**המחלקה להנדסת תוכנה**

**פרויקט גמר – תשע"ח**

**RSA מבוזר למערכות IoT**

**Distributed RSA For IoT**

**מאת**

**שרה ספרין**

**רעות נגר**

**מנחה אקדמי: דר' גיא לשם אישור: תאריך:**

**רכז הפרויקטים: דר' אסף שפנייר אישור: תאריך:**

מערכות ניהול הפרויקט:

|  |  |  |
| --- | --- | --- |
| # | מערכת | מיקום |
| 1 | מאגר קוד | https://github.com/reutnagar/distributed-RSA-for-IoT |
| 2 | יומן | https://trello.com/b/DkjV5sEx/a |
|  |  |  |
|  |  |  |

מומלץ למלא בשלב ההצעה (אך לא חייב - יושלם בדוחות הבאים):

* תקציר
* תוכן העניינים
* מילון מונחים, סימנים וקיצורים

# מבוא

## אבטחת מידע

אבטחת מידע (באנגלית: Information Security) היא ענף העוסק בהגנה של מידע ומערכות מידע מפני כל גישה למידע שאינה ע"י גורמים מאושרים, לכך עליה לספק את שלושת הבאים: סודיות, שלמות וזמינות של המערכות והמידע בהן. אבטחת מידע היא תחום מתקדם מאוד בימינו. האפשרויות הרבות שעומדות לתוקפים של מערכות ממוחשבות להזיק בתחומים כמו פרטיות, פיננסים וביטחון מניעה את האנושות להגן ככל האפשר על מערכות אלו. מושקעים משאבים רבים בעיצוב המערכות, קידוד ותחזוקה שוטפת כדי לאתר פרצות אבטחה מוקדם ככל האפשר. עם התקדמות היכולות של התוקפים נדרשות לעתים פריצות דרך מצד קהילת המפתחים ולכן אבטחת מידע זהו תחום שמושקעים בו כסף ומשאבים רבים במיוחד על מנת לחקור ולגלות דרכי הגנה חדשות ויעילות יותר להתמודדות מול התוקפים[1].

כוח יישומי חשוב באבטחת המידע היא קריפטוגרפיה. זהו ענף במתמטיקה ומדעי המחשב העוסק במחקר ופיתוח שיטות אבטחת מידע ותקשורת נתונים, ומייצר שיטות למימוש בפועל של מושגי אבטחת המידע. הגנה זו מבוצעת על ידי הצפנת המידע בעזרת פונקציית הצפנה כלשהי, ושימוש במפתח (Key) שהוא רצף תווים סודי שאינו ידוע לתוקף.  הצופן   (Cipher) הוא כתב הסתר שמתקבל על ידי הפעלת פונקציית ההצפנה על טקסט הקלט. פונקציה הצפנה אדיאלית היא כזו שבהינתן הצופן- הפלט, לא ניתן להסיק ממנו מידע על הקלט.

## הצפנת RSA

הצפנת RSA (על שם מקימיה: Rivest, Shamir and Adleman) היא ההצפנה הא-סימטרית המעשית הראשונה שפותחה (1978) שמשמשת לרוב להפצת מפתחות סימטריים. חוזקה מתבסס על קושי פירוק של מכפלות לגורמים ראשוניים. כיום הצפנת RSA נחשבת לאחת הבטוחות ביותר שקיימות ונמצאת בשימוש נרחב במערכות השונות.

הצפנת RSA היא שיטה אסימטרית הנבדלת משיטה סימטרית בכך, שבשיטה הסימטרית אותו מפתח משמש להצפנה ולפענוח. בשיטה הא-סימטרית מקבל הצופן מפרסם את מפתח ההצפנה כמפתח פומבי (שניתן לפרסמו ברבים ללא חשש), בעזרתו מבוצעת ההצפנה ואילו הפענוח מתבצע אך ורק באמצעות המפתח הפרטי (הסודי) שנשאר בידיו בכך נחסכת בעיית העברת מפתח ההצפנה. לשיטה יש ביסוס מתמטי מקיף, והיא נשענת על העובדה שקל מאוד ליצור מספרים ראשוניים ענקיים, אך קשה לגלותם מתוך המכפלה שלהם. כך בנוי המפתח מחלק סודי וחלק פומבי אשר רק בהינתן שניהם ניתן לגלותו[2].

