יסודות הקריפטוגרפיה שיעור 8#

הרצאת אורח: תקשורת בטוחה מל ערוצים לא אמינים:

דרישות:

- מידע יגיע
- סודיות: המידע יגיע רק לנמען המיועד:
  - זיהוי בן זוג ושיחה
  - לכמה זמן הסודיות?
- יעילות
- אימות: שולח, תוכן
- אנונימיות צדדי השיחה
- אי הכחשה: ראיות לקיום שיחה
- הגנה נגד אנליזת תנועה
- סטגנוגרפיה
- *Provability*: להיות מסוגלים לוודא לעצמינו בשלב התכנון שהפרוטוקול המוצע מקיים את התכונות הנדרשות ואמין.

ניתוח פרוטוקול:

- מידול של תכונות הפרימיטיביים הבסיסיים
- מידול של תכונות הבטיחות הדרושות
- הוכחה שפרוטוקול המידע מקיים את כתונות בהסתמך על:
  - נכונות הפרימיטיביים
  - הנחות נוספות על היריב

פתרון ראשון לתקשורת בטוחה:

לכל זוג צדדים יהיה מפתח משותף. למשל זוג A, B עם המפתח k. הצד A שולח את ההודעה שלו m מוצפנת: $E_k(m)$. ישנן דרכים שונות להצפנה ואותנטיקציה, למשל:

- $E_{k_e}\left(MAC_{k_A}(m), m\right)$ - לא בטוח.
- $c = E_{k_a}(m), MAC_{k_b}(c)$
- $E_{k_a}(m), t = MAC_{k_b}(m)$

<u>פתרון ראשון: *Mac-then-encrypt*</u>:

$E_k(m) = [m_1 \oplus k_1] \circ \ldots \circ [m_n \oplus k_n] = c_1 \circ \ldots \circ c_n$

לכל c_i נוסיף ביט נוסף, כלומר נכפיל את מספר הביטים שלו. אם זה0, יהפוך ל-00; אם זה 1 יהפוך לאחד מ-3 האפשרויות האחרות.

$m \to t = MAC_{k_a}(m), E_{k_b}(m, t) = c$

ה-*ciphertext* נראה כעת כאוסף זוגות ביטים.

אלגוריתם ההצפנה, שוב:

- תחילה מבצעים הכפלה של הביטים שלm כך ש-0 הופך ל-00 ו-1 הופך למשהו מ-3 האפשרויות האחרות.
- לאחר מכן על ההודעה המנופחת מבצעים*one-time-pad*.
- הפענוח יהיה תחילה *one-time-pad* אח"כ *decoding* – כל זוג מקודד חזרה לביט יחיד המתאים.

התקפה: ברשותי הודעה מוצפנת בת $2n$ ביטים (כאשר ההודעה m היא בעלת n ביטים): $c_1 \ldots c_{2n}$. כמו כן m מורכבת מחלק מקורי ומה- t שהוא ה-*MAC*. נניח כי הביט הראשון של ההודעה הוא 0, שהופך בקידוד ל-00, ובהצפנה עם המפתח הופך ל-$k_1 k_2$. בהתקפה <u>נהפוך</u> אותם: $\overline{k_1 k_2}$. התוקף מעביר לצד השני של השיחה, המפענח, מפענח את הביטים הללו ל-11, המתורגם ל-1. אם התחלנו מ-1, נניח פוענח ל-10, שמקודד ל-$\overline{k_1} k_2$, היריב הופך ל-$k_1 \overline{k_2}$ ואז הצד השני של השיחה, המפענח מתרגם את זה ל-01 (הפוך מהקלט המקורי), שמתורגם ל-1. כלומר: 0 הועבר ל-1, אך 1 נשאר 1.

<u>פתרון שני לתקשורת בטוחה</u>:

שרת מפתחות מרכזי שיספק מפתח לכל שיחה. להלן פרוטוקול למניעת מחזור הודעות:

- יוזם השיחה I שולח הודעה ראשונה לבקשת הקמת $session$ עם המקבל, R: $I \underset{I,R}{\rightarrow} KS$ (KS הוא שרת המפתחות).
- $KS \underset{N}{\rightarrow} I$: השרת שולח הודעה N ל-I.
- $I \xrightarrow[MAC(I,R,N)]{} KS$: היוזם שולח אותנטיקציה לשרת.

<u>פתרון שלישי: הצפנה באמצעות מפתח פומבי</u>

<u>פתרון רביעי: מע' חתימה</u>

- שימוש באלגוריתם ליצירת מפתח חתימה ווידוא: $G() \rightarrow s, v$
- אלגוריתם נוסף להחתמת ההודעה: $SIG_s(m) \rightarrow \sigma$
- אלגוריתם וידוא $Ver_v(m, \sigma) = 0 \; or \; 1$

שימוש: כל שחקן בוחר מפתח הצפנה ופענוח, שומר מפתח פענוח ומפתח הצפנה, כנ"ל לגבי מפתחות חתימה ווידוא. כיצד ניתן להעביר מפתח פומבי בצורה אמינה לצדדים האחרים:

- העברת המפתח ביד – לא פרקטי בקנה מידה גדול.
- שימוש בשרת מפתחות.

דרך סטנדרטית להקמת תקשורת בטוחה:

- הסכמה על המפתח משותף – $key\ exchange$
- הצפנה ואימות של התקשורת עם המפתח המשותף.