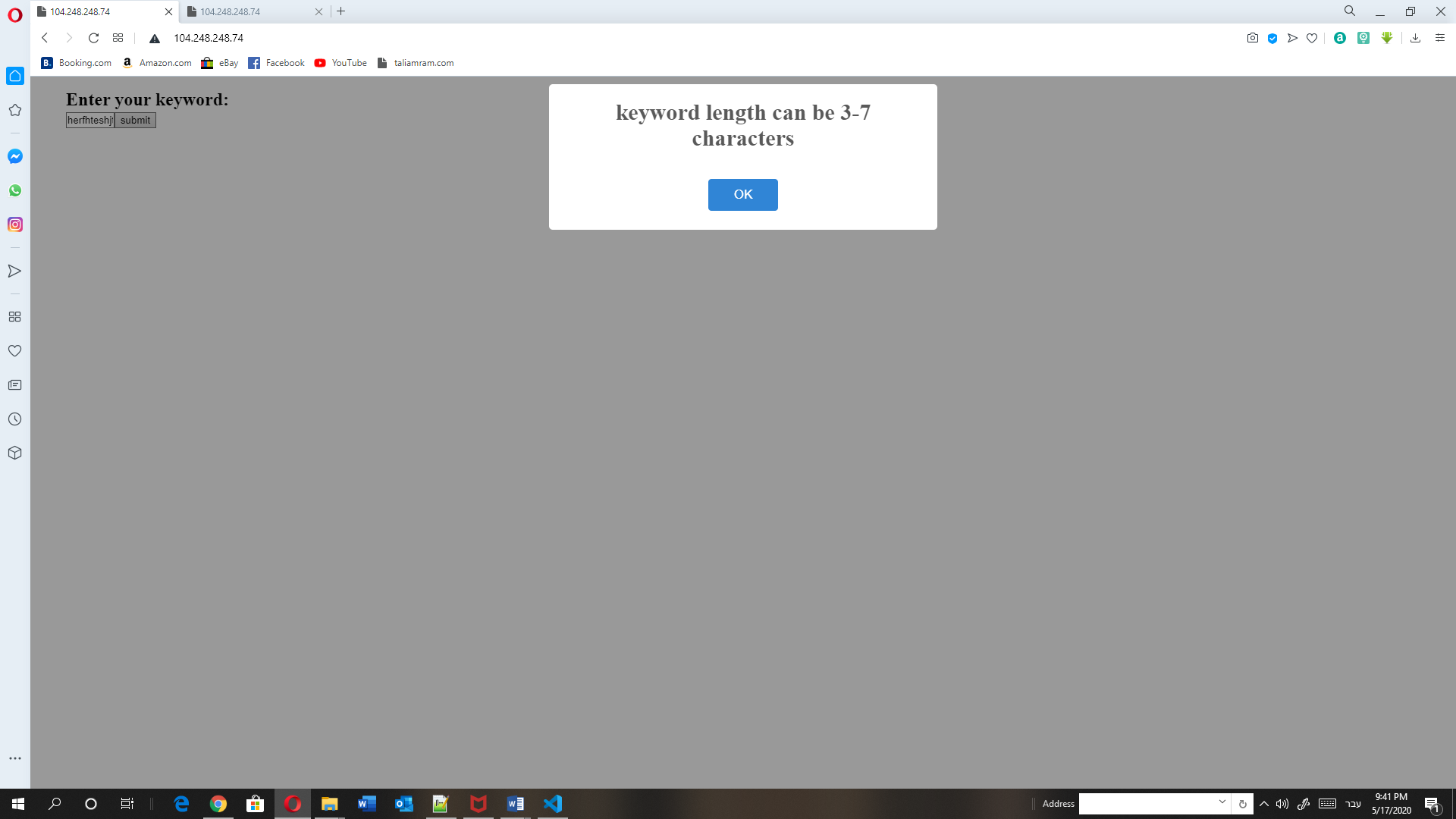
כפתור submit: שולח את מילת המפתח לשאר המשתמשים.

הודעה למשתמש- alert



כאשר המשתמש מקיש מספרים, תווים או אותיות בעברית קופצת התראה זו אשר מודיעה איזה תווים מותר להכניס וכמה. (אותיות באנגלית ובין 3-7)

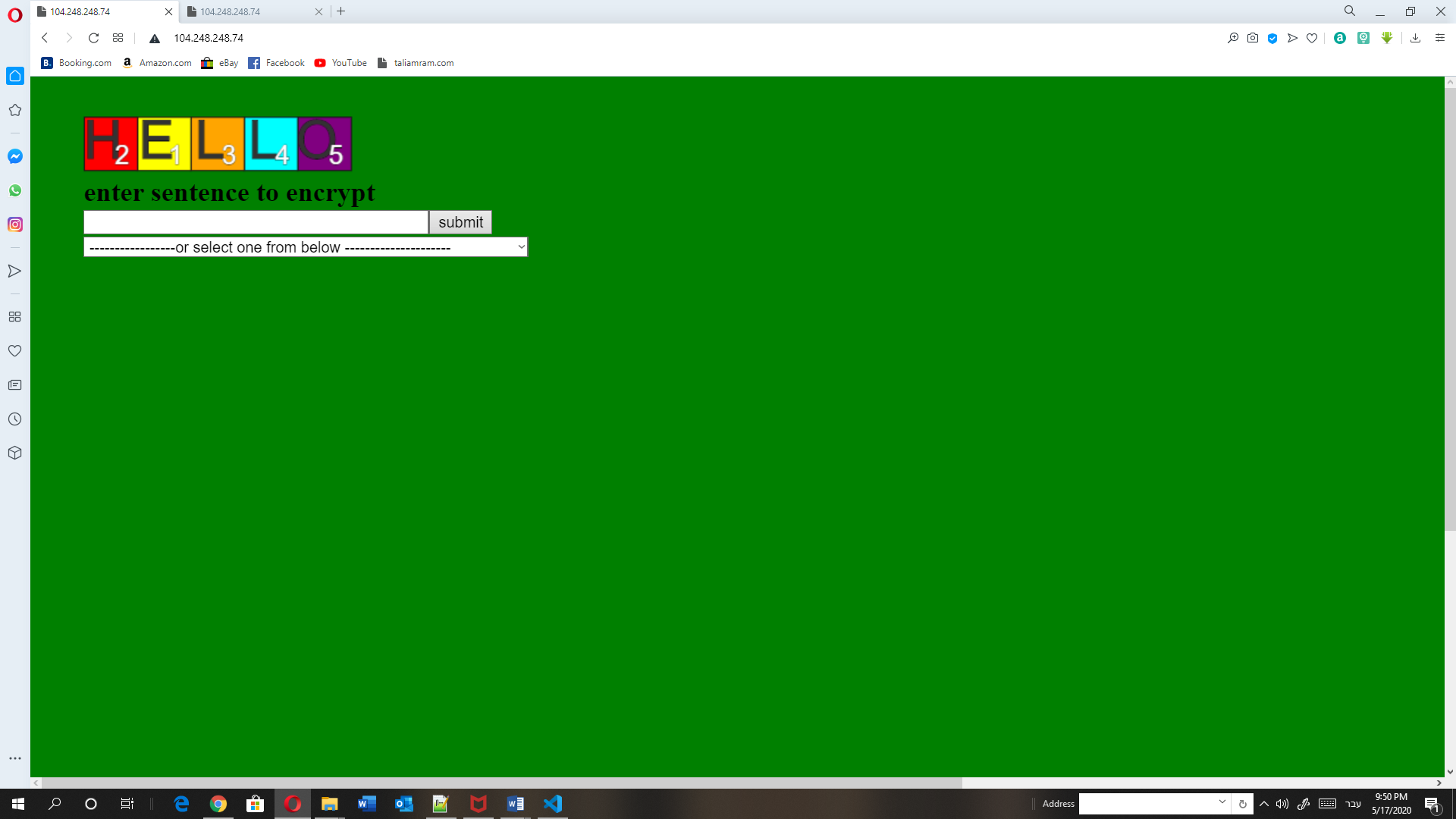
הודעה נוספת:



הודעה זו קופצת כאשר המשתמש מקיש אותיות באנגלית אך יותר או פחות ממספר האותיות הרצוי.

בכדי שההודעה תיעלם יש ללחוץ על הכפתור OK.