### פירוט האלגוריתם

1. בוחרים שני מספרים ראשוניים גדולים **p** ו- **q**. עפ"י המספרים האלו מייצרים את שני המספרים:

**n**=p\*q ו- **e** (זר ל p-1 ול q-1 ) שהם המפתחות הציבוריים.

1. מחשבים את המפתח הפרטי **d** כך:

d\*e = 1 mod (p-1)(q-1)

1. על מנת להצפין הודעה **m** כלשהי, מקטינים אותה כך שאורכה יהיה קטן יותר מ-n. ואז מצפינים בעזרת הנוסחה:

Encn(m) := me(mod n)

מתקבל **c**, שהוא הקידוד המוצפן.

    4. הפענוח נעשה ע"י הנוסחה:

Decd(c) := cd (mod n) = m

האופי המתמטי של הנוסחאות הוא כזה שלא ניתן לשחזר את m אפילו בהינתן e ו-n, אלא אך ורק באמצעות d. כמובן, יעילות ההצפנה נעשית לפי גודל המפתחות, ולרוב משתמשים במפתחות בגודל 128 בתים לפחות.

### שימושים וגרסאות

ל-RSA קיימות מספר גרסאות שונות ששיפרו את ההצפנה במהלך 30 השנים האחרונות. כך למשל ניתן למצוא את RAS-CRT, Batch RSA, Multi-power RSA ועוד כמה גרסאות שונות. את RSA ניתן למצוא היום במרבית תחומי אבטחת המידע והוא משמש לחתימות דיגיטליות, הצפנות דוא"ל ומידע כלליות, שרתי SSL וגם בהצפנות WPA תחת אימות המשתמש וההצפנה.

## מכשירי IoT

בעולם הטכנולוגי כיום קיימת מגמה מואצת להפוך כל מכשיר המכיל שבב אלקטרוני לבעל יכולת חיבור לרשת. כבר כיום ניתן לראות מכשירים מכל הסוגים שקיימת בהם אפשרות חיבור לאינטרנט. לדוגמה: מצלמות, מדפסות, שלטי מזגן ועוד. החזון לחבר כל מכשיר חשמלי לרשת נובע מן הרצון שמכשירים כאלו ישדרו למכשירים ומערכות סביבם את המידע שבידם, ויקבלו מידע מן הרשת לגבי אירועים ותרחישים שונים. הודעות אלו ישדרגו את יכולותיהם ופעילותם והם יוכלו להתנהג בצורה יותר "חכמה", להסיק מסקנות ולפעול אוטומטית על פיהם ללא התערבות אנושית. לדוגמה, כאשר השבב של מערכת החלונות המותקנת ב"בית חכם" קולט שידור ממערכת המיזוג על הפעלת המזגן, הוא יודע לסגור את החלונות המתאימים באופן אוטומטי כדי לייעל את פעולת המיזוג.

מגמה זאת נקראת:"אינטרנט של דברים" (IoT- Internet Of Things). זוהי רשת של חפצים פיזיים, או "דברים" המשובצים באלקטרוניקה, תוכנה וחיישנים המאפשרים תקשורת מתקדמת בין החפצים ויכולות איסוף והחלפת מידע. רשת זו צפויה להוביל לאוטומציה בתחומים רבים. כיום ישנה התפתחות נרחבת בתחום ה IoT, למשל "הבית החכם", שבו כל המכשירים מחוברים לרשת וניתן להפעיל אותם בשלט רחוק ולתאם בין פעולותיהם. תחום הIoT צפוי לגלגל מחזור של כ20 ביליון דולר בשנת 2020, על פי הודעת חברת 'סיסקו' העולמית, ומושקעים בו משאבים רבים לפיתוח מצד החברות בתחום החומרה והתוכנה.

