# מנגנון הצפנה WEP

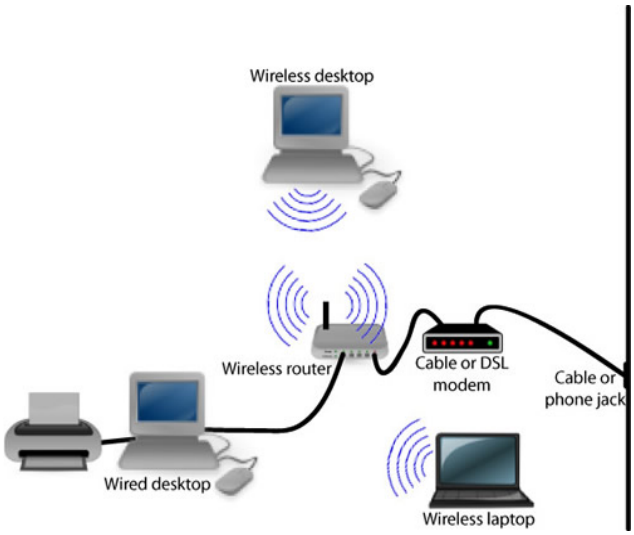
מאת הרצל לוי

## מבוא – IEEE 802.11

IEEE 802.11 זהו אוסף סטנדרטים הנושאים את הרשת המקומית האלחוטית, או בשמה הנפוץ WLAN (Wireless Local Area Network), בתדרים של 2.4, 3.6, ו-5GHz.

משפחת ה-802.11 מכילות שיטות אפנון (מודולציה) לצורך העברת המידע באוויר ושימוש באותו פרוטוקול בסיסי שמשמש לרשת מקומית קווית (LAN).

הפרוטוקול הראשון של ה-802.11 הוצג בשנת 1997, אך הגירסה 802.11b היא זו הראשונה שהופצה והתקבלה בשנת 1999. כיום ישנם גירסאות נוספות שכוללות שיפורים ותוספות והנפוצות מביניהן, הן הגירסאות 802.11b ו-802.11g.

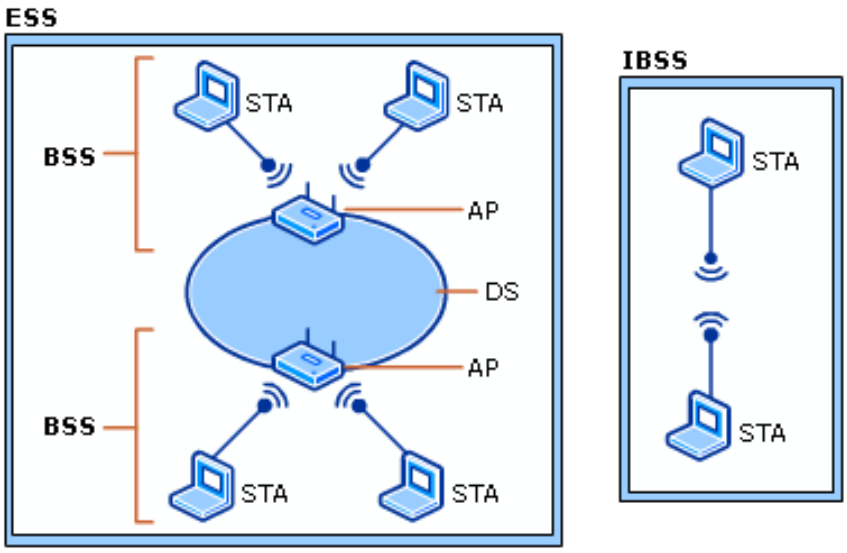


### מבנה ה-802.11

המבנה הלוגי של ה-802.11 מכיל מספר מרכיבים עיקריים: תחנה (STA), נקודת גישה אלחוטית (AP), מערך שירות בסיסי עצמאי (IBSS), מערך שירות בסיסי (BSS), מערכת הפצה (DS), ומערכת מורחבת (ESS).

- IBSS זוהי רשת אלחוטית, מכילה לפחות שתי STA שעובדות ללא תלות במערכת הפצה DS. רשת זו נקראת גם רשת אד-הוק (Ad hoc wireless network).
- BSS זוהי רשת אלחוטית, מכילה AP אחד התומך באחד או מספר קליינטים אלחוטיים. רשת זו נקראת גם רשת אלחוטית בסיסית. כל ה-STA ברשת BSS מתקשרים דרך ה-AP. ה-AP משמש גם כמתווך לרשת ה-LAN הקווית וגם כמגשר בין הרשת הקווית לתחנות (STA).

האיור הבא ממחיש את ההסבר הנ"ל:



## אבטחת מידע ברשת אלחוטית

צורת הגישה לרשת האלחוטית היא שונה משמעותית מצורת הגישה לרשת הקווית. לרשת האלחוטית חסר את הפרטיות המינימלית שמקבלים מהרשת הקווית. בעוד שהרשת הקווית יכולה להחשף רק למי שיש גישה פיזית לנקודת רשת, הרשת האלחוטית יכולה להחשף לכל מי שנמצא בטווח השידור של הרשת ויש לו אנטנה מתאימה (אנטנה שמשולבת כיום כמעט בכל מחשב נייד).