מסך שולח מילת המפתח:



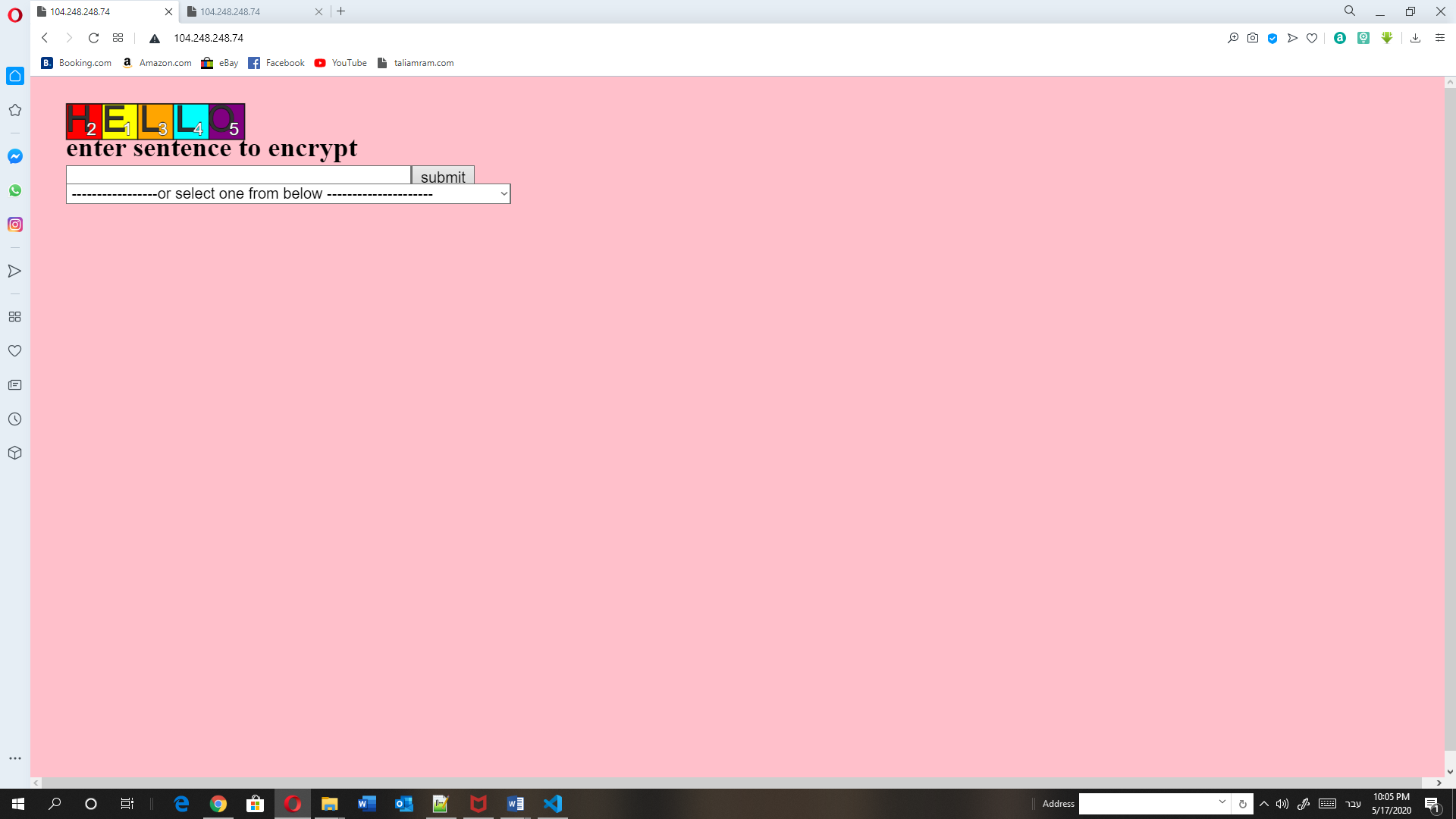
המסך הופך לירוק ומילת הקוד הופכת למסודרת בטבלה לפי צבעים וממוספרת לפי הabc על מנת שההצפנה תיהיה נוחה וקלה. כעט המשתמש יכול להכניס משפט להצפנה

כפתור submit: לאחר שהמשתמש מכניס את המשפט להצפנה לחיצה על הכפתור מצפינה את המשפט שנקלט.

תיבת הטקסט: המשתמש צריך להכניס את המשפט "הסודי" אותו הוא רוצה לשלוח לאחר שיוצפן לתוך תיבת הטקסט.

מאגר המשפטים or select one from below : המשתמש יכול לבחור משפט מרשימת המשפטים.

מסך מקבל מילת המפתח:



המסך הופך לורוד ומילת הקוד שנשלחה ממשתמש אחר ועכשיו מוצגת על המסך בטבלה לפי צבעים וממוספרת לפי הabc על מנת שההצפנה תיהיה נוחה וקלה. כעת המשתמש יכול להכניס משפט להצפנה משלו או לבחור מרשימת המשפטים הקיימים.

כפתור submit: לאחר שהמשתמש מכניס את המשפט לחיצה על הכפתור מצפינה את המשפט שנקלט.

תיבת הטקסט: המשתמש צריך להכניס את המשפט "הסודי" אותו הוא רוצה לשלוח לאחר שיוצפן לתוך תיבת הטקסט.

מאגר המשפטים or select one from below : המשתמש יכול לבחור משפט מרשימת המשפטים.

\*גם שולח מילת הקוד וגם מקבל מילת הקוד יכולים להכניס משפט להצפנה ושליחה.

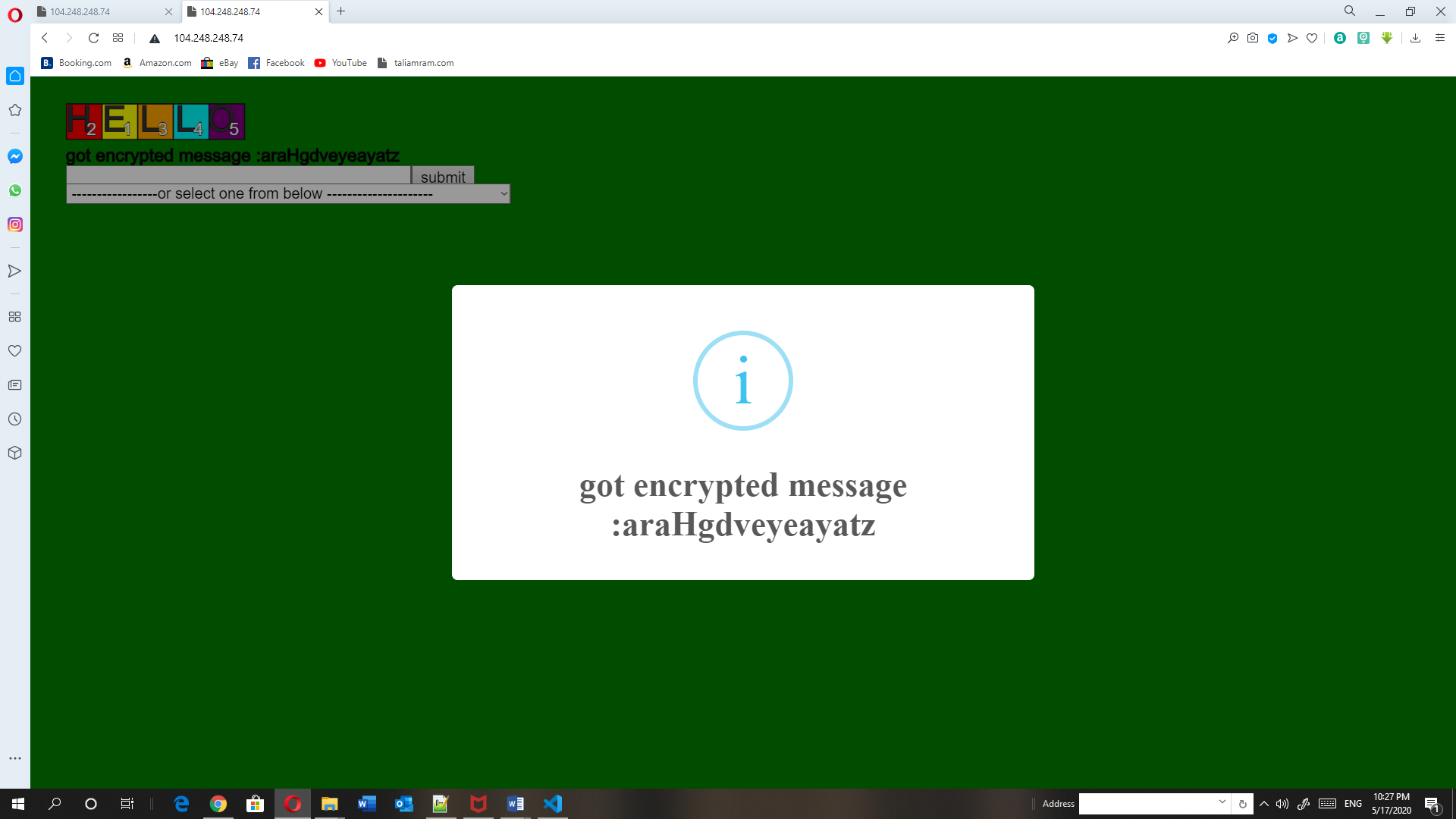
מסך לאחר הכנסת משפט להצפנה:



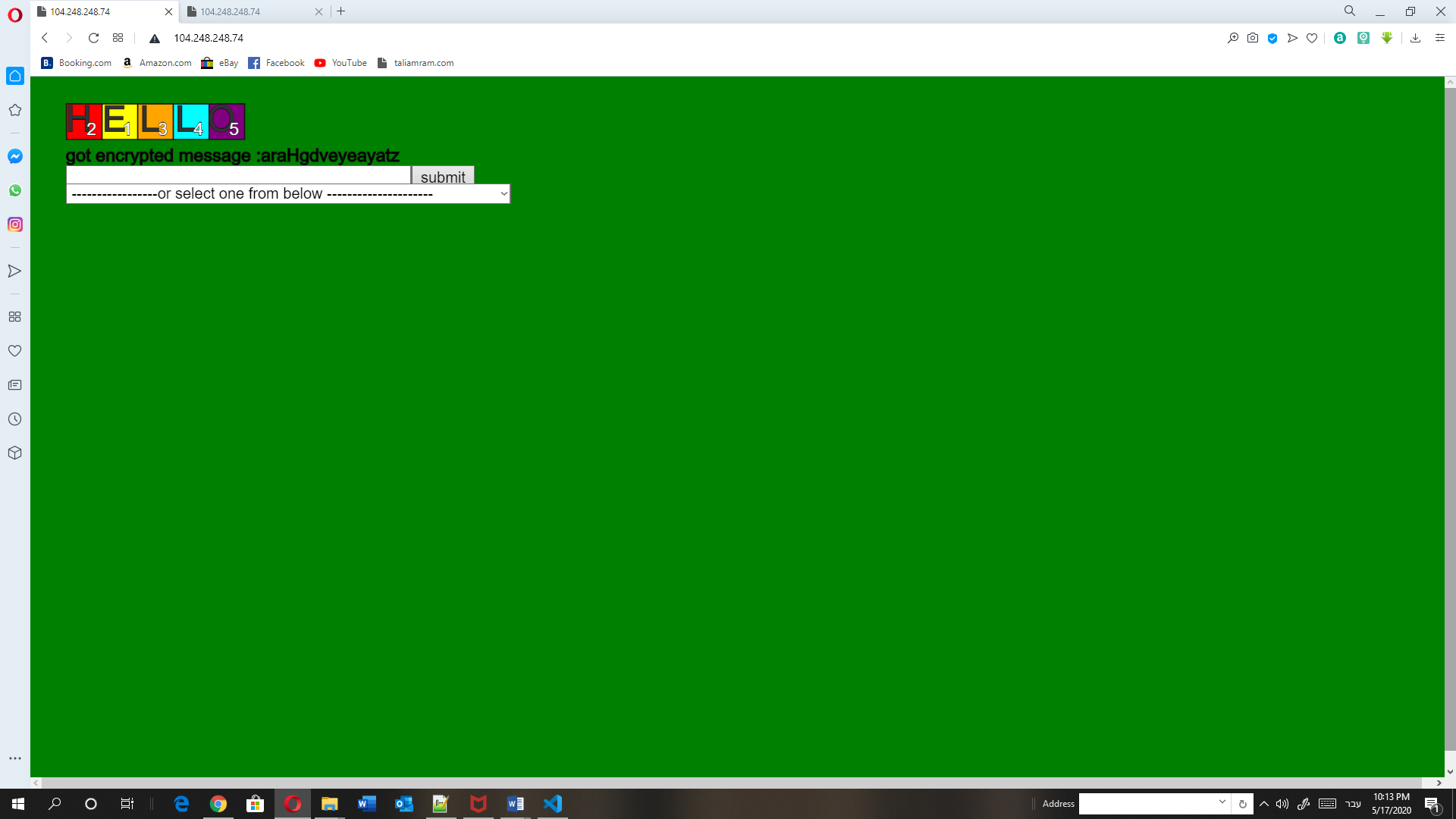
לאחר שהמשתמש הכניס משפט להצפנה, המשפט מוצג בצורה גרפית וצבעונית בטבלה לפי שיטת הצפנת העמודות, חלקי המשפט המוצפן לפי המיספור והצבעים מוצגים בשורות ומתחתיהם המשפט המוצפן שגם נשלח למשתמשים האחרים.

המסך של מקבל ההודעה המוצפנת לאחר שהתקבל משפט מוצפן ממשתמש אחר:

הודעה "קופצת" למשך 2.5 שניות על מסך המשתמש ומודיעה כי התקבל משפט מוצפן.



לאחר מכן ההודעה נעלמת.

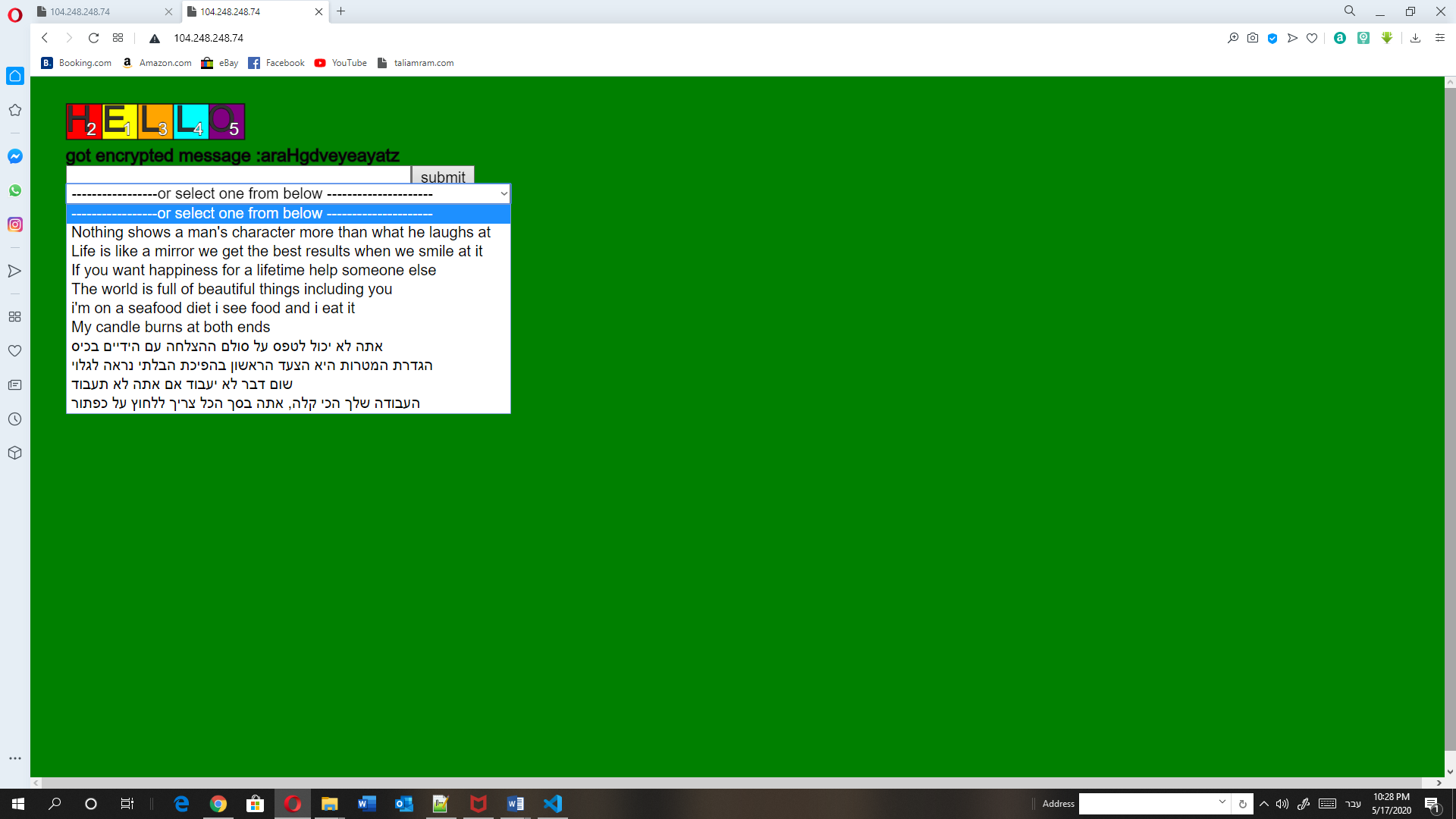


המשפט המוצפן שהתקבל מוצג בצורה גרפית על המסך, וכעת המשתמש צריך להכניס את הפענוח שלו למשפט. המשתמש יכול להקליד בתיבת הטקסט או לבחור משפט מרשימת המשפטים.