לקראת השינוי הזה יידרש שיפור גם ברמות האבטחה המקובלות כיום בקרב מכשירים כאלו, שעצם חיבורם לרשת חושף אותם להתקפות חיצוניות והם עלולים להוות טרף קל לתוקף. בפרויקט זה נתמקד בחקירת פתרונות אבטחה, בפרט בשימוש בהצפנת RSA, עבור תחום ה"אינטרנט של הדברים" ויצירת פתרונות אבטחה ייעודיים עבורו המתחשבים בחוזקות והחולשות של המוצרים הקיימים בשוק[3].

# תיאור הבעיה

בהבנה של הצורך הבסיסי באבטחה ראויה למידע המשתמש והכרה במגבלות המשאבים של מכשירים אלקטרוניים קטנים, ניתן להבחין במספר בעיות ביישום אבטחה במכשירי IoT:

* מכיון שמכשירי הIoT הינם מכשירים זולים וקטנים לרוב, ומאופיינים ביכולות עיבוד חלשות, ומשאבים נוספים דלים כמו: זיכרון, שידור וחישה, לכן להטמיע בהם יכולות אבטחה מתקדמות כמו שקיימות במערכות מחשבים גדולות זוהי משימה קשה וכמעט לא נתמכת מבחינת החומרה של ה IoT.
* מכיוון שהשימוש ב IoT הוא כמכשירים שיש להם בדרך כלל תפקיד עיקרי ייעודי והחיבור לרשת רק מוסיף להם יתרון, הם לא נתפסו עד היום בציבור כבעלי ענין עבור תוקפים. אך עם השימוש הגובר בהם מיום ליום נוצלו פרצות האבטחה שבמכשירים מסוג זה לתקיפת מערכות רגישות, כמו מצלמות אבטחה, מדפסות ועוד.
* פתרונות האבטחה שכן מיושמים כיום בתחום ה IoT הים ייעודיים עבור מכשיר מסוג מסוים, ומוטמעים על ידי היצרן. לא נלקחת בחשבון התאמה לשוק המוצרים הכולל של IoT, ולכן פתרונות אלו אינם מתאימים מבחינת תצורה, מגבלות משאבים וייעוד, עבור כל התחום.

על מנת לפתור את הבעיות הנ"ל נדרש פיתוח אבטחתי חדש שיענה על דרישות האבטחה הגבוהות בשוק, יחד עם המגבלות המאפיינות את מכשירי הIoT.

# תיאור הפתרון

הרעיון באופן כללי:

מכיוון שהתקני ה- IoT בעלי כוחות חישוב קטנים ויכולת עיבוד קטנה, אבטחת מכשירים אלו היא לא אפשרית בתנאים הקיימים. לצורך אבטחה טובה של התקנים מסוג זה יש צורך להשתמש באלגוריתם כדוגמת RSA על מנת לאבטח כראוי. מימוש אבטחת RSA במתכונתה הרגילה דורשת יכולת חישוב ועיבוד חזקים, על מנת לייצר מס' ראשוניים גדולים, מה שלא שייך ב-IoT.

כאן מגיע הפתרון שלנו שהוא IoT מבוזר. הפתרון שלנו מתבסס על ההנחה שבעוד כמה שנים יהיו בבתים מכשירים רבים שיהיו מחוברים לרשת. כלומר בכל מכשיר חשמלי יהיה מעבד קטן בעל נק' גישה לרשת, כלומר IoT (מקרר, תנור, מכונת כביסה, טייפ או מערכת, שלט של מזגן וכ"ו).

אנחנו ננצל עובדה זו, ובמקום שכל התקן ידאג רק לעצמו, נאחד את כוחות החישוב של כל ההתקנים בבית על מנת לאבטח את המכשירים. במקום מחשב אחד בעל יכולת חישוב גדולה שייצר מספרים ראשוניים גדולים וידאג להפצתם , נבזר את החישוב על פני כמה מכשירים קטנים בעלי יכולות חישוב קטנות.