עקב עובדה זו הפרוטוקול 802.11 מספק אמצעי אבטחה שמחולקים לשלושה חלקים עיקריים:

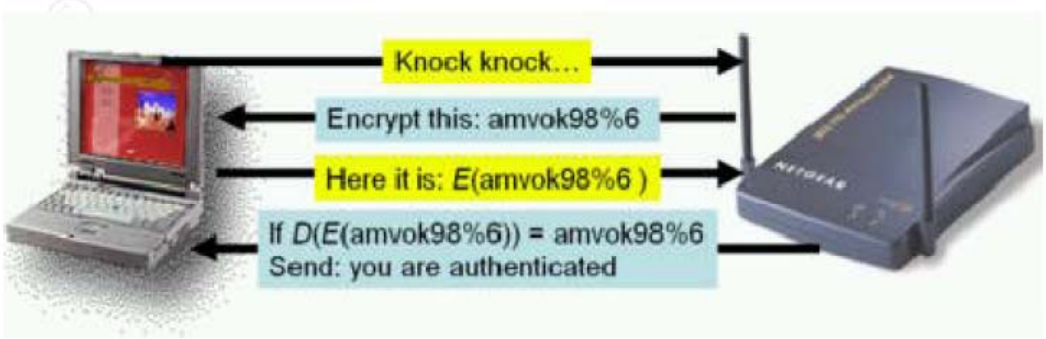
I. אימות (Authentication).
II. סינון (Filtering).
III. הצפנה (Encryption).

### אימות

כל קליינט חייב להזדהות וליצור שייכות עם AP (נקודת גישה) לפני שהוא משדר מידע. השייכות היא החיבור בין הקליינט ל-AP. פרוטוקול 802.11 תומך בשתי שיטות זיהוי:

I. **אימות במערכת פתוחה**, שזהו חלק מדרישות הפרוטוקול וברירת המחדל של רוב ה-AP. מערכת פתוחה מאפשרת לכל הקליינטים לתקשר עם ה-AP, כל עוד הם מחוברים לאותה רשת אלחוטית (SSID זהה). עובדה זו מקנה אפשרות התחברות לרשת זו לכל קליינט בטווח השידור של הרשת.
II. **אימות מפתח משותף**, שולט על הגישה לרשת האלחוטית באמצעות מפתח משותף ועל ידי כך מקשה את ההתחברות לרשת של קליינטים לא רצויים (קליינטים ללא המפתח). ההצפנה חייבת להיות מאופשרת במקרה של מפתח משותף, מכיוון שהמפתח משמש להצפנה משמש גם לאימות.

האיור הבא ממחיש בצורה גרפית את הנ"ל:



הסבר:

I. יצירת התקשרות.
II. ה-AP עונה לקליינט עם מחרוזת רנדומלית מסויימת כאתגר זיהוי.
III. הקליינט מצפין את המחרוזת בעזרת המפתח המשותף שלו ומחזיר את המחרוזת המוצפנת ל-AP.
IV. ה-AP מפענח את הקוד שקיבל בעזרת המפתח המשותף שלו ובודק האם המחרוזת שהתקבלה זהה לזו ששלח בשלב II. אם כן, הקליינט מאומת והוא שולח לו הודעה מתאימה.

## סינון

נקודות גישה אלחוטיות (AP) יכולות לסנן תחנות המנסות להתחבר לרשת על ידי שתי דרכים:

1. סינון כתובות MAC (MAC address filtering).
2. סינון כתובות IP (IP address filtering).

אך שיטות אלה אינן מספיקות כלל. פולש לרשת (או האקר) יכול יחסית בקלות לזייף את כתובת ה-MAC וגם ה-IP לאחת כזאת שכן יש לה גישה לרשת, על ידי האזנה לתעבורת הרשת וכך לקבל כתובת מה-AP ולהתחבר לרשת. את שיטה זו ניתן לבצע בקלות כאשר תעבורת הרשת אינה מוצפנת על ידי תוכנות שמופצות ברחבי האינטרנט. בהמשך נלמד שגם כאשר התעבורה מוצפנת יש דרכים להאזין לתעבורת הרשת ולהתחזות לכתובת מאומתת. אופציה אחת היא שההצפנה לא תופעל על כותרות המנות (Packet headers), אלא רק על גוף המנה (החלק של המידע במנה). כידוע בכותרת המנה נמצאות כתובות IP של המקור ושל היעד. מקרה כזה קיים עם הצפנת WEP לדוגמה.

## הצפנה

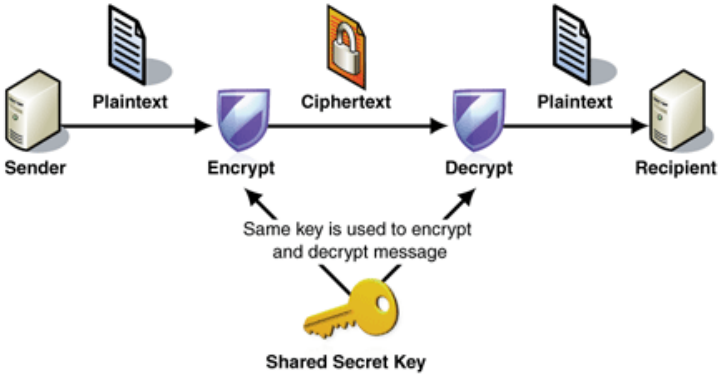
מושגים בקריפטולוגיה

1. **Plaintext** – המסר המקורי.
2. **Ciphertext** – המסר המוצפן.
3. **Cipher** – הצופן, שיטת הפיכת המסר המקורי למסר מוצפן.
4. **Key** – המפתח הסודי, המשומש בצופן על ידי המצפין/מפענח.
5. **Encrypt (encipher)** – המרת המסר המקורי למסר מוצפן.
6. **Decrypt (decipher)** – המרת (פענוח) המסר המוצפן למסר המקורי.
7. **קריפטוגרפיה** – מחקר שיטות הצפנה.
8. **קריפטו-אנליזה (שבירת צפנים)** – מחקר שיטות לגילוי הצופן או המפתח, מבלי לדעת את המפתח מראש.
9. **קריפטולוגיה** – שדה המשלב את הקריפטוגרפיה והקריפטו-אנליזה.

