פרוטוקול WEP וצופן RC4

One time pad

- שיטת הצפנה מושלמת שייחודה בכך שקיימת הוכחה מתמטית לכך שאם המפתח המשמש להצפנה נבחר באקראי והשימוש בו הוא חד-פעמי, ההצפנה בלתי ניתנת לשבירה אפילו ליריב בעל עוצמת חישוב בלתי מוגבלת.

- מפתח בגודל ההודעה לפחות.
- מפתח רנדומלי (מתפלג בצורה אחידה בהינתן כל המפתחות האפשריים ולא תלוי בהודעה).
- שימוש חד פעמי.
- שני צדדים בלבד מחזיקים במפתח הסודי.

One time pad

הצפנה: $E_k(m) = m \oplus k = c$

פענוח: $D_k(k, c) = k \oplus c = k \oplus m \oplus k = m$

```
  1010   (A - הודעה)
⊕ 1100   (B - מפתח)
---------
  0110   (C - טקסט מוצפן)
```

```
  0110   (C - טקסט מוצפן)
⊕ 1100   (B - מפתח)
---------
  1010   (A - הזרנו להודעה המקורית!)
```

צופן זרם

- מצפין כל סיבית של ההודעה באמצעות XOR עם זרם מפתח.
- ב- OTP זרם המפתח הוא אקראי לחלוטין וחד-פעמי.
  בצופן זרם, זרם המפתח מיוצר מתוך מפתח קצר יותר ע"י פונקציה פסאודו-אקראית.

- מחולל אקראי – בלתי ניתן לשחזור, מצריך מקור חיצוני (חום, זרימת מים, קרינה)
- מחולל פסאודו אקראי - נראה אקראי, אבל מיוצר באמצעות אלגוריתם מתמטי דטרמיניסטי. אם יודעים את מצב המחולל (Seed) ניתן לשחזר את הזרם כולו.

צופן זרם

- עבור כל הצפנה נשתמש במפתח אחר!
- כאשר משתמשים **באותו מפתח פעמיים** בהצפנה עם XOR אפשר **לחלץ מידע** מההודעות המוצפנות.
- אם לתוקף יש את c1 , c1 שהוצפנו ע"י אותו מפתח.

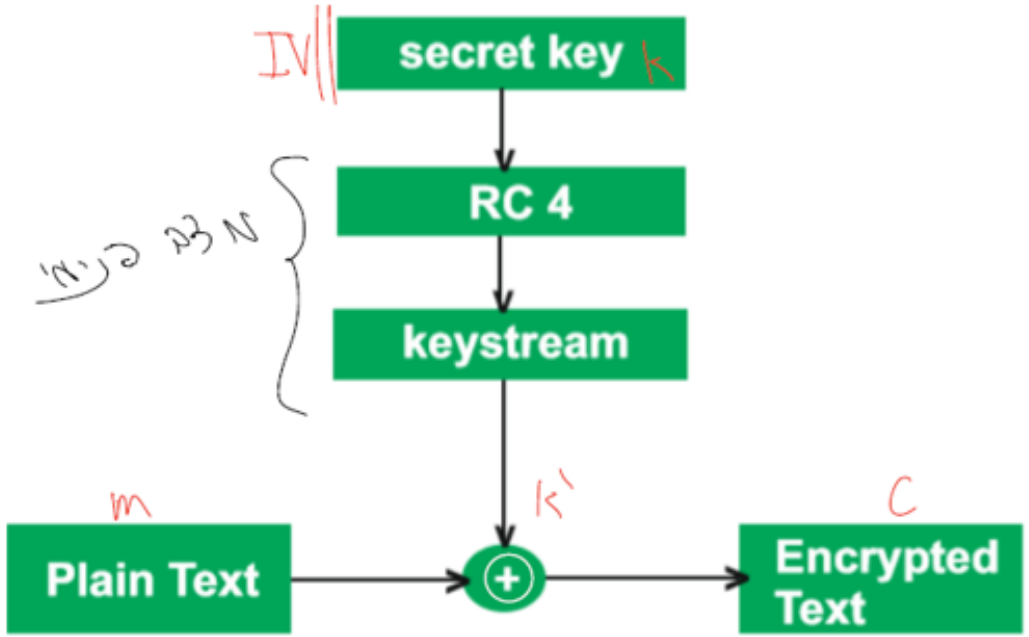
אל: הדקרו כך שמתוכו יוצא ש- $c_1 = m_1 \oplus k$! $c_2 = m_2 \oplus k$ הוא יכל לעשות?