כפתור submit: לאחר שהמשתמש מכניס את המשפט לחיצה על הכפתור מצפינה את המשפט שנקלט מהמשתמש האחר.

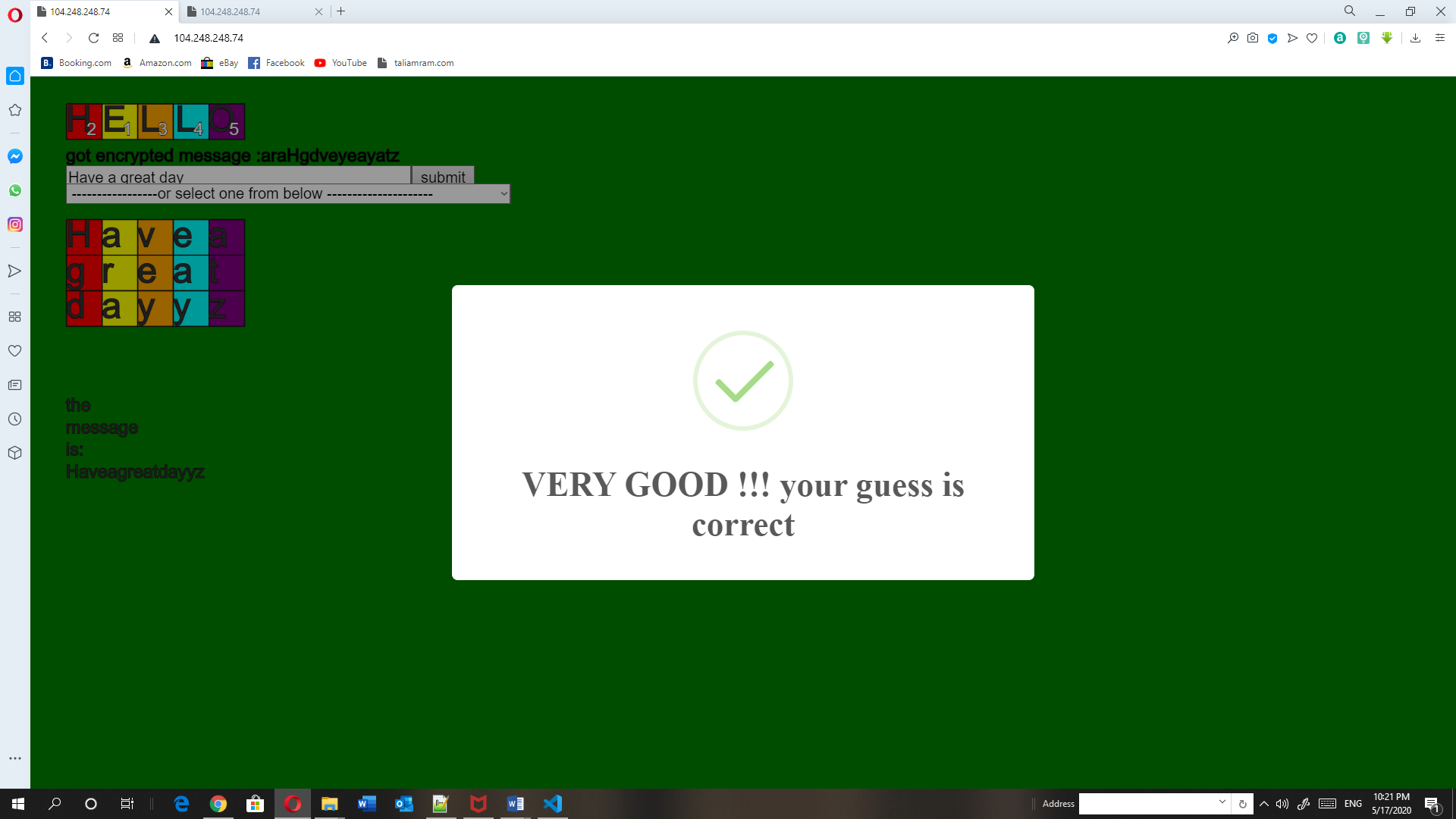
תיבת הטקסט: המשתמש צריך להכניס משפט מפוענח או ניחוש לפענוח של המשפט שהתקבל.

מאגר המשפטים or select one from below : המשתמש יכול לבחור משפט מרשימת המשפטים אשר הוא חושב שאחד מהמשפטים הוא המשפט המוצפן.

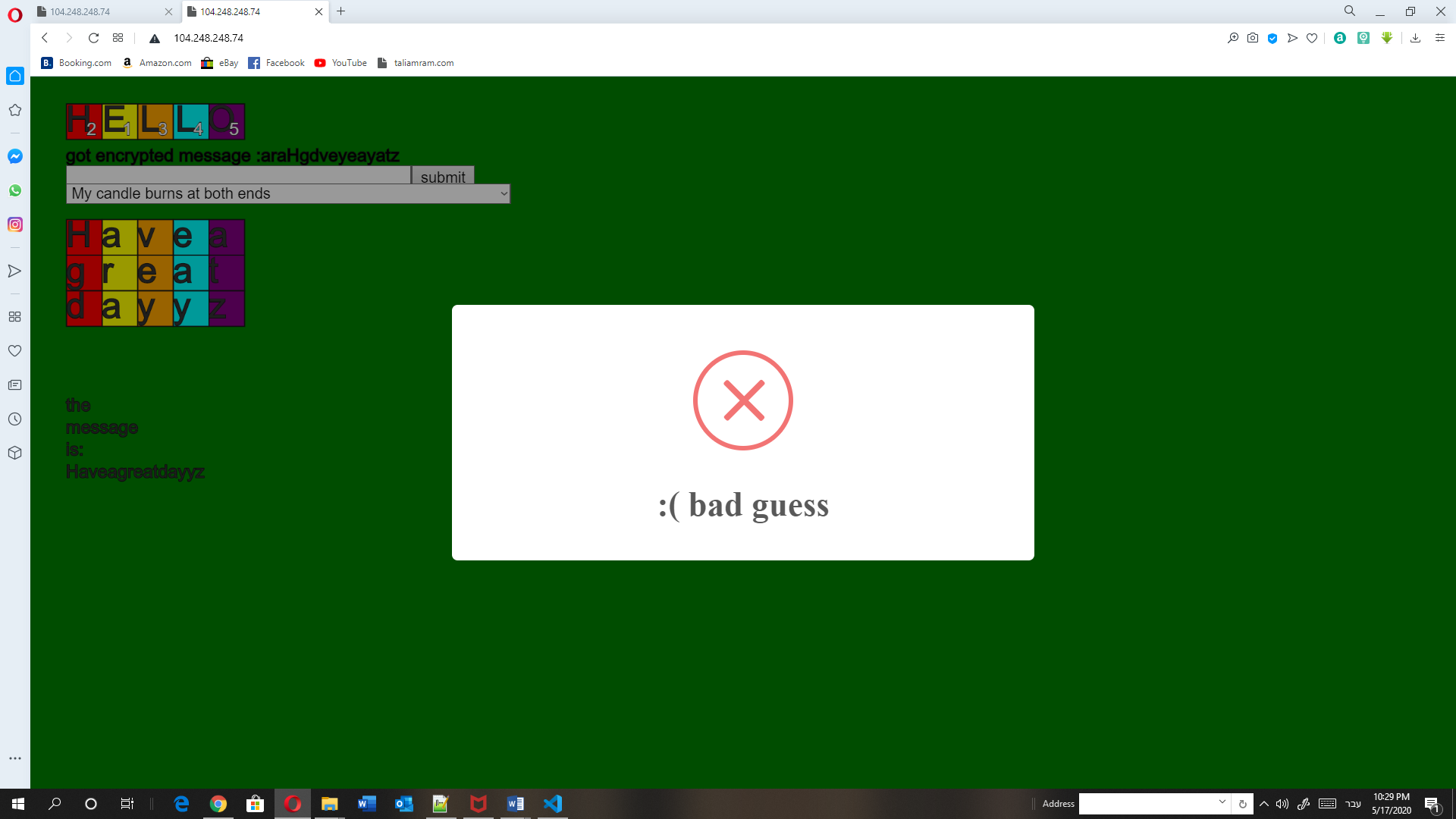


המסך אם המשתמש צדק בפענוח שלו:

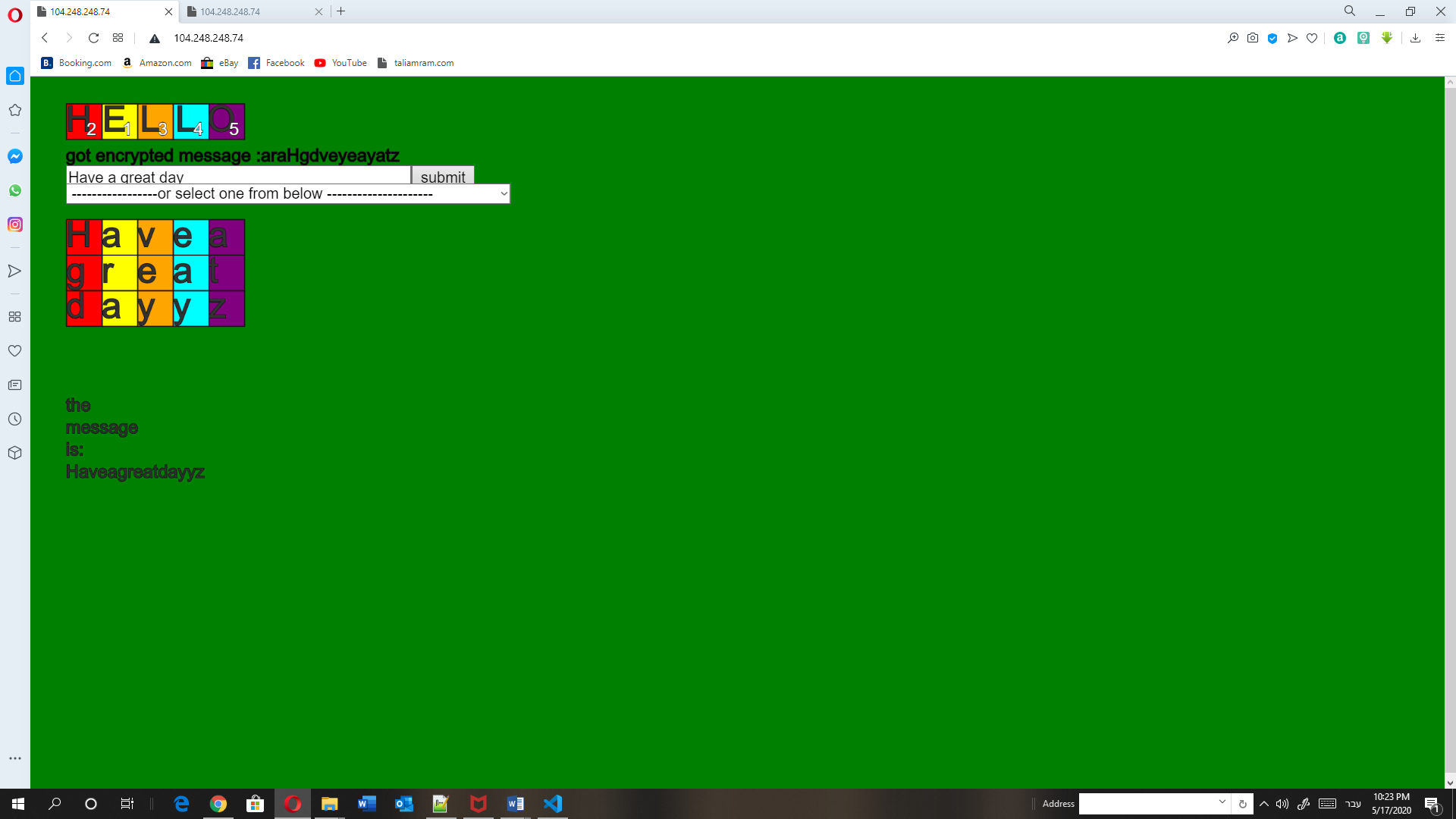
alert: אשר מודיעה למשתמש כי צדק בניחוש המשפט והצליח לפענח כראוי



alert: אשר מודיעה למשתמש כי טעה בניחוש המשפט ולא הצליח לפענח כראוי



המסך הסופי:



מסך זה מציג למשתמש כיצד להציב את המשפט בטבלה, עמודה אחרי עמודה לפי צבעים וסדר לוגי ומראה את המשפט המקורי לאחר הפענוח.

הוראות משחק:

על אחד המשתמשים להקליד מילת מפתח אשר תשמש להצפנת ופיענוח המשפט.

על אחד המשתמשים להכניס משפט שברצונו לשלוח בצורה מוצפנת למשתמש האחר.

המשתמש שאליו נשלחת ההודעה מקבל את ההודעה בצורה "סודית" ורק לאחר שינסה לפענח אותו המשתמש יגלה מה המשפט ואם צדק בניסיון פיענוח המשפט או טעה.

ההצגות הגרפיות של הטבלאות מלמדות את המשתמשים כיצד שיטת ההצפנה עובדת.

# מדריך למפתח

שם הקובץ: server.js

מיקום: תקיית האם

תפקיד: הקובץ המתפעל את node js

אופן הרצה: אפשרות א- node server.js בחלון cmd במיקום שהקובץ נמצא בו

אפשרות ב- npm start בחלון cmd במיקום שהקובץ נמצא בו

תוכן הקובץ והסברים על פעולותיו ומשתנים:

var express = require ('express'); //שימוש בטכנולוגית node JS express.

var app= express(); //יצירית אובייקט מסוג אקספרס שיוצר את הסרבר באופן מהיר ואוטמטי

var server= app.listen(3000); //האנזנה לפורט 3000 (הקוד בדיגיטל אושן מאזין לפורט 80)

app.use(express.static('public')); //הפנייה לתת ספרייה public המכילה את קובץ האייץ טי אמ אל והגאווה סקריפט

console.log("Tali pogram"); //הדפסה למסך שמסמל לי שהסרבר התחיל לרוץ

var socket =require('socket.io'); //שיומוש בספרייה

var io = socket(server); //האזנה לסוקט

io.sockets.on('connection', newTaliConnection); //הפעולה שתתבצע כל פעם שיש חיבור של משתמש חדש

function newTaliConnection (socket) { //חיבור של משתמש

console.log("new connection:" + socket.id); //הדפסה ללוג

socket.on('mouse-out', mouseMsg); //דוגמא שלמדתי ממנה

socket.on('encriptedMessage', stringMsg); //קפיצה לפונקציה כל פעם שמגיעה הודעה עם הכותרת הרשומה

socket.on('KeyWord', updateKeyWord);

function stringMsg (data) {

socket.broadcast.emit('encriptedMessage',data); //שולח לכל המשתמשים לא כולל שולח ההודעה עצמו

console.log(data);

}

function mouseMsg (data) {

socket.broadcast.emit('mouse-in', data);

//io.sockets.emit('mouse', data); שולח לכל המשתמשים כולל שולח ההודעה

//console.log(data);

}

function updateKeyWord(data) {

socket.broadcast.emit('KeyWord', data);

console.log("KeyWord was exchanged : " + data);

}

}

שם הקובץ: index.html

מיקום: בספריית public שנמצאת תחת תקיית האם

תפקיד: הקובץ הראשון הנפתח על ידי הדפדפן

אופן הרצה: הסרבר מפנה לקובץ זה, לאחר שמשתמש (client) פונה לסרבר.

תוכן הקובץ והסברים על פעולותיו ומשתנים:

הקובץ מפנה לספריות צד שלישי שהתוכנית משתמשת בהם ובהם p5 js, socket, sweetalert.

כמו כן, הוא מפנה לקבצי הג'אווה סקריפט של התוכנית שלי, בתוכנית זו הקובץ נקרא textedit.js זהו הקובץ היחיד שמכיל את הקוד עבור כל התוכנית.