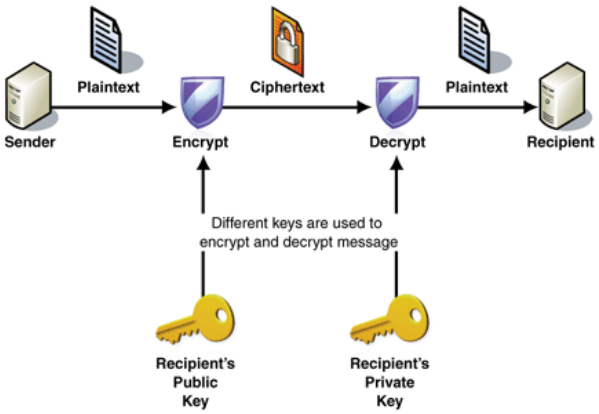
מה זו הצפנה?

הצפנה זהו תהליך שבו הופכים מידע (Plaintext) לקוד (Ciphertext) כדי להחביא את משמעותו ובכך למנוע מכל מי שאינו אמור לקבל מידע זה מלקבל אותו. משמע, שמשתמשים בעיקר בהצפנה כדי להבטיח פרטיות. חברות בדרך כלל מצפינות את המידע לפני שהן שולחות אותו, כדי לוודא שהמידע בטוח גם במהלך השידור. המידע המוצפן נשלח ברשת הציבורית ומפוענח על ידי הנמען הרצוי. ההצפנה מתבצעת על ידי העברת המידע (המיוצג בתור מספרים) דרך נוסחת הצפנה מסויימת (הנקראת מפתח). קיימות שתי סוגי הצפנות נפוצות:

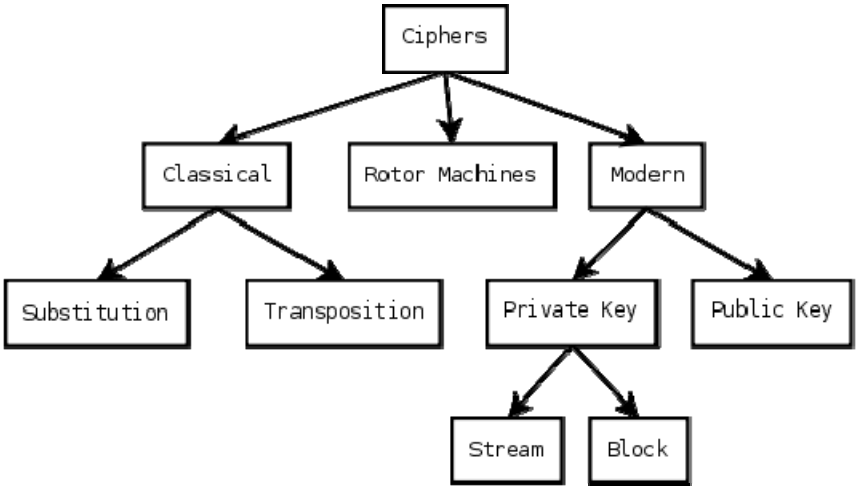
1. **הצפנה סימטרית** - סוג הצפנה שבה אותו מפתח משומש כדי להצפין ולפענח את המידע. מנגנון ההצפנה WEP הוא סימטרי. האיור הבא מתאר הצפנה סימטרית:




2. **הצפנה אסימטרית (הצפנה פומבית)** - סוג הצפנה שבה משתמשים במפתח אחד להצפנת המידע ובמפתח אחר לפענוח ההצפנה. האיור הבא מתאר הצפנה אסימטרית:



האיור הבא מתאר את אבולוציית ההצפנה:




לרשת האלחוטית WLAN קיימות מספר הצפנות נפוצות:

1. WEP
2. WPA
3. AES/CCM
4. Upper Layer Encryption

חלק זה של אבטחת המידע ברשת האלחוטית WLAN (הצפנה), הוא החלק שבו ארחיב ואפרט בהמשך. ההתמקדות תהיה במנגנון ההצפנה WEP.

## מנגנון הצפנה WEP

WEP (Wired Equivalent Privacy), זהו מנגנון הצפנה שתוכנן לספק אבטחה אלחוטית למשתמשי הרשת האלחוטית WLAN (802.11).

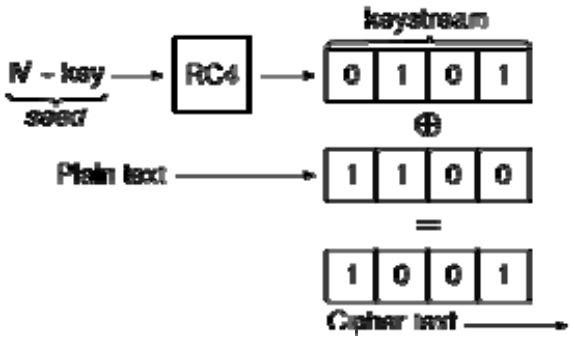
WEP זהו מנגנון הצפנת זרם סימטרית (Symmetric Stream Cipher) אשר לוקח את גוף מסגרת מידע (Data frame body) ומעביר אותו דרך אלגוריתם הצפנה. גוף מסגרת המידע אז מוחלף בגוף מסגרת המידע המוצפן ומשודר לאוויר. התחנה הקולטת משתמשת באותו אלגוריתם על גבי המידע המוצפן כדי לפענח אותו לצורתו המקורית. חשוב לציין שמנגנון ה- WEP, מצפין אך ורק את גוף המסגרת (החלק המכיל מידע) ולא את כותרת המסגרת (Header) ובכך משאיר את כתובת המען והנמען חשופים לכל.