עבודה זו תציג יישום מקביל חדשני של שידור מפתח ההצפנה עבור מכשירים קטנים, באמצעות עיבוד מקבילי מופץ של RSA.

עם כוח מחשוב מבוזר (מיקרו-מעבדים) טכנולוגיה ופיתוח טכנולוגיה מקבילה, כוח המחשוב של מערכות המחשב יכול לקבל שדרוג ענק. באמצעות ריבוי הליכי הטכנולוגיה ושיפור היעילות של נהלים באמצעות העברת הודעה במקביל ממשק צמתים מרובים יכולים לאפשר במשותף את החישוב על מנת לקצר את הפעולה.

בפרויקט זה נתמקד ב- 2 שיטות חדשות במקבול RSA. השיטה הראשונה מתמקדת ברגישות המערכת לאורכו של המפתח המופץ, השיטה השנייה מתמקדת בבחירת מספרים ראשוניים קצרים p ו- q ובשיתוף מחדש של חלקי המפתח למפתח אחד גדול, השיטה השלישית מתמקדת ב- RSA המקביל.

## **איך זה עובד מבחינה מעשית?**

בפרויקט זה נתמקד בפיתוח 2 פרוטוקולים חדשים:

## **שיפור אלגוריתם הפצת מפתחות RSA באופן הבא:**

ערכת נתוני בדיקת RSA:

א. כדי להבטיח תוצאות דומות, נשתמש באותה ערכת נתונים לבדיקת תהליך הבדיקה כולה.

ב. הכנת ערכת נתוני הבדיקה המשותפת:

ג. נשתמש בפונ' RANDOM כדי ליצור רשומות באורך שונה. נתחיל עם רשומה באורך 50 תווים, אח"כ באורך 2x50 ונמשיך כך i ^2 X50 עד ל- i-8

בדיקת תוכנה:

א. תקן RSA: ישנם יישומים רבים של RSA באמצעות אלגוריתמים ושפות שונות.

ב. הפצה מודולארית אקספוננציאלית.

ג. RSA מואץ:  גירסה מיוחדת שפיתחנו.

**בדיקת תצורה:**

א. תצורה א:  Arduino יחיד עם מעבד ואחסון מינימאליים.

ב. תצורה ב': 8 יחידות Arduino (כמו לעיל) מחוברות זה לזה.

בדיקת השערות:

השערה א':

* ניצול משאבי RSA [כלומר CPU ואחסון] הוא ביחס לאורך ההודעה המוצפנת.
* בדיקה: בצע את כל היישומים של RSA, תוך שימוש במערך הבדיקה [מההודעות הקצרות ועד להודעות ארוכות] עד שהתהליך נכשל.
* נתוני בדיקה: נתוני RSA Test מוגדרים.
* תצורה: תצורה א'.
* הפלט הצפוי עבור כל רשומה שנבדקה: זמן ביצועים, ניצול זיכרון וניצול אחסון.

השערה ב':

* RSA מבוזר (RSA עם האצת מחשבון אקספוננציאלי מודולרי) דורש פחות משאבים מכל יישום סטנדרטי של RSA
* בדיקה: חזור על הבדיקה עם RSA מבוזר

השערה ג':

* האצה אקספוננציאלית מודולארית ניתנת לביצוע מקבילי
* בדיקה: ביצוע אקספוננציאלי מודולארי מואץ עבור a^b mod n
* בדיקת נתונים: השתמש בערכים רנדומאליים ל- a,b,n עם אורכים שונים בעלי 20,40,60,80,100,150,200,250 ספרות.
* תצורה: הרץ את הבדיקה פעמיים, אחת עם תצורה א' ופעם שנייה עם תצורה ב'
* הפלט הצפוי עבור כל נוסחה שנבדקה עבור a^b mod n: זמן הביצוע, ניצול זיכרון וניצול האחסון.

השערה ד':

* modular exponentiation מואץ מהיר יותר מ-modular exponentiation רגיל
* בדיקה: בדיקה חוזרת של השערה ג'.

