1 קריפטוגרפיה

1.1 שיטת ההצפנה הפומבית של RSA.

1.1.1 מה זה הצפנה?

אליס (A) רוצה לשלוח הודעה לבוב (B) כך שרק בוב יוכל לקרוא את ההודעה הזאת. ההודעה נכנסת למצפין. יוצאת הודעה מוצפנת למרחב הפתוח. בפרט רואה אותה האיש הרע (E). ההודעה נכנסת למפענח, שמחזיר אותה להודעה המקורית שבוב יכול לקרוא.

M מרחב ההודעות, M' מרחב ההודעות המוצפנות. ברשות A ו-B נמצאים מפתחות הצפנה ופענוח סודיים, המגדירים פונקציות הצפנה ופענוח סודיות. פונקציית הצפנה $f_E : M \to M'$, ופונקציית פענוח $f_D : M' \to M$ כך שלכל $m \in M$, מתקיים $f_D(f_E(m)) = m$.

ב- 1977 $Diffie \,\&\, Hellman$ הציעו את הרעיון התיאורטי של שיטת הצפנה פומבית. יש הרבה משתמשים. כל משתמש יכול לייצר מפתח הצפנה פומבי. (ולכן פונקציית הצפנה פומבית) ומפתח פענוח פרטי שרק הוא מכיר, ושמאפשר לפענח את ההצפנה.

דרישה טכנית: נדרוש כי $M = M'$ ולכן אם $f_D(f_E(m)) = m$, אז גם $f_E(f_D(m)) = m$. (זה מאפשר את שימוש 2).

שימושים:

1. ספר טלפונים של משתמשים המכיל את מפתחות ההצפנה הפומביים של כל המשתמשים, כל אחד יכול לכתוב הודעה מוצפנת למשתמש, רק המשתמש יכול לקרוא.
2. חתימה דיגיטלית. A מפרסם את $F_E^{(A)}$. כדי לחתום על מסמך m, A מפרסם את הזוג $(m, f_D^{(A)}(m))$. רק A יכול לחתום על m, אבל כולם יכולים לוודא $f_E^{(A)}(f_D^{(A)}(m)) = m$ ובכך לוודא את החתימה.

הדרישה היותר מדוייקת: בהינתן מפתח הצפנה\פענוח, ניתן לחשב באופן יעיל את פונקציית ההצפנה\הפענוח. ללא המפתח לא ניתן לעשות זאת באופן יעיל.

נחשוב על $M = M' = \{0, ..., n-1\}$. ונחשוב על פונקציות מודולו n.

$$f_E : x \to x + a \ (mod(n))$$

$$f_E : x \to x^2 \ (mod(n))$$

1.1.2 שיטת ההצפנה הפומבית של RSA (1978)

אלגוריתם 1 שיטת ההצפנה הפומבית של RSA (1978)

---

1. נגריל שני מספרים ראשוניים שונים, p, q, כל אחד בגודל בערך 2^{500}. נגדיר $n = p \cdot q$. נגדיר $M = \{0, ..., n-1\}$.
2. נמצא $1 \leq \underline{e} \leq (p-1) \cdot (q-1)$ מספר (די קטן) כך ש-$\underline{e}$ זר ל-$(p-1) \cdot (q-1)$.
3. נמצא $1 \leq d \leq (p-1) \cdot (q-1)$ כך ש-$d \cdot \underline{e} \equiv 1(mod(p-1)(q-1))$
4. נפרסם את הזוג (n, e) כמפתח הצפנה פומבי. נשמור לעצמנו את d כמפתח פענוח פרטי.

פונקציות ההצפנה והפענוח:

$$f_E(x) = x^e(modn)$$
$$f_D(y) = y^d(modn)$$

__**שאלות:**__

1. שאלות מתמטיות: למה קיימים ראשוניים p, q בשלב הראשון? למה קיים $\underline{e}$ בשלב השני? למה קיים d בשלב השלישי? למה לכל $m \in M$ מתקיים $f_D(f_E(m)) = m$.
2. שאלות אלגוריתמיות: למה כל הפעולות ניתנות לביצוע יעיל? כלומר למה ניתן לבצע את כל השלבים של האלגוריתם של RSA באופן יעיל? למה פונקציות ההצפנה והפענוח ניתנות לחישוב יעיל?

נשים לב כי כאשר מדובר באלגוריתמים המקבלים כקלט מספר טבעי או זוג מספרים טבעיים ומחזירים מספרים טבעיים, אלגוריתם נחשב יעיל אם זמן הריצה שלו פולינומי בגודל **הייצוג** של המספרים בקלט.

1.1.3 הרקע המתמטי הנדרש - תורת המספרים האלמנטרית

__**1) פעולות מודולריות:**__

__**הגדרה:**__ בהינתן שני מספרים טבעיים a ו-b, ניתן לרשום באופן יחיד $b = q \cdot a + r$ כאשר q הוא מספר טבעי ונקרא לו __**המנה**__ ו-$0 \leq r \leq a$ הוא מספר טבעי שנקרא לו __**השארית**__.