$c_1 \oplus c_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2$

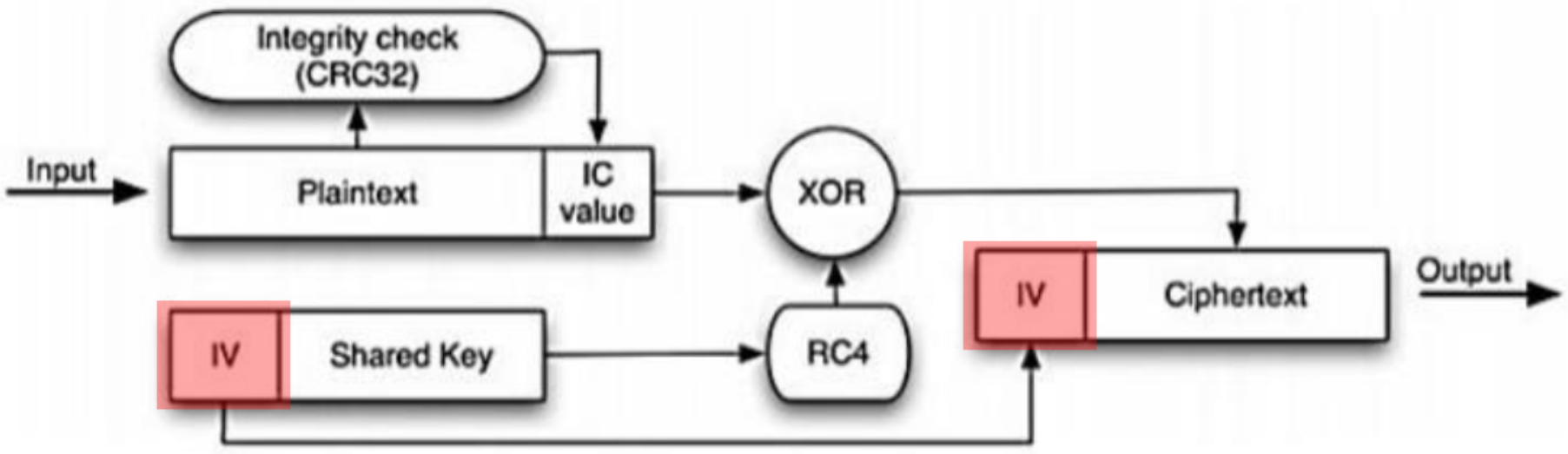
- מתקבל XOR של ההודעות המקוריות. לכן כל הודעה חייבת להיות מוצפנת ע"י זרם מפתח שונה.

צופן RC4

- צופן זרם, כלומר מחולל בתים מקריים
  - ההצפנה מתבצעת באמצעות ביצוע XOR של בית מקרי עם בית ההודעה
  - כך גם הפיענוח
- באתחול מקבל מפתח סודי ויוצר מצב פנימי
- בכל פעם שמבקש לחולל בית מקרי
  - נעזר במצב הפנימי
  - ומשנה את המצב הפנימי



וקטור אתחול



- כמות מסוימת של בתים מקריים ולא סודיים
- הם משורשרים למפתח הסודי ומתקבל מפתח מורחב
- המפתח המורחב משמש כמפתח של RC4
- וקטור האתחול מוגרל מחדש בהצפנה של כל הודעה
- הוא משורשר לפני תחילת ההודעה המוצפנת כדי לאפשר פענוח
- מבטיח שהודעות שונות תוצפנה באמצעות מפתחות שונים

למה צריך וקטור אתחול

- יש לנו מפתח סודי K. ממנו RC4 מחולל רצף בתים מקריים R
- הוצפנו שתי הודעות A ו-B והתקבלו שתי הודעות מוצפנות X ו-Y
- התוקף
  - לא יודע A, B, K, R
  - כן יודע X, Y
- מה הוא יכול לעשות?
  - $Z = X \oplus Y = (A \oplus R) \oplus (B \oplus R) = A \oplus B \oplus (R \oplus R) = A \oplus B$
- התוקף יכול לעבור על כל המילים במילון ולעשות מילה $Z \oplus$
  - אם מה שמתקבל זה גם מילה, אז התוקף מצא את ההתחלה של A ו-B
  - הוא ממשיך באותו האופן

- IV לבדו לא נותן אבטחה.
הוא רק משתנה לכל הודעה כדי להבטיח שכל הודעה תוצפן עם זרם מפתח ייחודי.