## **פרוטוקול "לחיצת יד" חדש עבור רשת התקני IoT על ידי מערכת חדשה לניהול מפתחות המבוססת על שיתוף מפתחות הסתברותי בין ההתקנים.**

## להל"ן הפרוטוקול:

1. צור קבוצה של התקני IoT  עם תקשורת בינהם.
2. הגדר מנהיג לקבוצה (ההתקן בעל הכוח הרב ביותר).
3. עבור כל התקן בקבוצה, המנהיג נדרש לשלוח תת קבוצה של מפתחות (k) מתוך מאגר מפתחות שהוא נדרש לייצר.

גודל המאגר:

המנהיג צריך לקבוע מה יהיה גודל המאגר, P מתבסס על גודל הזיכרון הפיזי של המכשיר, ואת ההסתברות הנדרשת על ידי המערכת שנועדה להבטיח חפיפה (לפחות מפתח משותף אחד בין 2 התקני IoT ).

האלגוריתם למציאת גודל תת הקבוצה:

M - גודל הזיכרון הפיזי (לדוג' 32M).

n - מספר התקני ה-IoT ברשת.

Pc  - ההסתברות שלשני התקני IoT יש קישוריות באופן ודאי.

k - גודל הקבוצה של המפתחות מתבסס על M   k מוגדר ע"י הגבול של M.

'n - גודל השכונה של צומת ברשת האלחוטית .

p' - ההסתברות שלשני צמתים קיים מפתח משותף.

חשב את c, כאשר c קבוע:

https://lh5.googleusercontent.com/oPNwTwULAVGT9zdLpXk5pTttHDa_sIZs_U-QyxZnAUCoftw336Uk6GT9pk_lrsfd-j5esOgIO6CXhcXyzGpM8aatGVezNo2ZrpgrN0tqWSpEh2pjTDc72C3IT_vH42S1395BISTb

חשב את p: ההסתברות ששני צמתים מחוברים ישירות:



חשב את d: הערך המצופה של הצומת:

https://lh5.googleusercontent.com/spCiRq3CDPin_W1-VfwLs7urZYRMAPEJaIDiduLsjHN7VTEAZ7CkXGX0MExFbsL74QZ74K5rt47J9hrtaYNc-pxNTmoy3QEAOk7lZw7cx12KbCZD3V0_gVaFDVwx6_qpx8CjWgo6

חשב את p' :

d ניתן מהשלב הראשון ו- n' נתון, מספר הצמתים בשכונה של הצומת:



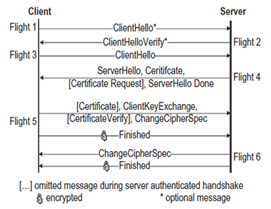
בהתחשב בערך של p', השתמש במשוואה הבאה כדי לחלץ את הערך של P:



מ-p' , כעת נוכל לחשב את P ( גודל המאגר)[4].

4) בהינתן גודל המאגר, P, כמו שחושב באלגוריתם המוצג בשלב 3, המנהיג צריך לייצר מאגר של מפתחות בגודל P (לפחות 1000), לכל מפתח במאגר יוסף מספר סידורי (index).

5) המנהיג יוצר  'לחיצת יד' מאומתת לחלוטין עם כל הקבוצה.



6) בהתבסס על תקשורת 'לחיצת היד' המאומתת לחלוטין, המנהיג שולח לכל חבר בקבוצה תת קבוצה שונה של מפתחות.

7) בהתבסס על תת קבוצת המפתחות שכל התקן מחזיק, 'לחיצת יד' מאומתת חדשה תהיה קלה.

8) המנהיג ישלח תת קבוצה חדשה של מפתחות לכל התקן שיצטרף לקבוצה.

## תיאור הכלים המשמשים לפתרון

בפרויקט שלנו אנחנו נעבוד עם מכשיר Andruino , מכשיר בעל קלט, פלט ויכולת עיבוד קטנה על מנת לבדוק וליישם את הרעיון.

הכתיבה תיעשה בשפת Python , על מנת שנוכל להעיזר בספריות שלה, שיקלו ממנה לעומת כתיבה ב- C,C++.