__**הגדרה:**__ יהי a מספר טבעי, נגדיר פונקציה $mod(a) : \mathbb{N} \rightarrow \{0, ..., a-1\}$ באופן הבא: לכל $b \in \mathbb{N}$ נתאים את השארית של חלוקה של b ב-a.

__**לדוג':**__

$$\begin{array}{rcccccccccccc} mod(5): & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots \\ & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & \cdots \end{array}$$

__רישום:__ נרשום (היסטורית) את $(mod(a))(b)$ באופן אחר: $b(mod(a))$ נרשום גם $b \equiv c(mod(a))$ כרישום מקוצר להגיד ש-$b(mod(a)) = c(mod(a))$.

__**תכונות של פעולות מודולו:**__

לכל $a, b, c \in \mathbb{N}$ מתקיים:

.1 .

$$(b+c)(mod(a)) = (b(mod(a)) + c(mod(a))\,(mod(a))$$

.2 .

$$(b\cdot c)(mod(a)) = (b(mod(a)) \cdot c(mod(a))\,(mod(a))$$

דוגמא:

$$mod(7) :(13+5)^{100} = (6+5)^{100} = 4^{100} = 16^{50} = 2^{50} = 4\cdot 2^{3\cdot 16} = 4\cdot 8^{16} = 4\cdot 1^{16} = 4$$

הגדרה: **מחלק משותף מקסימלי** של שני מספרים טבעיים a,b הוא המספר הטבעי הגדול ביותר ש-a ו-b מתחלקים בו. נסמן אותו ב-$gcd(a,b)$.

לדוג':

$$gcd(48,20) = 4$$

הגדרה: **אלגוריתם אוקלידס** מקבל כקלט שני מספרים טבעיים a,b ומחזיר את $gcd(a,b)$ בזמן פולינומי באורכי הייצוגים של a,b.

הגדרה: **אלגוריתם אוקלידס המורחב** מקבל כקלט שני מספרים טבעיים a,b ומחזיר שני מספרים שלמים x,y כך ש-$x\cdot a+y\cdot b = gcd(a,b)$.

(נלמד בתרגול). (בפרט האלגוריתם מוכיח כי קיימים x,y כאלה).

הגדרה: שני מספרים טבעיים a,b נקראים **זרים** אם $gcd(a,b)=1$.

הגדרה: מספר טבעי נקרא p יקרא ראשוני אם הוא מתחלק רק בעצמו וב-1.

עובדה (פירוק לגורמים ראשוניים): כל מספר טבעי ניתן להצגה יחיד כמכפלה של חזקות של ראשוניים, כלומר עבור $a\in\mathbb{N}$:

$$a = p_1^{k_1}\cdot p_2^{k_2}\cdot \ldots \cdot p_t^{k_t}$$

כאשר $p_1,\ldots,p_t$ ראשוניים שונים, $k_1,\ldots k_t$ מספרים טבעיים.

לדוג':

$$48 = 2^4\cdot 3$$

מסקנות:

1. a מתחלק בראשוני p אמ"ם p מופיע בפירוק של a לגורמים ראשוניים.
2. אם a מתחלק בשני מספרים ראשוניים שונים p, q, אז הוא מתחלק גם ב-$p \cdot q$.
3. a, b מספרים זרים אמ"ם אין מספר ראשוני שמופיע גם בפירוק של a וגם בפירוק של b לגורמים ראשוניים.

הגדרה: עבור מספר טבעי a, נגדיר $\pi(a) = |\{p : 1 \leq p \leq a, p\ is\ prime\}|$ (כמות כל הראשונים שקטנים מ-a).

עובדה (התפלגות הראשוניים): $\pi(a) \sim \frac{a}{ln(a)}$.

עובדה: יהי p מספר ראשוני, אזי המבנה האלגברי הבא: $\{0 \leq x \leq p-1$, עם פעולות חיבור וכפל מודולו $p\}$ $\mathbb{F}_p$ הוא שדה.

טענה (המשפט הקטן של פרמה): יהי p מספר ראשוני, ויהי a מספר טבעי שלא מתחלק ב-p. אזי $a^{p-1} \equiv 1(mod(p))$

לדוג':

$p = 7$, $a = 20$:

$$20^6 = 6^6 = 36^3 = 1^3 = 1$$

הוכחה (המשפט הקטן של פרמה):

בגלל התכונות של הכפל מודולו p, מספיק להוכיח כי $(a(mod(p))^{p-1} \equiv 1(mod(p))$ ולכן מספיק להוכיח כי לכל $a \in \mathbb{F}_p$, $a \neq 0$ מתקיים (בשדה $\mathbb{F}_p$) כי $a^{p-1} = 1$. נגדיר העתקה $\phi : \mathbb{F}_p \to \mathbb{F}_p$ באופן הבא: $\phi(x) = a \cdot x$. נשים לב לכך שאם $a \cdot x = a \cdot y$ עבור $x, y \in \mathbb{F}_p$, אזי $a^{-1}(ax) = a^{-1}(ay) \Leftarrow x = y$. לכן $\phi(x)$ חח"ע ולכן $\phi(x)$ על (כי היא חח"ע על קבוצה סופית). בנוסף $\phi(0) = 0$ ולכן ϕ חח"ע ועל גם על הקבוצה $\{x \in \mathbb{F}_p : x \neq 0\} = \{1, ..., p-1\}$.