בצורתו המקורית, WEP משתמש במפתחות הצפנה באורכים של 40 bit או 104 bit. בתחילת שנת 2001 מספר חולשות קריטיות התגלו על ידי חוקרים, מה שהוביל לכך שכיום תעבורת WEP ניתנת לפריצה באמצעות תוכנה זמינה מתאימה תוך מספר דקות. תוך מספר חודשים מתגלית זו, הקימו IEEE צוות מיוחד (802.11i) כדי לפתור חולשות אלו.

בשנת 2003 הכריזו צוות 802.11i על החלפתו של ה-WEP במנגנון ההצפנה המשופר Wi-Fi Protected Access (WPA).

### אופן פעולת מנגנון WEP ואלגוריתם ההצפנה

מנגנון ה- WEP משתמש באלגוריתם ההצפנה RC4, אשר פותח על ידי חברת האבטחת מידע RSA. מבנה המנגנון:



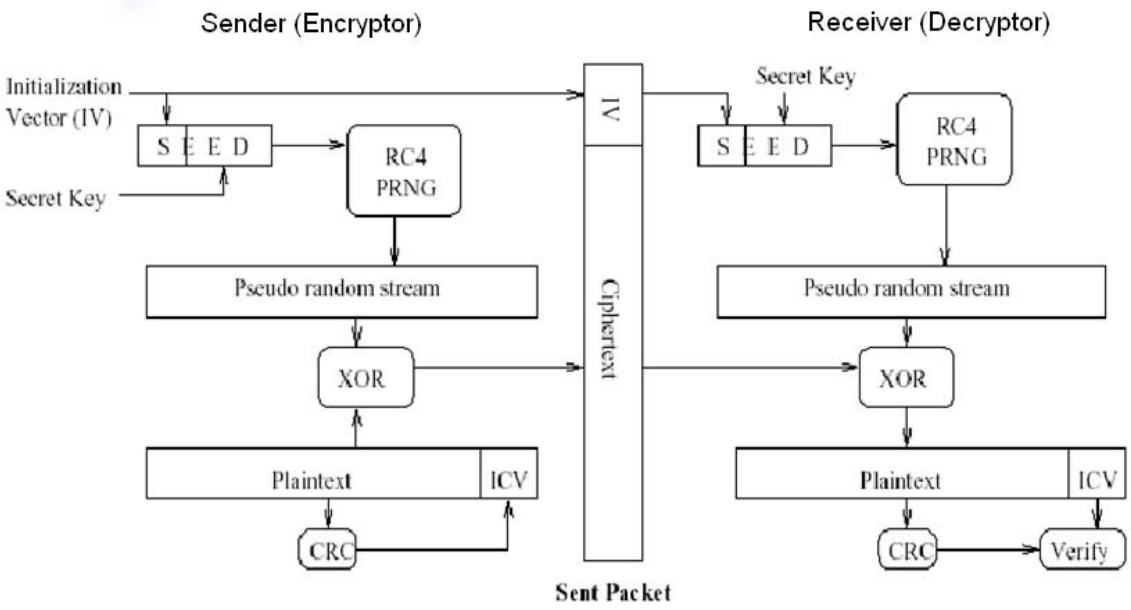

- WEP 64 ביט הסטנדרטי (WEP-64 bit) משתמש במפתח של 40 ביט (לכן ידוע גם בתור WEP-40), אשר משורשר עם ווקטור אתחול (IV) של 24 ביט.
- WEP 128 ביט זוהי הגרסה המורחבת שבה משתמשים במפתח של 104 ביט אשר משורשר ל-IV בגודל 24 ביט (IV + key = 104 + 24 = 128 bit).
- WEP 128 בדרך כלל מיוצג על ידי מחרוזת של 26 תווים הקסדצימלים (בסיס 16: 0-9 ,A-F). כל תו מייצג 4 ביטים מהמפתח. 26 תווים, כאשר כל אחד מהם בגודל 4 ביטים יוצרים ביחד את המפתח בגודל של 104 ביטים.
- WEP 256 מיושם לפעמים על ידי יצרנים (למשל של נתבים). גם בהרחבה זו, גודל ה-IV הוא 24 ביטים, מה שמשאיר את גודל המפתח להיות בגודל 232 ביטים. 232 תווים אלו מיוצרים על ידי 58 תווים הקסדצימלים (58 × 4 = 232 bits).

ווקטור האתחול (IV) משורשר עם המפתח הסודי ומועבר ביט אחר ביט (stream) דרך האלגוריתם RC4 ובכך יוצר את ה-keystream. על ה-keystream והמידע הגלוי (plain text) מבצעים פעולת XOR ובכך נוצר הקוד (המידע המוצפן או cipher text). לפני ההצפנה checksum (CRC32) מופעל על המידע, נוסף אליו ומוצפן ביחד איתו.

פיענוח של המידע המוצפן (decryption) נעשה באופן דומה: על הקוד והמפתח הסודי מבצעים פעולת XOR ובכך מקבלים את המידע. לבסוף מבצעים בדיקה של ה-checksum כדי לראות האם הוא תואם לערך שבתקבל לפני ההצפנה (בדיקה זו מבוצעת כדי לגלות אם נוצרו שיבושים במידע במהלך ההצפנה).

