קריפטוגרפיה - מערכי ההצפנה

מערכי ההצפנה האסימטריים:

צד ע"י אפשרות סודיות - אפשר ההצפנה ואפשר הפענוח.

משמעות האפשר ההצפנה כך, להצפין את ההודעה ואפשר הפענוח כך, לפענח את ההודעה המוצפנת.

בהצפנה היום שעל אותו אחד (למשל צד שני האפשרות) לעיון להצפין ולפענח.

הקריפטוגרפיה המודרנית - שיטות ההצפנה הסימטריות.

Diffie & Helman 76' - הצעה על ההצפנה הפומבית.

אם שניים נוהגים בדומה Rivest, Shamir, Adelman את שיטת ההצפנה הפומבית RSA.

רעיון ההצפנה הפומבית: שני אפשרות- אפשרת ההצפנה ואפשרת הפענוח כאשר אפשרת ההצפנה **פומבית** ואפשרת הפענוח סודי.

נניח לשתקנים פעסקים בהצפנה ופענוח A, B, C - Alice / Bob

ל Alice ו Bob יש אפשרת הצפנה ואפשרת פענוח, השתקנים פעקבלו על ההצפנה ופענוח.

פעקבלו ההצפנה והפענוח של Alice P_A, S_A הן פעקבלו- פתח עף אחרית ההודעה D ואחרת ההודעה המוצפנת- שהיחד געתו אף לפעל- D. $P_A: D \to D$, $S_A: D \to D$ (תמורות של D)

ובנוסף כך עף $x \in D$ מתקיים $S_A(P_A(x)) = x$, $P_A(S_A(x)) = x$

הדרישות הבסיסיות בהצפנה פומבית:

(1) עף משתנה Y הינן עף שהוא תפשהר לאפשרת ההצפנה של Alice.

(א) מכירה פומבית) ובאו יכל לחשב בקלות את ההצפנה $P_A(x)$ עף הודעה x.

(ב) רק Alice תכל לפתח את ההודעה המוצפנת $P_A(x)$ עף (בעזרת) האפשרת ההצפנה, שפתח אפשר הפענוח. כלו"ז - קשה כי: אף יודע לחשב $S_A(x)$, אלא כלי האפשרת הפענוח לינו לחשב בקלות את $S_A(x)$.

$\mathbb{Z}_n^* = \{a \mid 1 \le a \le n-1 \text{ ו- } \gcd(a,n)=1\}$.

החבורה הכפלית $\mathbb{Z}_n^*$ מורכבת מכל המחלקות מגדל n שנציגיהן זרים ל-n.

החבורה הציקלית מגדל n: $\mathbb{Z}_n = \{1, \dots, 0\}$ והפעולה היא חיבור מודולו n. $n = |\mathbb{Z}_n|$.

החבורה הכפלית מגדל n

• תכונות מגדירות: בחבורה ציקלית מגדל n

הגנרטורים הינם פונקציות אוילר המחלק המשותף של a ו-b.

האלגוריתם הינו פונקציות המקבלות x,y המקיימות $ax+by=\gcd(a,b)$

• קיים אלגוריתם יעיל לחישוב $\gcd(a,b)$ – האלגוריתם של אוקלידס

• קיים אלגוריתם יעיל לחישוב המקדמים x,y המקיימים $ax+by=\gcd(a,b)$

זהו אלגוריתם אוקלידס המורחב.

• תכונה: $\gcd(a,b)$ – הגדול המחלק המשותף של a ו-b.

אלגוריתמים מספריים:

$\gcd(a,b)$ – המחלק המשותף המקסימלי של a ו-b.

• d מחלק משותף של a,b אם d מחלק את a וגם את b.

• המחלק המשותף המקסימלי $\gcd(a,b)$ הוא המספר הטבעי הגדול ביותר שניתן להציגו כ-$ax+by$ כאשר $x,y \in \mathbb{Z}$

• האלגוריתם יעיל לחישוב $\gcd(a,b)$ – מספר הצעדים הוא פולינומי בגודל הקלט.

• d מחלק משותף של a,b אם d מחלק את $\gcd(a,b)$

$\gcd(a,b)$ – המחלק המשותף המקסימלי של a ו-b.

שיטת קושי הדיפי-הלמן (המשך) את קושי הסבירות של שיטת RSA שהיו שיטת ההצפנה הפומבית שעליה קושי על פי רוב מסוג בעיות הלוגריתם הדיסקרטי.

