יסודות הקריפטוגרפיה שיעור #12

נושאי היום:

- סכמות זיהוי, ספציפית פיאט-שמיר.
- סכמות הצפנה פומבית בסגנון knapsack ושבירתן.

סכמות זיהוי:

מודל ונושאים עיקריים:

המטרה היא לאפשר זיהוי בכדי לתת גישה למשאבים וכו'. בדוגמא הכללית אליס רוצה להזדהות בפני בוב ואיב רוצה להתחזות לאליס. התחזויות:

- One time impersonation
- Full time impersonation: identity theft.

תרחישים שונים הדורשים זיהוי:

- זיהוי לוקאלי: ע"י אדם מזהה או ע"י מתקני זיהוי.
- זיהוי מרחוק: זיהוי תחילה ע"י אדם מזהה...

זיהוי תחילתי:

הבעיה היא כיצד אליס תחילה משכנעת מישהו שהיא אכן אליס. נניח שהזיהוי הראשוני מתבצע ע"י צד שלישי שעליו סומכים, נניח פקיד בבנק. נסמנו כ-Carol. קרול יכולה להעביר את חומר הזיהוי לאליס באמצעים מאובטחים. כיצד איב תתחזה לאליס?

סכמת פיאט-שמיר:

- אתחול
- Setup
- בניה בסיסית
- בניה משופרת
- Zero knowledge
- הסרת קשר

הסכמה:

- בוב מקבל $N = pq$ מקרול אך לא את הפירוק שלו.
- אליס בוחרת m מספרים באקראי R_i מ-$\mathbb{Z}_N$, מחשבת את הריבועים שלהם: $S_i = R_i^2$.
- אליס נותנת לבוב את S_i ושומרת בסוד את R_i.

שכנוע בוב שאליס היא אליס תעשה ע"י הוכחה שהיא יודעת את השורשים הריבועיים מבלי לחשוף את ה-R_i הסודיים – זה יעשה ע"י zero-knowledge. רוצים אם כך שיטה שתאפשר לבוב (ולכל מאזין) כלום מלבד לדעת שאליס יודעת למצוא את השורשים הריבועיים.

נניח כי $S_1 = R_1^2 (mod\ N)$, כיצד אליס תשכנע את בוב שהיא יודעת את S_1?

- אליס תבחר $X_1 \in \mathbb{Z}_N$ ומחשבת את $Y_1 = X_1^2 (mod\ N)$, ושולחת את Y_1 לבוב.
- אליס אומרת לבוב: היא יודעת את השורש הריבועי של Y_1 ואת השורש הריבועי של $Y_1 S_1$ $(mod\ N)$, ומכאן שהיא יודעת את השורש הריבועי של $S_1 (mod\ N)$. היא נותנת לבוב בחירה איזה מהשורשים של הנ"ל הוא רוצה שהיא תתן לו כהוכחה.
- בוב יבחר באקראי בהסתברות $\frac{1}{2}$ איזה מבין השניים הוא רוצה שאליס תתן לו. בהסתברות $\frac{1}{2}$ אליס תתבקש לתת את השורש של Y_1 ואז בעצם כל אחד יכול לעשות זאת (להתחזות לאליס ע"י יצירת X_1 וה-Y_1 המתאימים לו, לשלוח את המידע לבוב ולקוות שבוב יבקש את השורש של Y_1). אם נחזור על זה הרבה פעמים הסיכוי להתחזות שלא תתפס קטן. יתכן גם שמתחזה ידע את השורש של $Y_1 S_1$ ולא את השני, ואז גם בהסתברות $\frac{1}{2}$ (לכל היותר) המתחזה לא יתפס (באיטרציה אחת).

אם אליס יודעת את השורש של Y_1 ואת של $Y_1 S_1$, היא יודעת את השורש של S_1. אם היא לא יודעת את השורש של S_1, היא לא יודעת או את השורש של Y_1 או את השורש של $Y_1 S_1$ (או שניהם), ואז בהסתברות חצי בוב יעלה על מתחזה.

בפרוטוקול אליס בוחרת $Y_1, \dots, Y_m$, ובוב מטיל מטבעות $b_1, \dots, b_m$, ובוב מקבל את אליס אם מי שמולו מצליח **בכל** m המקרים.

פרוטוקול יעיל יותר:

בוב גם כאן בוחר m ביטים כאשר 0 עבור בקשת שורש ל-Y_iS_i ו-1 עבור בקשת שורש Y_i. הייעול הוא שבוב מבקש במקום עבור אחד אחד את:

- $\Pi\sqrt{Y_iS_i}\ where\ b_i = 1$ שזה $\Pi(X_iR_i)$
- $\Pi\sqrt{Y_i}\ where\ b_i = 0$ שזה $\Pi(X_i)$

זה ניתן כיוון ש-$\Pi\sqrt{a_i} = \sqrt{\Pi a_i}$. בעצם צמצמנו את תשובת אליס לשתי חזרות במקום m חזרות.

טענה: מול אליס שאינה מתחזה איב לא לומדת שום דבר חדש (כל דבר שהיא לומדת היא יכולה לסמלץ בעצמה).