ה-IV (ווקטור האתחול) ששורשר עם המפתח הסודי משורשר כעת למידע המוצפן ומשודר לאוויר.

האיור הבא מציג את התהליך המלא:



**פעולת XOR:**

סימון: ⊕

XOR זהו אופרטור לוגי שפועל על שני אופרנדים ומתואר על ידי הטבלת אמת הבאה:

| $x$ | $y$ | $x$ XOR $y$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

דוגמאות לשימושים ב- XOR

- 01011010101 Plaintext 1
- XOR 10111110000 Keystream
- 11100100101 ciphertext 1

- 11100100101 ciphertext 1
- XOR 10111110000 Keystream
- 01011010101 Plaintext 1

- ניתן לראות שזהו אופרטור סימטרי, מה שמאפשר גם להצפנה להיות סימטרית, שזה אומר הצפנה ופענוח באמצעות אותו המפתח.

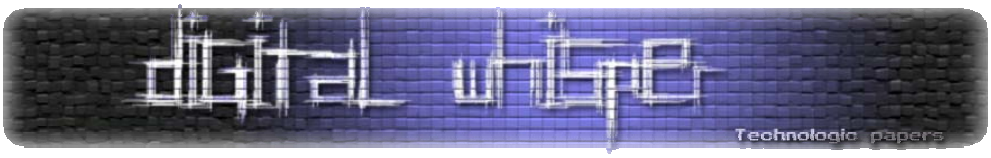
**ה- Keystream:**

כל IV שונה מייצר Keystream שונה, המפתח הסודי נשאר קבוע ונקבע על ידי מקים הרשת (עד שהוא בוחר לשנות אותו אם בכלל). לכן מפתח סודי יחיד ייצר $2^{24}$ Keystream-ים שונים (24 ביט זהו הגודל המקסימלי של ה-IV).

בסופו של דבר ההצפנה והפענוח של WEP זוהי פעולת XOR עם אחד מה-Keystream-ים. כדי לבצע פעולת פענוח, ה-IV נלקח מהמנה (packet) שנקלטה במקלט (ראה איור לעיל) ויוצר Keystream שהוא זהה לזה שנוצר בתהליך ההצפנה (במידה וגם המפתח הסודי זהה כמובן). Keystream זה והקוד עוברים פעולת XOR וכך מקבלים את המידע.

פעולת ההצפנה היא פחות נוקשית מהמובן שה-Keystream לא חייב להיות ספציפי והוא וריאציה כלשהי שהיא אחת מ- $2^{24}$ האפשרויות. למרות שתחנת שידור לא אמורה לפעול כך, זה אפשרי לגלות Keystream יחיד ואז לשלוח מנות שונות עם אותו Keystream ו-IV. ובכך, על ידי גילוי Keystream אחד, תוקף יכול לשדר כל מידע מוצפן או לפענח מנה נקלטת אשר משתמשים באותו Keystream.

בעזרת ה-XOR מתקיימת התכונה: $Cipher \oplus Plaintext = Keystream$. לכן דרך אחת לגילוי ה-Keystream היא ידיעה של הקוד והמידע וביצוע XOR ביניהם. את הקוד ניתן לגלות פשוט על ידי האזנה למנה משודרת. אם ה-Keystream מחולץ מהקוד, ניתן לשדר מנות עם אותו ה-IV שקיבלנו מההאזנה. Keystream זה יכול לשמש כדי לפענח כל מנה נקלטת המשתמשת באותו ה-IV. אך הבעיה העיקרית בחישוב ה-Keystream בצורה הזו היא שחייבים לדעת מראש את המידע לצורך השוואה עם התוצאה שקיבלנו.




## אלגוריתם RC4

### הקדמה

RC4 אשר פותח על ידי רון ריווסט מחברת Security RSA בשנת 1987, הוא הצופן זרם הנפוץ ביותר כיום ומיושם בפרוטוקולים פופולריים כגון SSL (פרוטוקול לאבטחת תעבורת רשת) ו-HTTPS. למרות שיישומו בתור תוכנה הוא מאוד פשוט ומהיר ועובדת היותו מאוד נפוץ, ל-RC4 יש חולשות שמטילות בספק את מקומו במערכות חדשות.

חולשות אלגוריתם זה הם: החלק ההתחלתי של הפלט (ה-Keystream), שימוש במפתחות לא רנדומליים או קשורים אחד לשני, או שימוש באותו מפתח יותר מפעם אחת. דרכים לא בטוחות לשימוש ב- RC4, עלולות להוביל לפגמים באבטחת המידע. דוגמה לכך הוא מנגנון ההצפנה WEP.

### צופן זרם (Stream Cipher)

יש מגוון רב של סוגי צפנים, אך החלוקה העיקרית ביניהם היא לצפנים קלאסיים (היסטוריים) ולצפנים מודרניים.
צופן זרם היא אחת השיטות המודרניות להצפנת מידע ואחת הפשוטות מביניהן, כאשר בשיטה זו מצפינים את המידע (זרם ביטים) ביט אחר ביט.

### מבנה האלגוריתם

אלגוריתם RC4 זהו צופן זרם סימטרי. אותו אלגוריתם משמש גם להצפנה ולפענוח, כאשר זרם המידע והמפתח המיוצר עוברים פעולת XOR.