- אם לתוקף יש IV אבל אין לו את K- הוא לא יכול לשחזר את זרם המפתח.
אם לתוקף יש גם את IV וגם את K - הוא יכול לשחזר בדיוק את אותו זרם מפתח ולקבל את ההודעה המקורית.

פרוטוקול WEP

- משמש להצפנת תעבורה אלחוטית
- משתמש בצופן RC4
- לא בטוח לשימוש
  - התגלו חולשות בRC4
  - פרוטוקול WEP משתמש בRC4
  - כל חבילה שנושאת מידע מתחילה בכותרת קבועה
  - זה והחולשות ביחד מאפשרות לגלות את המפתח (פרטים אצל המרצה)

פרטים טכניים

- מפתח
  - אורך המפתח הסודי של WEP – 5 בתים. נסמן ABCDE
  - אורך וקטור האתחול – 3 בתים. נסמן XYZ
  - אורך המפתח המורחב – 8 בתים. בסדר הזה: XYZABCDE
- סוגי חבילות
  - יש כמה סוגי חבילות
  - רק חבילות נושאות מידע מוצפנות
  - בכל חבילה יש וקטור אתחול שונה, אבל המפתח הסודי נשאר זהה
  - בכל חבילה נושאת מידע, ארבעת הבתים הראשונים זהים

קצת על Wireshark

Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Tp-LinkT_1f:73:b0	Broadcast	802.11	149	Beacon fra
2	1.413691	Tp-LinkT_1f:73:b0	Shenzhen_72:87:5c	802.11	258	Probe Resp
3	1.416251	Tp-LinkT_1f:73:b0	Shenzhen_72:87:5c	802.11	258	Probe Resp
4	1.418303	Tp-LinkT_1f:73:b0	Shenzhen_72:87:5c	802.11	258	Probe Resp
5	1.420864	Tp-LinkT_1f:73:b0	Shenzhen_72:87:5c	802.11	258	Probe Resp
6	2.551417	HuaweiTe_ea:b5:1e	Broadcast	802.11	108	Data, SN=1
7	2.635347	ChinaDra_2b:54:d7 (…	Avm_0b:2e:35 (34:81…	802.11	16	Request-to
8	4.122323	AskeyCom_bf:0b:0b (…	Azurewav_b2:e1:b7 (…	802.11	16	Request-to
9	4.122324		AskeyCom_bf:0b:0b (…	802.11	10	Clear-to-s
10	4.140286	Tp-LinkT_1f:73:b0	IPv4mcast_7f:ff:fa	802.11	332	Data, SN=1
11	4.242173	Tp-LinkT_1f:73:b0	IPv4mcast_7f:ff:fa	802.11	341	Data, SN=1
12	4.342526	Tp-LinkT_1f:73:b0	IPv4mcast_7f:ff:fa	802.11	404	Data, SN=1

```
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Tp-LinkT_1f:73:b0 (00:23:cd:1f:73:b0)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: HuaweiTe_ea:b5:1e (8c:eb:c6:ea:b5:1e)
BSS Id: Tp-LinkT_1f:73:b0 (00:23:cd:1f:73:b0)
STA address: Broadcast (ff:ff:ff:ff:ff:ff)
.... .... .... 0000 = Fragment number: 0
0100 0100 0110 .... = Sequence number: 1094
▾ WEP parameters
    Initialization Vector: 0xcea26f
    Key Index: 0
    WEP ICV: 0xcd24ff64 (not verified)
```

```
0000  08 42 00 00 ff ff ff ff  ff ff 00 23 cd 1f 73 b0   ·B····· ···#··s·
0010  8c eb c6 ea b5 1e 60 44  ce a2 6f 00 fc 98 7d dd   ======`D ··o···}·
0020  ca 59 74 19 2a a5 79 b6  20 bc 61 89 75 e3 31 ec   ·Yt·*·y· ·a·u·1·
0030  27 e8 2d 6d 28 3e 87 1b  25 41 0a a5 f5 21 cb 11   '·-m(>·· %A···!··
0040  d2 57 ff 09 69 48 6c 41  69 37 87 98 30 f9 a2 34   ·W··iHlA i7··0··4
0050  38 fc 5c 7e f3 fb db 03  6b 68 25 3a ca c0 03 07   8·\~···· kh%:····
0060  ed af 08 8c 23 25 28 91  cd 24 ff 64               ····#%(· ·$·d
```