מרכיבים חיוניים להצלחה:

- אינטראקציה.
- רנדומיזציה.

שיפור נוסף:

בוב מעביר לאליס במקום הגרלת b_i שונים את $b_1b_2 \dots b_m = H(Y_1, \dots, Y_m)$ - פונ' hash על Y_i שקיבל מאליס. אבל, הפונ' H ידועה לכולם והיא פסאודו-אקראית (פונ' hash מאובטחת).

מערכות עם מפתח פומבי מסוג knapsack:

ניזכר בבעיית $subset - sub \in NPC$:

נתונים n טבעיים שונים $a_1, \dots, a_n > 0$ ונתון $S \in \mathbb{N}$ (כולם בייצוג בינארי). השאלה (הכרעה): האם יש תת קבוצה של ה-a_i שסכומה הוא S. בעיה זו שקולה לבעיה: האם קיים וקטור $x_1 \dots x_n \in \{0,1\}^n$ כך ש-$\sum_{i=1}^n x_ia_i = S$.

מערכת מסוג knapsack:

- מפתח פומבי: $a_1, \dots, a_n$.
- הצפנה: $x_1 \dots x_n \in \{0,1\}^n$ כך ש-$ciphertext = S = \sum_{i=1}^n x_ia_i$

כדי לאפשר פענוח מוטב שיהיה מבנה נסתר (trapdoor info) שיתן יתרון למקבל הלגיטימי על פני המאזין. נתאר דרך ספציפית – הראשונה שהוצעה בספרות ע"י Merkle & Hellman (1978, יחד עם RSA).

נגדיר סדרה super increasing (עולה חזק) המקיימת:

- $a_2 > a_1$
- $a_3 > a_2 + a_1$
- $a_i > \sum_{j=1}^{i-1} a_j$

למשל (לא לקריפטו): $a_i = 2^i$. טענה: אם $\{a_i\}$ סדרה סופר עולה, הפענוח קל (בדיקה בינארית על כל איברי הסדרה האם הם נכנסים לסכום).

איך להסתיר את המבנה הסופר עולה? ההצעה הראשונית של MH: נבחר M הגדול מסכום ה-b_i שהם איברי הסדרה הסופר עולה הראשונית שמתחילים איתה. נבחר $W < M$ וזר ל-M, ונגדיר $a_i' = b_i \cdot W (mod\ M)$. נבחר באקראי תמורה $\pi \in S_n$ (תמורה על n איברים) ונגדיר $a_i = a'_{\pi(i)}$ (תמורה של ה-a_i') ומפרסמים את $\{a_i\}$.

- מפתח פומבי: $a_1, \dots, a_n$
- מפתח פרטי: M (מודולוס), W (כופל) ו-π (התמורה).
- פענוח: נתון $S = \sum_{i=1}^n x_ia_i$, x_i לא ידועים ורוצים למצוא אותם.

כיוון ש-W זר ל-M, יש לו הופכי $W^{-1} (mod\ M)$. נחשב:

$$C = S \cdot W^{-1} = \sum_{i=1}^n x_i(a_iW^{-1})\ (mod\ M) = \sum_{i=1}^n x_ib_{\pi(i)}$$

בעזרת תכונת הסדרה הסופר עולה מוצאים איזה $x_i = 1$ ולבסוף מפעילים את התמורה ההופכית למצוא מיקומים מקוריים. מומלץ לבחור את $b_i \approx 2^{i+n}$.

שריגים מעל $\mathbb{Z}^n$:

נתון בסיס $\overrightarrow{v_1}, \dots, \overrightarrow{v_n} \in \mathbb{Z}^n$ (n וקטורים שכל הקורדינטות שלהם שלמות). השריג הנפרש ע"י $\{\overrightarrow{v_i}\}$ הוא $L(\overrightarrow{v_1}, \dots, \overrightarrow{v_n}) = \{\sum_{i=1}^{n} a_i \overrightarrow{v_i} \mid a_i \in \mathbb{Z}\}$.

<u>שאלה בעלת עניין (וקשה)</u>: מהו הוקטור הקצר ביותר השונה מ-0 הנפרש ע"י הבסיס?

אלגוריתם של LLL: אם הוקטור הקצר ביותר בשריג n מימדי קצר בהרבה מהשני – יש אלג' יעיל למצוא אותו.

<u>ולעניינינו: שבירת knapsack "גנרית"</u>:

בהינתן מערכת knapsack נבנה עבורה שריג $n+1$ מימדי:

$$\begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \dots & & \ddots & \dots & \dots \\ 0 & 0 & \dots & 1 & -a_n \\ 0 & 0 & \dots & 0 & S \end{bmatrix}$$

וקטור הקשור לפענוח: $\sum_{i=1}^{n} x_i v_i + v_{n+1} = (x_1, x_2, \dots, x_n, 0)$ כאשר קורי ה-x_i הם 0 או 1. אם a_i גדולים יחסית, הוקטור הנ"ל יהיה קצר מאוד ואלגוריתם LLL ימצא אותו ואת ה-x_i ולכן יפענח. היוריסטיקה (לא מוכח ב-100%) שעובדת!