<!DOCTYPE html>

<html>

<head>

<script type="text/javascript" src="https://cdn.socket.io/socket.io-1.4.5.js"></script>

<script src="https://cdnjs.cloudflare.com/ajax/libs/p5.js/0.5.11/p5.min.js"></script>

<script src="https://cdnjs.cloudflare.com/ajax/libs/p5.js/0.5.11/addons/p5.dom.min.js"></script>

<script src="https://cdnjs.cloudflare.com/ajax/libs/p5.js/0.5.11/addons/p5.sound.min.js"></script>

<script src="https://cdn.jsdelivr.net/npm/sweetalert2@9"></script>

<script src="textedit.js"></script>

<style> body {padding: 0; margin: 0;} </style>

</head>

<body>

</body>

</html>

שם הקובץ: textedit.js

מיקום: בספריית public שנמצאת תחת תקיית האם

תפקיד: הקובץ הראשי בתוכנית שמבצע אותה

אופן הרצה: נקרא דרך index.html. ברגע שדפדפן כלשהו מתחבר לסרבר, שמפנה אותו לקובץ index.html שמפנה לקובץ הזה.

תוכן הקובץ והסברים על פעולותיו ומשתנים:

הקובץ מפנה לספריות צד שלישי שהתוכנית משתמשת בהם ובהם p5 js, socket, sweetalert.

כמו כן, הוא מפנה לקבצי הג'אווה סקריפט של התוכנית שלי, בתוכנית זו הקובץ נקרא textedit.js זהו הקובץ היחיד שמכיל את הקוד עבור כל התוכנית.

//רשימת משתנים גלובלים לשימוש בין הפונקציות השונות

let UserStr = []; //המחרוזת שמחזיקה את המשפט שמיועד להצפנה/פענוח תלוי במצב במכונת המצבים

let encryptStr = []; //המשפט לאחר ההצפנה

let decryptStr = []; // המשפט לאחר הפענוח

let sendStr = []; // המשפט המפוענח

let colors = []; // מערך המחזיר צבעים- כל עמודה בעלת צבע אחד

let SqSize; //מגדיר מהו גודל כל ריבוע ופיקסלים

let StrIndex=0; // המצביע על המיקום הנוכחי במחרוזת

let DrawIndex=0; // מצביע על המיקום הנוכחי בציור הטבלה

let Xstart; //קורדינטה המציעה על קודקוד הציור בציר האיקס

let Ystart; //yקורדינטה המציעה על קודקוד הציור בציר ה

let row; //מציין את מספר השורה הנוכחית

let column;//מציין את מספר העמודה הנוכחי

let KeyLen; //מציין את אורך מילת המפתח

let KeyWord;// = 'apple' מחזיק את מילת המפתח

let orderOfletters; //מערך המחזיק את סדר מילת המפתח לפי הא-ב

let state; //מחזיק את המצב הנוכחי של מכונת המצבים

let recivedStr; //המחרוזת שהגיעה מהסוקט

let columnLen; //אורך כל תור(מספר השורות)

let buttonKeyWord; //מצביע על הכפתור שמשמש למילת המפתח

let greetingKeyWord; //מצביע להודעה של הכנסת מילת מפתח

let inputKeyWord; //מצביע לתיבת הקלט של מילת הקוד

let buttonMessage; //מצביע כל כפתור המשמש לקליטת המשפט להצפנה

let greetingMessage; //מצביע להודעה של הכנסת משפט להצפנה

let greetingError; //לא בשימוש

let inputMessage; //מצביע לתיבת הקלט של המשפט

let sel; // מצביע על מאגר המשפטים

let isreceiver; //דגל שמסמל אם התוכנית במצב של מצפין ההודעה או מפענח

function setup() { //נקרא פעם אחת בתחילת התוכנית על ידי p5JS

createCanvas(window.innerWidth, window.innerHeight);//(windowWidth, windowHeight);

socket = io.connect('http://127.0.0.1:3000'); //פתיחת קשר עם השרת

socket.on('encriptedMessage',decriptMessage); //האזנה להודעות מהשרת

socket.on('KeyWord',updateKeyWord); //האזנה להודעות מהשרת

stroke(20);

SqSize = windowHeight/20;

Xstart = SqSize;

Ystart = SqSize;

isreceiver = false;

row=0;

column=0;

state = 'nostate';

frameRate(14);

colors = ["red", "yellow", "orange","Cyan","Purple","blue", "green","gray"]; //קביעת הצבעים

inputKeywordBox(); //קפיצה לפעולה המטפלת בקלט מילת המפתח

noLoop();

}

function draw() { //נקרא על ידי p5Js כל פעם שהתוכנית במצה loop איקס פעמים בשנייה

if(state == 'DrawKeyword'){ //מצב של קבלת מילת מפתח

if(StrIndex<KeyWord.length) //מצייר את מילת המפתח

drawKeyword (KeyWord);

else // סיים ועובר לשלב הבא

{

row=0;

column=0;

StrIndex=0;

sortKeyWord(); //מיון לוגי של מילת המפתח

drawKeywordNum(); //הצגה גרפית של סדר הא-ב במשפט

inputSentenceBox(); //מעבר לפונקציה שתשנה למצב הבא

noLoop();

}

}

else if(state == 'encrypt'){ //מצב של מצפין ההודעה

if(UserStr.length > 0){ //מציג את המשפט בתוך טבלת העמודות

if(StrIndex<UserStr.length)

drawOrigin(UserStr);

else //סיים להציג בטבלה ואם הטבלה לא התמלאה עד הסוף מוסיף x y z

{

if(column != KeyLen-1)

{

// StrIndex = StrIndex-(KeyLen-column-1);

let l = 'z'.charCodeAt(0) - (KeyLen-1-column);

for(i=0;i<KeyLen-1-column;i++)

{

UserStr += String.fromCharCode(l+i+1);

}

}

else // סיים למלא את הטבלה במלואה ועובר להציג את המשפטים לפי אופן ההצפנה

{

drawEncryptedOrdered(); //מציג את המשפטים לפי הסדר הלוגי של העמודות -לב ההצפנה!

noLoop();

}

}

}

}

else if(state == 'decrypt'){ //מצב מפענח

if(recivedStr.length > 0){ //מצייר את המשפט המוצפן בטבלת הפענוח לפי עמודות ולפי סדר הא-ב

if(StrIndex<recivedStr.length)

drawDecrypt(recivedStr);

else//מפענח את המשפט המוצפן אחרי הצגתו בטבלה

{

decryptStr = decryptStr.join("");

textAlign(LEFT);

textSize(SqSize/2);

text("the message is: \n" + decryptStr, SqSize, Ystart+(SqSize\*(columnLen+2)),SqSize); //הצגת המשפט המקורי

if(decryptStr.includes(UserStr) == true) //התראה קופצת למשתמש אם המשפט שהוא הכניס הוא גם המשפט המקורי

{

//fill("green");

//text("VERY GOOD !!! your guess was correct \n",windowWidth/2, windowHeight/2,SqSize);

Swal.fire({

position: 'center',

icon: 'success',

title: 'VERY GOOD !!! your guess is correct',

showConfirmButton: false,

//timer: 1500

})

}

else // התראה קופצת שמודיעה למשתמש שהוא טעה בפענוח

{

//fill("red");

//text(" :( bad guess \n",windowWidth/2, windowHeight/2,SqSize);

Swal.fire({

position: 'center',

icon: 'error',

title: ':( bad guess',

showConfirmButton: false,

//timer: 1500

})

}

noLoop();

}

}

}

else{

noLoop();

}

}

function updateKeyWord(data) { //לאחר קבלת הודעה מהשרת פעולה זו הופכת את המסך של המשתמש לורוד ומשנה את המצב במכונת המצבים למצב המציג את מילת המפתח שנקלטה

KeyWord = data;

KeyLen = KeyWord.length;

Xstart = SqSize;

Ystart = SqSize-(SqSize/4);

row=0;

column=0;

StrIndex=0;

buttonKeyWord.hide();

greetingKeyWord.remove();

inputKeyWord.remove();

background("pink"); // Set the background to pink

state = 'DrawKeyword'; // שינוי מצב לציור מילת הקוד

loop(); //קיראה לdraw

}

function decriptMessage (data) {//לאחר קבלת המשפט המוצפן מהשרת פונקציה זו מתריאה על קבלת הודעה ומשנה את הדגל למצב מקבל ההודעה

recivedStr = data;

Xstart = SqSize;

Ystart = SqSize\*2;

textSize(SqSize/2);

textAlign(LEFT);

greetingMessage.remove(); //מחיקת ההודעה לבקשת קלט מהמשתמש

fill("black");

text("got encrypted message :" + data, Xstart, Ystart); // Text wraps within text box

Swal.fire({ //התראה שקופצת ומבשרת על קבלת משפט ממשתמש אחד

position: 'center',

icon: 'info',

title: 'got encrypted message :' + data,

showConfirmButton: false,

timer: 2500

})

StrIndex=0;

DrawIndex=0;

Xstart = SqSize;