# סקירת עבודות דומות בספרות והשוואה

סקרנו מס' פתרונות אפשריים שהוצעו עבור אבטחה ב- IoT, אולם לכל אחד מן הפתרונות קיימים חסרונות:

* שימוש בענן

ישנו פתרון אבטחה להתקניIoT המסתמך על שימוש בענן על מנת להשיג את האבטחה הרצויה. כל התקן ברשת יתחבר לשירות בענן שיתמוך בניהול האבטחה של כל ההתקנים, ומולו יתבצעו פעולות האימות וההצפנה[5].

פתרון זה דורש ניהול של שירות בענן, וזו תקורה שדורשת משאבים נוספים, בנוסף, יהיה צורך בהגדרת ספקים אמינים לכזה שירות, ופתרון במקרה של התחזות. במחקר שלנו אנו מנסים להביא את השליטה באבטחה להיות בבלעדיות אצל רשת ההתקנים המקומית, ללא קישור לשירות חיצוני.

* TMP:

פתרון זה מסתמך על מכשיר הTPM לביצוע פעולות קריפטוגרפיות ונתינת שירותי הצפנה למכשירים ברשת[6]. זה נראה אמנם רעיון ישים,

אך החיסרון בו שדרוש מכשיר TPM כזה עבור כל רשת IoT, וזה גובה עלות נוספת. בפרויקט שלנו אנו מממשים פתרון אבטחה שמתבסס אך ורק על מכשירים הקיימים ברשת, ללא עלות נוספת.

* ארכיטקטורת IoT מאובטחת לערים חכמות המטפלת בפגיעויות במערכות IoT מסורתיות:

הארכיטקטורה כוללת רשתות שחורות ומערכת ניהול מרכזית (KMS) המספקות סודיות, שלמות, פרטיות והפצה מרכזית יעילה. המטרה הייתה לספק שירותי אבטחה הממתנים את הפגיעות של רשתות IoT בשכבות הקישור והרשת, במיוחד עבור נתונים קריטיים.

החסרונות של גישה זו כוללים היעדר פתרון פרטיות להגדרת מיקום המכשיר ואיתור ניתוב חדש עבור צמתים ב- IoT שנוצרו על ידי הצפנת כותרת שנרדמת, מה שמוביל לאובדן נתונים.

* ארכיטקטורת SDN לפיתוח יישומי IoT כדי לחסל את אופי האבטחה גמיש של רשתות מסורתיות:

ארכיטקטורת SDN אומצה על מנת לספק בסיס לפיתוח מערכת אבטחה מאובטחת שמאפשרת למנהלי מערכות להציג את העולם באופן גלוי של איומים אפשריים להתקפות ברשת ה- IoT ולספק להם את הזכות לשלוט ברשת מפני האיומים.

עם זאת, אבטחה, מדרגיות ואמינות הן חלק מהחסרונות של רשתות SDN. ההפרדה בין מטוסי הבקרה והנתונים של ה- SDN גורמת לביצועים ירודים בעיבוד חבילות, אשר מובילה לבעיות משמעותיות, כגון עיכוב או אובדן של חבילות ומפיצה התקפות DoS (DDoS).

* ארכיטקטורת אבטחה חדשה המבוססת על SDN עבור ה- IoT, הידועה גם בשם תחום ה- SDN באמצעות בקרי הגבול:

המחברים תיארו כיצד ניתן להשתמש ב- SDN כדי לחבר בין התקני IoT הטרוגניים, כיצד ניתן לשפר את האבטחה של כל דומיין, וכיצד ניתן לחלק את כללי האבטחה מבלי לפגוע בביטחון של כל תחום.

עם זאת, המחברים לא היו מסוגלים להתמודד עם האתגר של הבטחת תעבורה רצויה ולא רצויה והגנה על הארגון, אשר הם החסרונות העיקריים של שימוש בבקרי הגבול.

