הצפנה משפחת סודי:

אולם לא כולם שמעוניין לשדר יודע ש־ה־מספר.

הצפנה משפחת סודי: נניח כעת שלשני הצדדים יש מילון משלב לי:

0	1
1	$n-1$
17	2
3	0
4	
⋮	
$2-n$	3
$n-1$	$2-n$

$i \to k$ ↔ ϕ

מספר $M = \{0, \dots, n-1\}$

כדי ליישם: אולם יכול מספרים מיוצג את טבלה

כלומר פונקציה $M \to M$: ϕ = המפתח הסודי.

פשוט מוצא את

כ. $m = (m)\phi)^{-k}$ (כי: ϕ^{-k} פונקציה הפוכה)

לדוגמה: $2 \xrightarrow{i \to k}$ 17 $\to$ 17 $\xrightarrow{\phi}$ 2

תרגיל: אולם זכות לדרכים להסכים מוגן כך שיתאים את המפתח הסודי: =הטבלה= המתאימה. אבל גם את כלה לשלם לשבור מכולם אשמה אנו לא יודעים מאום כמעט, משפחת הטון המפתח סודי. אבל בדרך לשם גם לא נדרוש שמפתח מוגן כמו שהוא מוגן בפועל. (ב) הפתרון הקשה יותר הוא בכך

לכל k (כדי לקבל בסכי תולדה ההצפנה) את סימון מלא

זכור שאנו יודעים שהמפתח הסודי, אולמנו מסתיים (בערך) להמין אלף שהם הקטנו לגמרי שנבנה ב־2^{256} ב־10^{308} מליארד בערך.

בפועל ברכה, הם מצמו לי פרטיות־הצפנה במפתח קבוע: הכמה ה־RSA ה־2^{128} ה־2^{64} שהיה הצו תשל כיוסן שמיר ואדלמן ב־1977, כשהמחשבים היו הרבה יותר איטיים ממה שהם היום, אולי מתאים, שהיו מיוחו יכול להאזין בקלות... אבל גם את כלה לשלם לשבור מכולם אשמה אנו לא יודעים מאום כמעט, משפחת הטון המפתח סודי. אבל בדרך לשם גם לא נדרוש שמפתח מוגן כמו שהוא מוגן בפועל. (ב) הפתרון הקשה יותר הוא בכך

שיטה זו שולל כיצד לא יוכל אף אחד אחר לחתום במקומו. $(P_A(m), m)$ אך בדרישת נכונות התוצאה $P_A(m) = (\text{שולל } S_A)$.

1. m = המסמך שלו אלס רוצה לחתום.
2. אלס מחשב $S_A(m) = \sigma$
3. אלס שולח בזאר את המסמך + החתימה: (σ, m)
4. א' שרלה לוודא שאכן אלס חתם על m פרץ לבדוק אכן $m = (\sigma) P_A$ (זה בר, לזה כי $m = (m) S_A P_A$).

סכמת החתימה הדיגיטלית:

תחתימה דיגיטלית מוגדרת ע"י סכמת ההצפנה הבאה:

P_A שולח m ומקבל $P_A(m)$, כך שקיים התאמה זו"ח בלוח שלפיו אלס חתם.

פרמליות: אלס רוצה לחתום על מסמך $m \in M$, כך שקיים התאמה זו"ח בלוח המתאים בדרך כלל תלוי לו שלך אחד לא יוכל להתחזות ולחתום במקומו. בזאר, לחתום אלו ולהתריע כך הזאר. לא יכול למנוע שלוח יקבלו את המסמך (m) ואת החתימה ($P_A(m)$) שנשלח ע"י אלס כלפי מסמך (מסמך הפוך: m).

שלבי הזרקה מלאים מאת אלס:

[מה שמשלה: למרות שלך הלוח מכיר את הפרץ P_A אלך אלס לכן יתלה על הפרץ S_A, ולמרות שלו יכול להבין את ל הלבלה וכמה למה אבל ולא מאוד צפוי מה להסתכן יש לו לזה מעט). הקשר: למעשה גם S_A, P_A של סוף הפסוק שמאוזן P_A לפי גם לא למעשה יש S_A כדי להבין את ל הלבלה.]

לכל $m \in M$ $\quad (P_A(m))S_A = m = ((m)S_A)P_A$ $\quad$ (פוך הפכיות לזוג S_A, P_A)

[מלכתחילה אלס מגדיר לאלס מפתח מסוג S_A, P_A

$P_B : M \to M$ $\quad$ $S_B : M \to M$ $\quad$ } כאשר יש לזכור שאין נשתמש כלל. כך שאנו יודעים.

אלס יש $\quad P_A : M \to M$ (מפתח) שאינו סודי public - ידוע לכל (אפילו כאל) $\quad S_A : M \to M$ (מפתח) שאינו סודי secret - סוד של אלס בלבד.]

סכמת החתימה הדיגיטלית: (מה שלא לאלס תמיד מלבין על מסמך אחת או אחרת).