Ystart = SqSize\*4;

row=0;

isreceiver = true; //שינוי הדגל למצב מקבל ההודעה ולא מצפין ההודעה

//buttonMessage.hide();

greetingMessage.remove();

//inputMessage.remove();

//sel.remove();

//state = 'decrypt';

//loop();

}

function drawKeyword (stringToDraw) { //מצייר לפי צבעים את מילת הקוד

column = DrawIndex%KeyLen;

fill(colors[column]);

rect(Xstart, Ystart, SqSize, SqSize);

fill(50);

textSize(SqSize);

textAlign(CENTER, CENTER);

let currChar = stringToDraw[StrIndex];

if(currChar != ' ') //לא יקרה מצב שבו יהיה רווח כי עשיתי בדיקה כזו בהכנסת הקלט

{

text(currChar, Xstart, Ystart+(SqSize/2),SqSize); // Text wraps within text box

StrIndex++;

DrawIndex++;

Xstart+=SqSize;

}

}

function drawOrigin (stringToDraw) { //מצייר את המשפט המקורי בטבלה מסודרת לפי הא-ב של מילת המפתח

column = DrawIndex%KeyLen;

fill(colors[column]); //צבעים

let currChar = stringToDraw[StrIndex];

if(currChar != ' ')

{

rect(Xstart, Ystart, SqSize, SqSize);

fill(50);

textSize(SqSize);

textAlign(CENTER, CENTER);

text(currChar, Xstart, Ystart+(SqSize/2),SqSize); // Text wraps within text box

encryptStr[column][row]=currChar;

StrIndex++;

DrawIndex++;

Xstart+=SqSize;

if(DrawIndex%KeyLen==0)

{

Xstart = SqSize;

Ystart += SqSize;

row++;

}

}

else

{

StrIndex++;

}

}

function drawDecrypt (stringToDraw) { //מציג בטבלה בצורה גרפית לפי צבעים ולפי סדר התורים לפי הא-ב את הצפנת המשפט

//column = DrawIndex%KeyLen;

columnLen = stringToDraw.length/KeyLen;

let col = Math.floor(StrIndex/columnLen);

if(col >= KeyLen)

console.log(stringToDraw);

column = orderOfletters[col];

fill(colors[column]);

rect(Xstart+(SqSize\*column), Ystart, SqSize, SqSize);

fill(50);

textSize(SqSize);

textAlign(LEFT, LEFT);

//textAlign(CENTER, CENTER);

let currChar = stringToDraw[StrIndex];

text(currChar, Xstart+(SqSize\*column), Ystart,SqSize); // Text wraps within text box

decryptStr[column+(row\*KeyLen)]=currChar;

StrIndex++;

Ystart+=SqSize;

row++;

if(StrIndex%columnLen==0)

{

row=0;

Ystart = 4\*SqSize;

}

}

function drawEncryptedOrdered () { //מציג את המשפטים בשורות לפי הסדר הלוגי של העמודות -לב ההצפנה

//Ystart += SqSize;

let xx=0;

textSize(SqSize/2);

for(let k=0;k<KeyLen ;k++)

{

encryptStr[orderOfletters[k]] = encryptStr[orderOfletters[k]].join("");

Ystart += SqSize/2;

textAlign(LEFT);

fill(colors[orderOfletters[k]]); //צובע כל שורה בצבע המתאים להבנת ההצפנה

text( encryptStr[orderOfletters[k]], Xstart, Ystart+(SqSize/2),SqSize);

for(let y=0 ; y < encryptStr[k].length ; y++)

{

sendStr[xx]= encryptStr[orderOfletters[k]][y];

xx++;

}

}

Xstart = SqSize;

textSize(SqSize/2);

sendStr = sendStr.join("");

Ystart += SqSize;

textAlign(LEFT);

text( sendStr, Xstart, Ystart+(SqSize/2));

StrIndex=0;

DrawIndex=0;

row=0;

column=0;

drawKeywordNum();

isreceiver = false;

socket.emit('encriptedMessage',sendStr); //שולח את ההודעה המוצפנת על גבי הסוקט לשרת

noLoop();

}

function drawKeywordNum () { //מציג על גבי מילת הקוד את סדר הא-ב להצפנה קלה יותר

column = DrawIndex%KeyLen;

Xstart = SqSize;

Ystart = SqSize-(SqSize/4);

fill("white");

textSize(SqSize/2);

textAlign(RIGHT, TOP);

for(let k=0;k<KeyLen ;k++)

{

let currChar = k+1;

text(currChar, Xstart+(orderOfletters[k]\*SqSize), Ystart+(SqSize/2),SqSize); // Text wraps within text box

}

}

function sortKeyWord () { //יצירת מערך שישמור את סדר הא-ב במילת המפתח

orderOfletters = new Array(KeyLen);

var k=0;

for(let i = 'A'.charCodeAt(0); i <= 'Z'.charCodeAt(0); i++){

var currentChar = String.fromCharCode(i);

if(KeyWord.includes(currentChar)){

for (j=0; j<KeyLen; j++) {

if(KeyWord[j] == currentChar){

orderOfletters[k] = j;

k++;

}

}

}

}

}

function inputKeywordBox () { //יצירת כפתור ותיבת קלט למילת הקוד

inputKeyWord = createInput(); //תיבת טקסט

inputKeyWord.size(60);

inputKeyWord.position(Xstart , Ystart);

buttonKeyWord = createButton('submit'); //כפתור

buttonKeyWord.position(inputKeyWord.x + inputKeyWord.width, Ystart);

greetingKeyWord = createElement('h2', 'Enter your keyword:'); //הוראה למשתמש

greetingKeyWord.position(inputKeyWord.x, inputKeyWord.y-50);

buttonKeyWord.mousePressed(getKeyword); //כאשר יש לחיצה על הכפתור קריאה לפעולה הבאה

}

function getKeyword () { //לאחר קבלת קלט של מילת קוד הפעולה עוברת למצב הראשון במכונת המצבים, שולחת את מילת הקלט לשאר המשתמשים ומשנה את צבע המסך של השולח לירוק

if(greetingError) //לא בשימוש

greetingError.remove();

KeyWord = inputKeyWord.value();

KeyWord = trim(KeyWord); // remove space from begining and end of string

KeyWord = KeyWord.toUpperCase(); // make all chat uper case - Big letters

KeyLen = KeyWord.length;

if(KeyWord.match("^[a-zA-Z]\*$")) // make sure that oly alpha beit is inserted

{

if(KeyLen > 2 && KeyLen <=7 ) //תנאי המכריח את מילת הקלט להיות בין2 ל7 תווים

{

buttonKeyWord.hide();

greetingKeyWord.remove();

inputKeyWord.remove();

socket.emit('KeyWord',KeyWord); //שליחת מילת המפתח לשאר המשתמשים דרך השרת

Xstart = SqSize;

Ystart = SqSize-(SqSize/4);

row=0;

column=0;

StrIndex=0;

background("Green"); // Set the background to green

state= 'DrawKeyword'; //המצב הראשון במכונת מצבים-מצב הצגת מילת הקלט

loop();

}

else //כאשר התנאי לא מתקיים קופצת התראה למשתמש שהקלט אינו תקין עם הסבר מהו קלט תקין

Swal.fire({position: 'top',title: 'keyword length can be 3-7 characters'});

}

else //התראה למשתמש על קלט אינו תקין והסבר מהו קלט תקין

{

Swal.fire({position: 'top',title: 'keyword can be only A-Z a-z and 3-7 characters length'});

//greetingError = createElement('h2', 'keyword can be only A-Z a-z and 3-7 length');

//greetingError.position(inputKeyWord.x, inputKeyWord.y+20);

}

}

function inputSentenceBox () { //יצירת תיבת טקסט להכנסת משפט להצפנה וכפתור

Xstart = SqSize;

Ystart = 2.5\*SqSize;

inputMessage = createInput(); //יצירת תיבת קלט

inputMessage.size(300);

inputMessage.position(Xstart , Ystart);

inputMessage.size = 400;

buttonMessage = createButton('submit'); //יצירת כפתור

buttonMessage.position(inputMessage.x + inputMessage.width, inputMessage.y);

greetingMessage = createElement('h2', 'enter sentence to encrypt');

greetingMessage.position(inputMessage.x, inputMessage.y-50);

buttonMessage.mousePressed(getSentece); //אם לוחצים על הכפתור אחרי הכנסת משפט בתיבת הקלט עובר לפעולה הבאה

inputSentenceDropDownBox(); // אם המשתמש לא לוחץ על הכפתור ובוחר משפט ממאגר המשפטים עובר לפעולה הבאה