* פרוטוקול לניהול מפתחות בצורה קלה:

הפרוטוקול תלוי בהתאמות של רכיבי אבטחה שונים ב- IoT כדי להגדיר ערוצי תקשורת מאובטחים ומוגנים עבור צמתים מוגבלים ודברים אלחוטיים. במהלך העברת הנתונים לאורך הערוץ, הפרוטוקול מבטיח סודיות נתונים ואימות צומת מוגבל.

עם זאת, פרוטוקול האבטחה מוגבל לפריקת פרימיטיבים קריפטוגרפיים כבדים למפלגות לא רצויות, ואינו מפרט את ההתאמה הנדרשת בין תקורה לתקשורת לבין מספר צדדים שלישיים]7].

# נספחים

## רשימת ספרות \ ביבליוגרפיה

[1] “אבטחת מידע – ויקיפדיה.” [Online]. Available: https://he.wikipedia.org/wiki/אבטחת\_מידע. [Accessed: 19-Nov-2017].

[2] “RSA – ויקיפדיה.” [Online]. Available: https://he.wikipedia.org/wiki/RSA. [Accessed: 19-Nov-2017].

[3] “האינטרנט של הדברים – ויקיפדיה.” [Online]. Available: https://he.wikipedia.org/wiki/האינטרנט\_של\_הדברים. [Accessed: 19-Nov-2017].

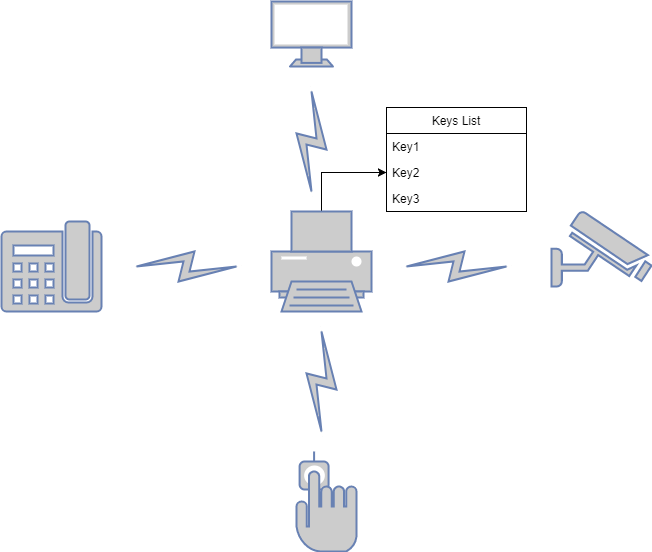
[4] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” *Proc. 9th ACM Conf. Comput. Commun. Secur.*, pp. 41–47, 2002.

[5] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, “Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, 2018.

[6] H. Hamadeh, S. Chaudhuri, and A. Tyagi, “Area, energy, and time assessment for a distributed TPM for distributed trust in IoT clusters,” *Integr. VLSI J.*, vol. 58, no. December 2016, pp. 267–273, 2017.

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” *J. Netw. Comput. Appl.*, vol. 88, no. March, pp. 10–28, 2017.

## תרשימים וטבלאות

מראה רשת בעלת RSA מבוזר ב"בית חכם". המכשיר המנהיג הוא המדפסת. בידיו נמצאת רשימת המפתחות.

## תכנון הפרויקט

|  |  |
| --- | --- |
| 19.1.2018 | יצירת קבוצת התקני IoT עם תקשורת בינהם |
| 5.5.2018 | הגדרת מנהיג לקבוצה |
| 26.5.2018 | שליחת K מפתחות ע"י המנהיג לכל התקן בקבוצה |

## טבלת סיכונים

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **הסיכון** | **חומרה** | **מענה אפשרי** |
|  | השערת המחקר אינה נכונה | 5 | ניתוח ספרות מעמיק |
|  | אי עמידה בזמני מימוש האלגוריתם | 4 | הערכת יכולות והערכות בהתאם |
|  | דרישות השוק משתנות | 3 | גמישות בשינוי המחקר והאלגוריתם |
|  | מתפרסם מחקר דומה | 4 | שמירה על סודיות |