יסודות הקריפטוגרפיה שיעור 9#

Elgamal Public Key Cryptosystem:

- RSA מבוסס על קושי פירוק אך לא ידוע שהוא שקול.
- Elgamal מבוסס של קושי לוגריתם ב-$\mathbb{Z}_p$ אך לא ידועה שקילות.

<u>תזכורת ל-Diffie-Helman</u>:

- שני פרמטרים פומביים: p ראשוני גדול ו-$g \in \mathbb{Z}_p^*$ איבר פרימיטיבי.
- אליס בוחרת $a \in [0 \dots p-2]$, $x := g^a$
- בוב עושה אותו דבר: $b, y := g^b$
- y הוא פומבי, אליס מחשבת: $y^a = (g^b)^a = g^{ab}$
- x פומבי, בוב מחשב: $x^b = (g^a)^b = g^{ab}$
- g^{ab} הוא המפתח הסודי

<u>אלגוריתם Elgamal PKC</u>:

רוצים לבנות מפתח פומבי ופרטי של בוב: p הוא ראשוני גדול כאשר הפירוק של $p-1$ ידוע ובעל גורם גדול; מומלץ $p = 2q+1$ כאשר q הוא ראשוני. יהי g איבר פרימיטיבי, p, g פומביים. בוב בוחר באקראי $a \in [0 \dots p-2]$ ומפרסם את $\beta = g^a$, וגם β פומבי. המפתח הפרטי של בוב הוא a.

הצפנה:

- אליס רוצה לשלוח הודעה m לבוב, מפרקת לבלוקים.
- אליס בוחרת $k \in [0 \dots p-2]$ ומחשבת את $g^k (mod\ p)$ ואת $m \cdot \beta^k (mod\ p)$.
- אליס שולחת את $E(m) := (g^k, m \cdot \beta^k)$ לבוב. k הוא פרטי של אליס. לכל הודעה יבחר k שונה בכל פעם.

נראה (לא הוכחה) כי הדרך היחידה לחילוץ m היא מציאת k מתוך g^k, אך זו בעיית discrete log.

פענוח $(g^k, m \cdot \beta^k) = (c_1, c_2)$ ע"י בוב:

- $(g^k)^a = (g^a)^k = \beta^k$ - יכול לחשב זאת כי לבוב יש את a.
- ע"י xgcd ניתן לחשב את ההופכי הכפלי של β^k ב-$\mathbb{Z}_p^*$ וכך ניתן לחשב את $m \cdot \beta^k \cdot (\beta^k)^{-1} (mod\ p) = m$. אלטרנטיבה: חישוב $(\beta^k)^{p-2}$ שהוא ההופכי הכפלי של β^k כי $(\beta^k)^{p-2} \cdot \beta^k = (\beta^k)^{p-1} \equiv 1 (mod\ p)$ (נכון לכל $x \in \mathbb{Z}_p^*$).

<u>תכונות של המערכת</u>:

- ההצפנה היא אקראית: k אקראי. עם אליס תשתמש פעמיים באותו k: $\begin{cases} g^k, m_1 \beta^k \\ g^k m_2 \beta^k \end{cases} \Rightarrow \frac{m_1}{m_2}\ is\ known$, כלומר ניתן לחשב יחס בין הודעות. לכן מומלץ להשתמש ב-k שונים בכל פעם, גם עבור אותה הודעה. אם אותה הודעה נשלחת פעמיים עם k שונים: $\begin{cases} g^{k_1}, m \cdot \beta^{k_1} \\ g^{k_2}, m \cdot \beta^{k_2} \end{cases}$ נראה שלא ניתן להבחין שזה אותו m.
- הצפנה לוקחת 2 העלאות מודולריות בחזקה, פענוח לוקח אחת.
- ה-ciphertext ארוך כפליים מ-m.

<u>אי עמידות ל-chosen ciphertext attack</u>:

ב-RSA בהתקפה כזו היריב בוחר R באקראי ומחשב את $M' = R^e \cdot S$ כאשר $S = E(M)$ ומבקש מבוב לפענח. אחרי הפענוח מתקבל $R \cdot S^d$ כלומר את $R \cdot M$ ומכאן אפשר מיד להוציא את M.