נשמע שאלו = בזה $\quad$ והתשובה = אלס

אלגוריתם ה-RSA (שדרוג מערכת ההצפנה P_A, S_A). בקורס אלמ"ס

① יהיו p, q ראשוניים גדולים (מספר ביט, מהסדר של 2^{300} ספרות) (מומלץ: p, q בגודל דומה אך לא קרובים מדי זה לזה, כדי שהפירוק לגורמים ראשוניים של n יהיה קשה)

② יהי $n = p \cdot q$

③ מצא מספר b כך ש- $\gcd(b, (p-1)(q-1)) = 1$ [ניתן לבדוק בקלות באמצעות אלגוריתם אוקלידס, ולשם כך אין צורך לדעת את הפירוק לגורמים ראשוניים של n]

④ מצא את ההופכי הכפלי של b מודולו $(p-1)(q-1)$. כלומר a כך ש- $a \cdot b \equiv 1 \pmod{(p-1)(q-1)}$ (ניתן לעשות זאת בקלות אם יודעים את הפירוק של n לגורמים ראשוניים)

⑤ האנשים בעולם שרוצים להצפין הודעות לאליס מפרסמים את הזוג (n, b) (מפתח ציבורי). הפונקציה $P_A(m) = m^b \pmod n$ (מפתח ציבורי) ידועה לכולם. הפונקציה $S_A(m) = m^a \pmod n$ (מפתח אישי) ידועה רק לאליס.

כדי לשלוח הודעה m לאליס, שולחים $P_A(m)$ (ניתן לחשב בקלות אם יודעים את b ואת n, אך לא ניתן לחשב את m מתוך $P_A(m)$ אם לא יודעים את a).

הערה: ניתן להניח ש- $m \in \{0, 1, \ldots, n-1\}$ שכן אחרת ניתן לפרק את n ע"י חישוב $\gcd(m, n)$.

הוכחת נכונות אלגוריתם ה-RSA:

טענה: יהיו P_A, S_A הפונקציות המתקבלות מאלגוריתם ה-RSA. אז לכל $m \in \{0, 1, \ldots, n-1\}$ מתקיים

$$S_A(P_A(m)) = m = P_A(S_A(m))$$

הוכחה: יהי m כנ"ל

$$S_A(P_A(m)) = P_A(m^b) = (m^b)^a = m^{ab} \equiv m^{ab \bmod (p-1)(q-1)} \pmod n$$

$$P_A(S_A(m)) = S_A(m^a) = (m^a)^b = m^{ab} \equiv m^{ab \bmod (p-1)(q-1)} \pmod n$$

נותר להוכיח כי $m^{ab} \equiv m \pmod n$

מכיוון ש- $ab \equiv 1 \pmod{(p-1)(q-1)}$ מספיק שניכיח כי ① $m^{ab} \equiv m \pmod p$ ② $m^{ab} \equiv m \pmod q$

(תזכורת: הוכחנו בתרגול שקיים g כך שמתקיים $g^a \equiv b \pmod n$ אם ורק אם $\gcd(b, n) = 1$).

נוכיח ①: אם $m \equiv 0 \pmod p$ אז $m^{ab} \equiv 0 \equiv m \pmod p$. נניח מעתה $m \not\equiv 0 \pmod p$.

מהנתון שידוע לנו כי $ab \equiv 1 \pmod{(p-1)(q-1)}$ נובע כי $(p-1) \mid ab-1$ ולכן קיים k כך ש- $ab = 1 + k(p-1)$

$$\Rightarrow m^{ab} \equiv m \cdot m^{k(p-1)} \equiv m \cdot (m^{p-1})^k \equiv m \cdot 1^k \equiv m \pmod p$$

(משפט פרמה הקטן)

② כיוון סימטרי:

$$m^{ab} \equiv m^{ab \bmod (p-1)(q-1)} \pmod q$$

$$\Rightarrow ab = 1 + k(p-1)(q-1) \Rightarrow ab - 1 = k(p-1)(q-1)$$

$$\Rightarrow \text{קיים } k \text{ שלם כך ש } 1 - pq = (1-b)(1-q)k \Rightarrow pq = 1 + (1-b)(1-q)k$$

$$\Rightarrow pq \mid (1-b)(1-q)k \Rightarrow pq \mid (1-b)(1-q)$$

(כי p, q ראשוניים)

מכיוון ש- b נבחר כך ש- $\gcd(b, (p-1)(q-1)) = 1$ נובע כי $p \mid 1-q$ או $q \mid 1-p$

נניח בה"כ כי $p \mid 1-q$ (אחרת נחליף את p ב- q ולהפך)

$$\Rightarrow \text{קיים } l \text{ שלם כך ש } 1 - q = lp \Rightarrow q = 1 - lp$$

$$\Rightarrow m^{ab} \equiv m^{1 + k(p-1)(q-1)} \equiv m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} \equiv m \pmod p$$

(משפט פרמה הקטן)

אבן הכריחו אותה לשנות את שם האתר...

ההצפנה של אותה שלישיה! הם פשוט כינו את מערכת RSA בשם "Ron was wrong, Whit is right" (משחק מילים על השמות של ריבסט, שמיר ואדלמן)

וכך הם פירקו לגורמים את n_1 ו-n_2 ואחר כך מצאו את d כמו קודם.

$$\left.\begin{aligned} n_1 &= pq \\ n_2 &= pr \end{aligned}\right\} \text{ אז } \quad p = \gcd(n_1, n_2)$$

כאשר יוסי ורון בחרו מספרים ראשוניים p ו-q שונים זה מזה, וחישבו את $n = pq$ ואחר כך את $\varphi(n) = (p-1)(q-1)$, הם בחרו מספר d שהוא זר ל-$\varphi(n)$ וחישבו את e כהופכי של d מודולו $\varphi(n)$. הפתח שלהם n היה משותף לכולם ולכן יכלה כל אחת מהשלישיות לפענח את ההודעות של השתיים האחרות. למרות שהמספרים היו גדולים מאוד, חישוב $\gcd$ לקח רק שבריר שנייה, ומכאן ואילך הכל היה פשוט.

* מעלים בדעתי כי מלבד זאת, יש מאגר שאינו שייך למפתח עד לכאן אך הוא מכיל מידע חשוב שאליו יש לגשת. האם מישהו יודע מהו?

סוף