}

function getSentece () { //טיפול במשפט מתיבת הקלט או של המצפין או של המפענח תלוי במצב במכונת המצבים

UserStr = inputMessage.value();

UserStr= trim(UserStr);// מחיקת רווחים מתחילת המשפט ומסופו

processUserStr(); //טיפול בקלט המשתמש

}

function inputSentenceDropDownBox() { //יצירת אפשרות בחירת משפט ממאגר משפטים או של המצפין או של המפענח תלוי במצב במכונת המצבים

textAlign(CENTER);

Xstart = SqSize;

sel = createSelect();

sel.position(Xstart , Ystart+(SqSize/2));

sel.option("-----------------or select one from below ---------------------");

sel.option("Nothing shows a man's character more than what he laughs at");

sel.option("Life is like a mirror we get the best results when we smile at it");

sel.option("If you want happiness for a lifetime help someone else");

sel.option("The world is full of beautiful things including you");

sel.option("i'm on a seafood diet i see food and i eat it");

sel.option("My candle burns at both ends");

sel.option("אתה לא יכול לטפס על סולם ההצלחה עם הידיים בכיס");

sel.option("הגדרת המטרות היא הצעד הראשון בהפיכת הבלתי נראה לגלוי");

sel.option("שום דבר לא יעבוד אם אתה לא תעבוד");

sel.option("העבודה שלך הכי קלה, אתה בסך הכל צריך ללחוץ על כפתור");

sel.changed(SelectEvent); //כאשר נבחר משפט מהמאגר

}

function SelectEvent() { // כאשר נבחר משפט ממכונת המצבים

UserStr = sel.value(); //הכנסת המשפט למשתנה המתאים

processUserStr();//טיפול בקלט המשתמש

}

function processUserStr() { //עושה שני תפקידים- תלוי אם המשתמש הוא שולח ההודעה או מקבל ההודעה

if(isreceiver == false) //דגל=שולח ההודעה, משנה את מכונת המצבים למצב מצפין ויוצר מערך דו מימדי ריק

{

if(UserStr.length > 2)

{

buttonMessage.hide();

greetingMessage.remove();

for (let x = 0; x < KeyLen; x++) {

encryptStr[x] = []; // create nested array

for (let y = 0; y <Math.ceil(UserStr.length/KeyLen); y++)

encryptStr[x][y] = "";

}

Ystart = 3.5\*SqSize;

state= 'encrypt'; //מצב מצפין

loop();

}

}

else //דגל= מקבל ההודעה, משנה את מכונת המצבים למצב מפענח ומוחק מהמשפט שהתקבל את הרווחים

{

UserStr= trim(UserStr);

UserStr = UserStr.replace(/\s/g, ''); // remove all spaces in user guess string

state = 'decrypt'; //מצב מפענח

loop();

}

}

# ריפלקציה

תהליך העבודה על הפרוייקט היה ארוך, קשה ואינטנסיבי. פיתחתי משחק משלי, בשפה שלא הכרתי, בסביבית עבודה שלא הכרתי והשתמשתי בטכנולוגיות עבודה רבות שלא נגעתי בהן או שמעתי עליהן מעולם. לימוד השפה והטכנולוגיות דרשו המון זמן ומשמעת עצמית. בנוסף, היו קשיים רבים במהלך כתיבת הפרוייקט שהייתי צריכה לשבת שעות על גבי שעות ואפילו ימים בכדי להבין היכן הטעות ואיך ניתן לתקן אותה. זאת ועוד, בתיק פרוייקט הצטרכתי להשתמש בתרשימים שלא התנסתי בהם בעבר באף עבודה. הייתי צריכה ללמוד לשלב בין הלימודים, הצופים ובניית הפרוייקט. אני תלמידה שהלימודים חשובים לה יותר מהכל וחשוב לי להצטיין בכל מקצוע שקיים ולמדתי לסדר לעצמי את זמן העבודה על הפרוייקט ואת זמן הלימדה לשאר המקצועות. במסגרת הצופים אני אחראית על פרוייקטים למען הקהילה כגון ארגון אירועי התרמה, ביקור קשישים ועזרה בגני ילדים לכן הייתי צריכה למצוא דרך לשלב הכל יחד.

גם תקופת הקורונה הקשתה על תהליך הפרוייקט, מרגע הפסקת הלימודים בכל יום נשלחו המון עבודות להגשה מבית הספר והייתי צריכה לסדר את הזמן כך שאצליח גם לסיים את כל העבודות וגם לסיים את תיק הפרוייקט.

אך למרות כל הקשיים והאתגרים, נהנתי מאוד מכל התהליך! אני ילדה מאוד סקרנית שאוהבת ללמוד ולהתפתח. החקר על שיטת ההצפנה, על השפה החדשה ועל סביבת העבודה שלא הכרתי היה מעניין (וארוך) ואני מרגישה שכמות הדברים שלמדתי מהפרוייקט הזה היא ענקית! בנוסף לכך, אני מאוד אוהבת לעצב וליצור, ובפרוייקט משלי שאני יוצרת מאפס, יכולתי לתת ביטוי אישי משלי בכל דבר ודבר. הצבעים, המשפטים והתצוגה הגרפית, אפילו התיק פרוייקט, הכל לפי הטעם והעיצובים שאני רציתי מה שגרם לי להנות עוד יותר מבניית הפרוייקט.

ההתמודדות עם הקשיים והאתגרים באופן עצמאי סיפקו אותי מאוד וגרמו לי להבין כי אין דבר העומד בפני ברצון. הפרוייקט העמיד בפניי אתגרים חדשים וקשים ולמדתי להעמיד רף גבוה אליו אני שואפת להגיע ולהבין שעם המון עבודה ומאמץ אני מצליחה.

החקר בהמלך פיתוח הפרוייקט, ההתנסות בפיתוח התוכנה, למידת השפה החדשה, העבודה עם כלים שונים שמתאימים לפרוייקט שלי כגון כלים לניהול קבצים, הפעלת שרתים, עבודה עם client server, והתנסות עם ספריות שונות ועוד, תרמו לי רבות והעינקו לי ניסיון רב. נפתחו לי עולמות חדשים בעולם התכנות והבנתי כיצד מה שאני לומדת בבית הספר יכול לעזור לי בעתיד וכיצד ניתן ליצור דברים שימושיים ומגניבים.

העבודה על הפרוייקט גם חיברה וחיזקה את הקשר שלי עם התלמידים האחרים מבית הספר שלי שעשו פרוייקט משלהם. כולנו שיתפנו חוויות ורגשות לגבי התהליך, התעניינו אחד בשני ואני שמחה מכך מאוד. לראות ולשמוע כיצד כל אחד מתקדם בפרוייקט שלו נתן מוטיבציה להמשיך ולהשקיע בפרוייקט ככל שניתן.

# ביבליוגרפיה

1. Github- אתר שמאחסן את הקבצים על ידי התוכנה git לניהול קבצים <https://github.com/>
2. p5.js- ספרייה <https://p5js.org>
3. לימוד השפה Java Script ופעולות שונות ומגוונות שניתן לעשות איתה באמצעות עמוד היוטיוב הזה: <https://www.youtube.com/user/shiffman>
4. פלטפורמה למכונות וירטואליות שבה ניתן לשכור שירות של מכונה וירטואלית-DigitalOcean <https://www.digitalocean.com/?utm_campaign=DO_Dev_Awareness_G_Search_B_Generic_Alpha&utm_adgroup=digital_ocean&_keyword=digital%20ocean&_device=c&_copytype=&_adposition=&utm_medium=brand_sem&utm_source=google&_dkitrig=&_2dkitrig=&gclid=CjwKCAjwwYP2BRBGEiwAkoBpAiYbNVe9v4PXcyRawt-suNa3tyIAryUDO8SVBelKPz2chvuoeT3IYxoCzAUQAvD_BwE>
5. goDaddy פלטפורה המספקת כתובות דומיין –<https://il.godaddy.com/en/offers/domains/domains?isc=ildomILS1&countryview=1&currencyType=ILS&gclid=CjwKCAjwwYP2BRBGEiwAkoBpAlfpYBf3EpBxeMm2RiNra5LjMwcAyrP4jycFQNZZzghEOY618iAQ6RoCgHYQAvD_BwE&gclsrc=aw.ds>
6. יוטיוב להסברים על שיטת ההצפנה- https://youtu.be/ODXfkZ4d7n4
7. מצגת של ד"ר עמית קליינמן על הפנת העמודות
8. בלוגים שונים של שאלות ותשובות לגבי שפות תיכנות לדוגמא- <https://stackoverflow.com/> <https://www.geeksforgeeks.org/>