לכן מתקיים

$$\prod_{\substack{x \in \mathbb{F}_p \\ x \neq 0}} x = \prod_{\substack{x \in \mathbb{F}_p \\ x \neq 0}} \phi(x) = \prod_{\substack{x \in \mathbb{F}_p \\ x \neq 0}} (ax) = a^{p-1} \prod_{\substack{x \in \mathbb{F}_p \\ x \neq 0}} x$$

נסמן $X = \prod_{\substack{x \in \mathbb{F}_p \\ x \neq 0}} x$, אזי $X \neq 0$ וקיים X^{-1}. החישוב הקודם נותן: $X = a^{p-1} \cdot X$. נכפול ב-X^{-1} בשני האגפים ונקבל כי $a^{p-1} = 1$ ב-$\mathbb{F}_p$.

1.1.4 הוכחות על RSA

טענה: פונקציית ההצפנה והפענוח של RSA הופכיות אחת לשנייה, כלומר לכל $m \in M$ מתקיים $f_E(f_D(m)) = f_D(f_E(m)) = m$

הוכחה: פונקציות ההצפנה והפענוח הן:

$$f_E(x) \equiv x^e (mod n)$$
$$f_D(y) \equiv y^d (mod n)$$

ולכן:

$$f_D(f_E(m)) \equiv (m^e mod\, n)^d (mod\, n) \equiv m^{d \cdot e} (mod\, n)$$

לפי בחירת d ו-e, ומהגדרת פונקציית המודולו קיים מספר טבעי b כך ש-$de = b(p-1)(q-1)+1$. צריך להוכיח כי:

$$m^{b(p-1)(q-1)+1} \equiv m (mod\, n)$$

באופן שקול, צריך להוכיח כי

$$m^{b(p-1)(q-1)+1} - m = m \cdot (m^{b(p-1)(q-1)-1} - 1)$$

מתחלק ב-n. נחלק למקרים:

1. m לא מתחלק לא ב-p ולא ב-q: m לא מתחלק ב-p גם $m^{b(q-1)}$ לא מתחלק ב-p. לפי המשפט הקטן של פרמה, $(m^{b(q-1)})^{p-1} = m^{b(p-1)(q-1)} = 1(mod\, p)$ כלומר $m^{b(p-1)(q-1)} - 1$ מתחלק ב-p. משיקול דומה, $m^{b(p-1)(q-1)} - 1$ מתחלק גם ב-q. לכן הוא מתחלק בשני ראשוניים שונים - p, q, ולכן מתחלק ב-$n = p \cdot q$ ולכן גם $m \cdot (m^{b(p-1)(q-1)-1} - 1)$ מתחלק ב-n.
2. m לא מתחלק ב-p וכן מתחלק ב-q: במקרה זה שוב $m^{b(q-1)}$ לא מתחלק ב-p. ולכן כמו קודם $m^{b(p-1)(q-1)} - 1$ מתחלק ב-p. בנוסף, על פי ההנחה, m מתחלק ב-q ולכן $m \cdot (m^{b(p-1)(q-1)-1} - 1)$ מתחלק ב-n.
3. m מתחלק ב-p ולא מתחלק ב-q: בדיוק כמו המקרה 2. (בהחלפת p ו-q)
4. m מתחלק גם ב-p וגם ב-q: במקרה זה m מתחלק ב-$n = pq$. מכיוון ש-$M \in m$ נקבל $m = 0$ בשדה ולכן בוודאי $m \cdot (m^{b(p-1)(q-1)-1} - 1) = m = 0$.

1.1.5 סיפורים

כך עושים את שלב 1 של האלגוריתם:

(הערה) האלגוריתם לבדיקת ראשוניות של מספר נתון m
1. נגריל a מקרי בין 2 ל-$m-1$.
2. נבדוק האם $a^{m-1} \equiv 1(mod\, m)$

1.1.6 מידע על המבחן:

יהיו ווריאציות במקום שינון. סוגי ווריאציות:

1. שלושה פסי ייצור במקום 2.
2. כיסוי קודקודים, שיכסה כל משולש (עיגול $\frac{1}{3}>$)
3. FFT^{-1} במקום FFT.

יהיו 2 ווריאציות כאלה ו2 שאלות חדשות. צריך לבחור 3 מתוך 4.