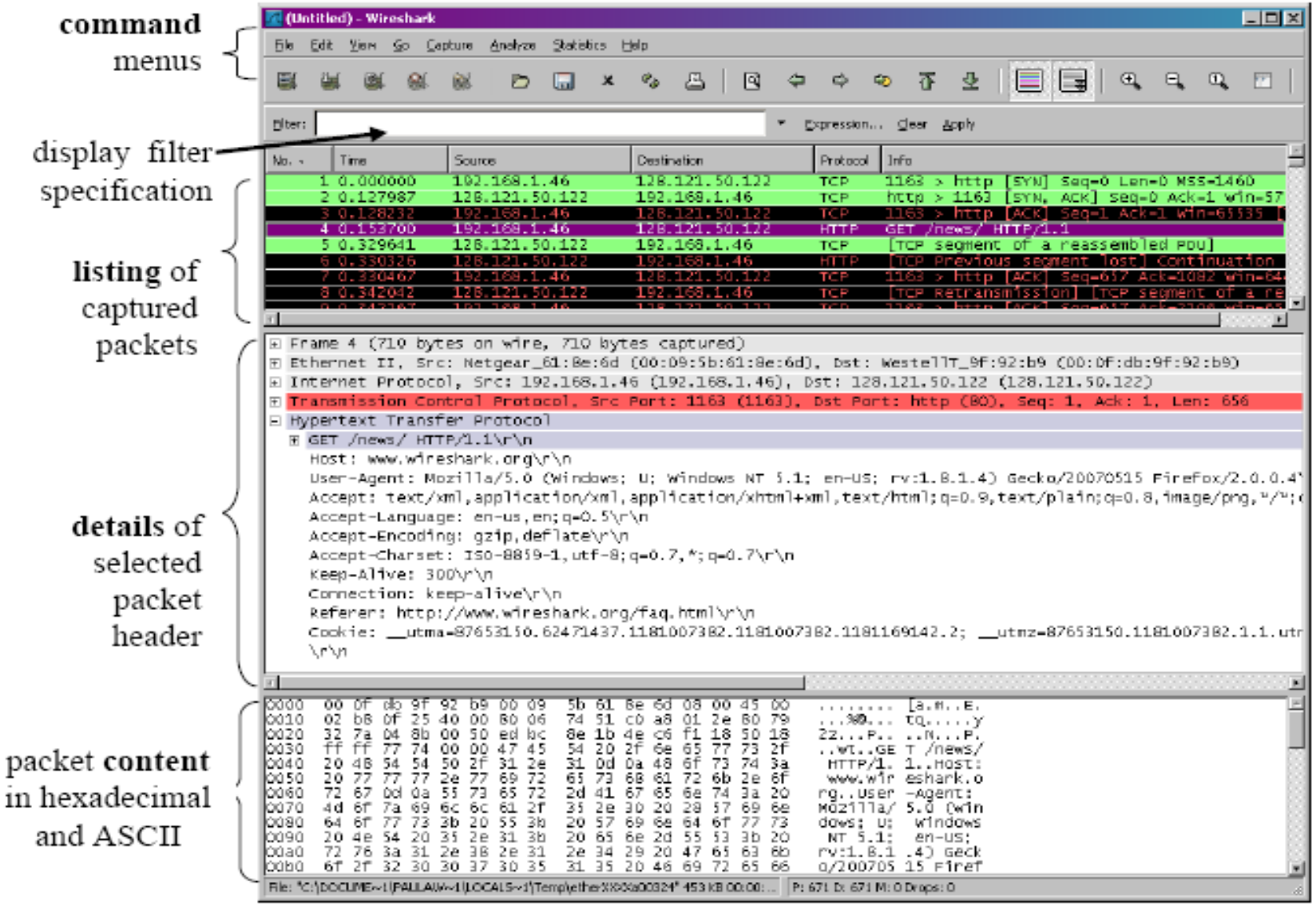
בונוסא לכך שניתן לראות
את ה- IV של כל
תבילה מוצפנת

Wirshark install

- **Windows**

Download from here
https://www.wireshark.org/download.html

Wireshark Interface



http vs https

- http vs https
- Filter query -> http
- From browser -> http://httpforever.com/
  Or https://example.com/
- from wireshark