RC4 מייצר זרם ביטים רנדומלי (יותר נכון פסאודו-רנדומלי), שזהו בעצם ה-Keystream, אשר לצורך הצפנה, משולב יחד עם המידע (Plaintext) בעזרת פעולת XOR. פעולת הפענוח נעשית באופן דומה (מאחר ופעולת XOR היא סימטרית).

לייצור ה- Keystream, הצופן משתמש במצב פנימי סודי אשר מורכב משני חלקים:

1. פרמוטציה של 256 בתים (Bytes) אפשריים (מסומן בתור S באיור הבא).
2. 2 משתני אינדקס בגודל 8 ביטים (מסומנים בתור "i" ו- "j" באיור הבא).

ה-RC4 מורכב משתי פונקציות פשוטות יחסית, KSA ו-PRGA, אשר ביחד יוצרות את ה-Keystream, שזהו זרם פסאודו-רנדומלי של ביטים.

```
PRGA(K)
Initialization:
    i = 0
    j = 0
Generation Loop:
    i = i + 1
    j = j + S[i]
    Swap(S[i], S[j])
    Output z = S[S[i] + S[j]]
```

```
KSA(K)
Initialization:
    For i = 0 ... N - 1
        S[i] = i
        j = 0
Scrambling:
    For i = 0 ... N - 1
        j = j + S[i] + K[i mod l]
        Swap(S[i], S[j])
```

**הפונקציה KSA**

KSA (Key Scheduling Algorithm), זוהי פונקציה שתפקידה לאתחל את ה-Keystream ולערבב אותו.

הסבר קוד הפונקציה:

התהליך מתחיל על ידי יצירת מערך S באורך (N) השווה באורכו לחיבור של ה-Plaintext וה- CRC (checksum). המערך S מאותחל על ידי קביעת ערכם של כל איבר במערך להיות שווה לערך האינדקס של אותו איבר (S[0] = 0, S[1] = 1, …., S[N] = N), שזוהי בעצם פרמוטציית זהות של S. בשלב הערבוב לכל i מאפס עד (N – 1), ה- KSA מחשב ערך ל- j על ידי הוספה (במודולו N) את הערך הקודם של j, את הערך באינדקס i של מערך S ואת הערך באינדקס i (במודולו l, שזהו האורך של k). כאשר k הוא מערך ה- IV (ווקטור האתחול) אשר בסוף התהליך גם משורשר למפתח. לבסוף הערכים של S[i] ו- S[j] מוחלפים. תהליך זה מתבצע על כל איבר במערך S. התוצר הסופי הוא מערך, S, אשר באורך של שילוב ה-Plaintext וה-CRC, ומעורבב לפי האינדקס של המפתח.

**הפונקציה PRGA**

PRGA (Pseudo-Random Generation Algorithm), זוהי פונקציה שתפקידה לקבל את הפלט של הפונקציה KSA שזהו מערך מעורבב וליצור את ה-Keystream, שזהו זרם ביטים פסאודו-רנדומלי (מדמה רנדומליות).

הסבר קוד הפונקציה:

המערך S שעבר תהליך ערבוב בפונקציה KSA, מגיע כעת לפונקציה זו ונכנס ללולאה שבה שוב עובר סידרה של N החלפות. אך הפעם, בניגוד לפעם הקודמת, בכל החלפה הפלט הוא הערך שמחושב. הפלט (z), שיוצר מערך באורך N בסיום הלולאה, זהו ה-Keystream הסופי שישמש כדי להצפין את המידע.

## תקיפות על מנגנון ההצפנה WEP

ל-WEP יש היסטוריה ארוכה של חולשות ו-"תיקונים". ההתקפות הראשונות לא נראו כל כך פרקטיות, לכן לחברות המיישמות הצפנה זו העדיפו שלא להשקיע בפתרונות אבטחה חדשים, אלא סיפקו תיקונים כדי להקטין עוד יותר את הסיכוי להתקפה הקשה לביצוע הזו. ההתקפות התפתחו במשך הזמן, והתקפות חדשות התגלו אשר מעמידות איומים חדשים ל-WEP. פעם נוספת תגובת התעשיה היתה ליצור תיקונים חדשים אשר יקטינו עוד יותר את הסיכוי להתקפה.

בסעיפים הבאים אני אציג את הבעיות העיקריות שנתגלו ב- WEP וכיצד החברות המיישמות הצפנה זו הגיבו.

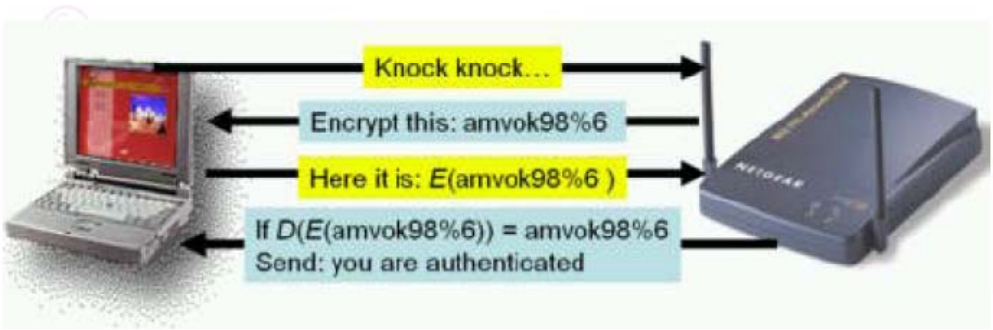
### התקפת Brute-Force

ההתקפה הנאיבית ביותר היא Brute-Force שבה מנסים את כל המפתחות האפשריים עד שמוצאים את המפתח המתאים. לפרוטוקול 802.11 הסטנדרטי יש מפתח באורך 40 ביט. התקפת Brute-Force על מפתח באורך זה באמצעות מחשב בודד מודרני תארך קרוב לחודש – מייגע אך אפשרי, במיוחד אם המשימה מחולקת (לתהליכים או Thread-ים שהם תתי תהליכים).