נניח ש-Bob רוצה לשלוח הודעה $x \in \mathbb{Z}_n^*$ ורוצה שאליס תדע כמה שיותר שאיש אחר לא יוכל לגלות את ההודעה Bob שולח את הצפן $(x, S_B(x))$

ההחתמה של Bob על ההודעה x.

כאשר מגיע A יכול לבדוק $x = (S_B(x))_{P_B}$ ולוודא את ההודעה, אבל שים - כל שלא את אפשרי הפענח הסוד קשה מאוד לחשב $S_B(x)$ מהצפן x, ולכן קשה לזייף את ההחתמה של Bob.

כפי
למשל $\mathbb{Z}_{12}^* = \{1,5,7,11\}$. הפעולה בחוגרה $\mathbb{Z}_n^*$ היו כפל מודולו n.

טבלת הכפל של $\mathbb{Z}_{12}^*$:

	1	5	7	11
1	1			
5		1		
7			1	
11				1

למה: $\mathbb{Z}_n^*$ סגורה לפעולת הכפל.

הוכחה: יהי $a \in \mathbb{Z}_n^*$. נמצא $b \in \mathbb{Z}_n^*$ כך ש $(a \cdot b) \bmod n = 1$.

מתקיים a זר ל n, כלומר קיימים מספרים שלמים x, y כך ש

$$ax + ny = gcd(a,n) = 1$$

לכן $ax \bmod n = 1 \leftarrow ax - 1 = -ny \overset{\bmod n}{=} 0$

נסמן $b = x \bmod n$ ואז $ab = ax \bmod n = 1$.

כי לפי אי הפשטות נכון $ab = ax \bmod n$.

אז נתון כי $b = x \bmod n \Rightarrow n \mid x - b$

$\Rightarrow$ יש k כך ש $x - b = kn$ לכן $ab - ax = a(b-x) = akn \overset{\bmod n}{=} 0$.

נראה כי $b \in \mathbb{Z}_n^*$. נמצא $y \in \mathbb{Z}_n$ שזר לפחות עם n.

נשים לב שמספיק למצוא מספרים x', y' כך ש

$$bx' + ny' = 1$$

נמצא x, y כך ש $ax + ny = 1$, $b = x - kn$

$$ax + ny = a(x - kn) + n(y + ka) = 1$$

$$ba + n(y + ka) = 1$$

נקבל $x' = a$, $y' = y + ka$ ונקבל את הפתרון הרצוי. ■

הערה: נשים לב כי הפתרון $b \in \mathbb{Z}_n^*$ יחיד ונסמן את $b = a^{-1}$ הפתרון ההפוך.

הגדרה (פונקציית אוילר) של $\mathbb{Z}_n^*$ מסומן ב $\varphi(n)$ ומקיים שמספר איברי n, ושווה:

יהי הפירוק של n לגורמים ראשוניים הוא $n = p_1^{e_1} \cdots p_k^{e_k}$ אז

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

למשל $12 = 2^2 \cdot 3$! $\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = \frac{12}{3} = 4$.

עמוד

הערה חשובה: בהינתן a, b, n שהם מספרים טבעיים, כך ש-$a < n$ ו-$b < n$, ניתן לחשב את $a^e \pmod n$ בסיבוכיות $O(\log e)$ פעולות כפל, ולכן בסיבוכיות $O(\beta^3)$ פעולות בסיביות.

שיטת ההצפנה הפומבית של RSA:

1. נבחר שני מספרים ראשוניים **גדולים** $p \neq q$.
2. נסמן $n = p \cdot q$.
3. נבחר e מספר זר ל-$(p-1)(q-1) = \varphi(n)$ (כלומר $\gcd(e, \varphi(n)) = 1$).
4. נחשב $d = e^{-1} \pmod{\varphi(n)}$.

* כל המספרים הפומבי: (n, e)
* המפתח הסודי (פרטי): (n, d)
* מרחב ההודעות: $\mathbb{Z}_n$
* פונקציות ההצפנה והפענוח:

$$P_A(x) = x^e \pmod n \quad \text{// הצפנה}$$
$$S_A(y) = y^d \pmod n \quad \text{// פענוח}$$

נוכיח: לכל $x \in \mathbb{Z}_n$ מתקיים $S_A(P_A(x)) = x$

הוכחה:

$$S_A(P_A(x)) = S_A(x^e \pmod n) = x^{ed} \bmod n$$

צריך להוכיח $x^{ed} \bmod n = x$

ראשי להוכיח שאם $a = 1 \pmod{\varphi(n)}$ אזי $x^a \bmod n = 1$