המענה של משווקי ה-WEP לתקיפה זו הוא הוספת תמיכה במפתח WEP באורך 104 ביט.

### שימוש חוזר ב- Keystream

ניתוחים שנעשו על WEP מצביעים על כך שרמת האבטחה של האלגוריתם אינה תלויה במפתח. לכן, נסיונות קודמים להגביר את רמת האבטחה של ה-WEP על ידי שימוש במפתחות יותר ארוכים לא הניבו פירות. אם Keystream נגלה, זה אפשרי לפענח מידע אשר משתמש באותו Keystream וגם לשדרו. מנגנונים לגילוי Keystream פותחו לאחר מכן. המנגנון הפרקטי ביותר מסתמך על שיטת 'אימות מפתח משותף' (Shared Key Authentication) להיות מאופשרת. לשיטה זו יש מנגנון למניעת כניסות לא מאומתות לרשת. איור זה מדגים את מנגנון אימות מפתח משותף:



ה-AP (במקרה זה, הראוטר) שולח מחרוזת טקסט גלויה בתור אתגר לתחנה שמנסה להתחבר לרשת. התחנה מאומתת על ידי מענה לאתגר שזה הצפנה של מחרוזת הטקסט שקיבלה. על ידי האזנה לאימות מסוג זה, לתוקף יש גם את ה-Cipher text (המסר המוצפן) שבמקרה זה, הוא E(*amvok98%6*) ואת המחרוזת הגלויה שבמקרה זה היא *amvok98%6*. על ידי ביצוע XOR ביניהם נוכל לגלות את ה-Keystream.
תקן 802.11 מתריע משתמשים משימוש חוזר ב-IV בתהליך האימות, מאחר ששימוש עתידי בהצפנה עם אותו IV עלול להיות מפוענח.

התגובה להתקפה זו היא הסתרת שם הרשת (SSID) וסינון כתובות MAC. אך כמובן גם נגד תגובות יש התקפות שעוקפות אותן בקלות יחסית כגון האזנה לבקשת שייכות לרשת או זיוף כתובת MAC.

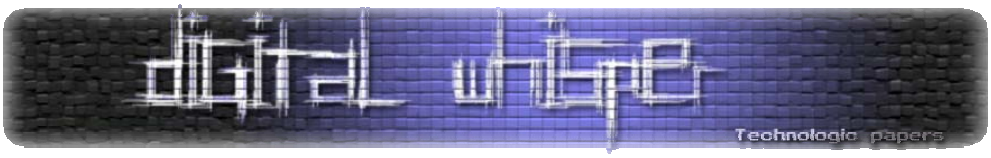
למרות התקפות אלה, לא נעשתה פעולה לתקן את הבעיה של שימוש חוזר ב-IV וזאת מהטיעון שלרשת יש - $2^{24}$ Keystream-ים שונים, מה שעושה את כל תהליך ההתקפה למסובך מדי.

### תקיפת IV-ים "חלשים"

מחקר נוסף שנעשה על WEP גילה כי ניתן לחשב (מתמטית) את המפתח. התקפה דרשה איסוף של בערך מיליון מנות שחלקן משתמשות ב- IV-ים "חלשים". למעשה IV "חלש" בודד נותן סבירות של 5% לגילוי בית (byte) אחד מהמפתח הנכון. על ידי איסוף מספר רב של סטטיסטיקות (IV-ים), המפתח שנותן את ההסתברות הכי גבוהה מחושב.

התקפה זו נתפסה כמאוד מסוכנת. אולי משום שזו הפעם הראשונה שבה היה ניתן ליצור כלים אוטומטים לגילוי המפתח. כעת, גם האקרים ללא ניסיון יוכלו לחדור לרשת שמשתמשת ב-WEP. התגובה להתקפה זו היתה בניית חומרה (פילטרים) אשר תסנן את ה- IV- ים ה"חלשים". על ידי יישום חומרה זו, מפצי ה-WEP רק החמירו את חולשת השימוש החוזר ב- Keystream, כי כעת נותרו פחות מ- $2^{24}$ Keystream-ים. התקפה זו לכן הומעטה בחומרתה בטענה שרק בנסיבות מסויימות ורק אחרי שהושג כמות גדולה של מנות, ניתן יהיה לבצע את ההתקפה. איסוף כמות זה של מנות יכול לפעמים לארוך ימים.

הסתבר שהיו יותר IV-ים "חלשים" ממה שפורסם. מפיצים נאלצו להתשמש בפילטרים נוספים, למרות שהבעיה כבר הפכה להיות ברורה לעין. יתרה מכך, IV-ים חלשים שנתנו הסתברות של 13% התגלו, אך פרטיהם מעולם לא פורסמו. כעת נדרש איסוף של כ-500,000 מנות כדי לחשב את המפתח. איסוף של כמות זו עדיין לוקח זמן ארוך יחסית, עובדה שמפיצי ה-WEP הסתמכו עליה.




### התקפות מודרניות

קיימים שתי בעיות עקריות עם ההתקפות בעבר. האחת היא איך לגלות Keystream באמינות והשניה היא איך לזרז את התקפת ה-IV-ים החלשים. שתי בעיות אלו נפתרו. כעת אפשרי לגלות בית (Byte) אחד של Keystream לאחר שליחה של לכל היותר 256 מנות. כדי לזרז את התקפת ה-IV-ים החלשים, זה אפשרי לא רק להאזין לתעבורת הרשת אלא גם לשלוח מנות WEP ל-AP ובכך ליצור תעבורת מידע גדולה יותר. בנקודה זו, ספקי WEP הבינו שהצפנה זו מתה. תוקף מיומן יכול לחדור למערכת בתוך מספר שעות בודדות (הערכה מוקצנת) על ידי שימוש בתכונות אלה.

## סיכום

כיום, כשהשימוש ברשתות אלחוטיות (WIFI) הפך להיות כל כך נפוץ, יש צורך בנקיטת אמצעי הגנה ואבטחה על הרשת האלחוטית. מעצם טיבעה, תקשורת אלחוטית מתאפיינת בכך שהמידע המשודר מהמחשב ואליו חשוף להאזנה. באמצעות כלים פשוטים, ניתן לצותת לתשדורת האלחוטית, מה שעלול להביא לחשיפה של מידע רגיש.

נוסף על כך, רשת אלחוטית שאינה מאובטחת כיאות, חושפת את הנתב והרשת הביתית עצמה להאקרים וגורמים זרים המעוניינים לזרוע בה הרס ולגזול רוחב פס מבלי שנדע. על מנת לפרוץ לנתב האלחוטי ולרשת הביתית, כל מה שנדרש הוא מחשב נייד, תוכנה וקצת סבלנות ולכן יש צורך חיוני ליישם מנגנוני אבטחה שיגנו על הרשת האלחוטית.

חשוב להדגיש שאין אבטחה מושלמת לשום רשת (חוטית או אלחוטית) ופורץ עיקש עם מטרה ברורה ואמצעים להשגתה, יוכל להתגבר על כל מנגנון אבטחה שניישם. עם זאת ובהנחה שעל המחשב שלכם לא שמורים סודות כמוסים ביותר, יישום אפשרויות האבטחה הנסקרות בסמינר זה יגביר עד מאוד את בטחון הרשת האלחוטית שלכם.

### סקירה קצרה של האפשרויות השונות לאבטחת הרשת

הטבלה להלן סוקרת את מנגנוני האבטחה השונים הקיימים בנתבים אלחוטיים בייתים ומדרגת את חשיבות יישומם ואת רמת ההגנה שהם נותנים. ברמה הבסיסית ההמלצה היא לכל אחד לאבטח את הנתב האלחוטי שלו בשלושה מישורים המודגשים בצהוב - שינוי סיסמת הכניסה לנתב, שינוי ה-SSID והגדרת הצפנה ברמת WPA לפחות.

| מנגנון | תאור קצר | חשיבות יישום | חוזק ההגנה |
|---|---|---|---|
| שינוי סיסמת כניסה לנתב | סיסמת הכניסה לנתב נותנת למשתמש גישה לתפריטי הניהול שלו. | גבוהה | בינונית |
| שינוי ה-SSID של הנתב | ה-SSID הוא השם של הרשת האלחוטית שהנתב משדר לסביבה. | בינונית | נמוכה |
| חסימת שידור ה-SID של הנתב | ה-SSID הוא השם של הרשת האלחוטית שהנתב משדר לסביבה. | נמוכה | נמוכה |
| ביטול מנגנון ה-DHCP | מנגנון ה-DHCP מחלק באופן אוטומטי כתובות IP למחשבים המתחברים לנתב. | נמוכה | נמוכה |
| סינון כתובות MAC בעלות גישה לנתב | ה-MAC הוא מזהה חד חד ערכי של כרטיס הרשת וניתן להגדיר בנתב רשימת MAC המאושרים לגישה. | נמוכה | נמוכה |
| הצפנת באמצעות סיסמא במנגנון WEP, WPA או WPA2. | הצפנה השידור האלחוטי באמצעות סיסמא המוסכמת בין המחשב לנתב. | גבוהה | WEP – נמוכה<br>WPA – גבוהה *<br>WPA2 – גבוהה |
| ביטול האפשרות לניהול מרחוק | מרבית הנתבים מאפשרים ניהול מרחוק על גבי רשת האינטרנט. | בינונית | גבוהה |
| הקטנת עוצמת השידור האלחוטי | הקטנת עצמת השידור האלחוטי מצמצמת את הרדיוס בו ניתן לקלוט את האות האלחוטי. | בינונית | בינונית |
| ביטול מנגנון ה-UPNP של הנתב | מנגנון ה-UPNP מאפשר לנהל את מרכיבי הרשת בצורה קלה ופשוטה יותר. | בינונית | בינונית |

* בתנאי שמפתח ההצפנה (הסיסמא) מורכב משילוב של אותיות, ספרות ותווים מיוחדים.

כפי שניתן לראות בטבלה לעיל, ההמלצה היא לא להשתמש במנגנון ההצפנה WEP, משום שכיום אין צורך להיות האקר מנוסה כדי לפרוץ את ההצפנה הזאת. קיימות ברחבי האינטרנט מספר לא קטן של תוכנות חינמיות ופשוטות לפריצת ההצפנה. הנפוצות מבניהן:

1. WEP Crack Utility
2. AirCrack
3. WepAttack
4. WEPWedgie

כל הצפנה חדשה שיוצאת כיום נמצאת במירוץ נגד הזמן, בסופו של דבר יגיע היום בו יצליחו לפרוץ אותה והיא כבר לא תהיה מספיק בטוחה. לכן חשוב להתעדכן בטכנולוגיות אבטחת מידע ומנגנוני הצפנה חדשים או נוספים מדי פעם.