גם הצפנה זו לא עמידה: נניח נתון לנו הצפנה של k: $m, (c_1, c_2) = (g^k, m \cdot \beta^k)$. אם בוחרים s אקראי $(c_1, s \cdot c_2) = (g^k, s \cdot m \cdot \beta^k)$. אם נקבל את הפענוח של (c_1, sc_2) נקבל את $s \cdot m$ וכך נוכל לחשב מיד את m.

- המערכת היא מולטיפליקטיבית, דוגמא במצגת שקופית 8.

<u>תזכורת: האם DH מסתירה אינפורמציה חלקית?</u>

האם אפשר להסיק בכל זאת משהו על ההודעה, בהינתן g^a, g^b (Diffie-Helman)?

- בשדה מחצית האיברים הם QR: $x \in QR$ אמ"מ $x^{\frac{p-1}{2}} - 1$ – לבדוק האם g^a, g^b הם QR זה קל.
- דבר נוסף: ניתן לדעת על זוגיות a (הביט האחרון שלו), שכן a זוגי אמ"מ g^a ב-QR (הוא שארית ריבועית). לכן למרות שמאמינים כי DL היא פונ' קשה לחישוב, הביט התחתון של המעריך "דולף".
- אם גם a וגם b אי זוגיים (קל לבדוק), אז $ab(mod\ p-1)$ אי זוגי ואז g^{ab}, המפתח המשותף, הוא לא ב-QR. אם אחד מ-a, b זוגי, אז g^{ab} הוא כן QR. לא בטוח שזה מעניין, אך זהו ביט שדלף לגבי המפתח הפרטי.

מסתבר שגם ל-Elgamal יש אינפ' חלקית שדולפת:

- $\beta = g^a$ פומבי, אז ניתן להכריע האם a זוגי או לא.
- מ-g^k גם על k ניתן ללמוד זוגיות
- אז על $\beta^k = g^{ak}$ ניתן ללמוד האם הוא ב-QR (בדומה ל-g^{ab} ל-RSA). כאשר התוקף יודע האם β^k הוא QR, אז הוא לומד גם האם $m \cdot \beta^k$ הוא QA. מכאן ניתן ללמוד האם m ב-QR (כי זו חבורה כפלית), וכך ללמוד על ביט אחד ב-m.

אם כן, אם לוקחים תת חבורה שהיא כולם ב-QR (ע"י לקיחת g של החבורה והעלות אותו בריבוע).

<u>תרגיל מחשבה</u>: אם $p = 2q + 1$ אז -1 אינו שארית ריבועית מודולו p.

<במצגת יש תזכורת על חתימות>

Elgamal Signature Scheme:

<u>יצירת המפתחות</u>:

יהי ראשוני גדול $p = 2q + 1$ כאשר q גם ראשוני גדול (p בגודל 1024 ביטים) ותהי H פונ' hash עמידה בפני התנגשויות.

- בוב בוחר איבר פרימיטיבי $g \in \mathbb{Z}_p^*$.
- $x \in [0 \dots p-2]$ נבחר באקראיות.
- בוב מחשב $y = g^x (mod\ p)$, והוא חלק מהמפתח הפומבי.

<u>אלג' החתימה</u>:

תהי M הודעה ותהי $m := H(M)$. בוב בוחר באקראי $k \in [0 \dots p-2]$ **זר** ל-$p-1$ (מתוך $\phi(p-1) \geq q-1$ כאלה).

- בוב מחשב את $r = g^k (mod\ p)$
- בוב מחשב את $s = (m - rx) \cdot k^{-1}\ mod\ p-1$
- בוב מוציא את r, s.
- החתימה היא: M, r, s.

<u>בדיקה של אליס שהחתימה היא אכן של בוב</u>:

- מפתח פומבי: p, g, y, $y = g^x$ ידועים.
- מפתח פרטי: x.
- אליס מקבלת M, s, r.

אליס בודקת האם $0 < r < p$ וגם $y^r r^s = g^m (mod\ p)$, ואם לא אליס דוחה.

מתקיים: $s = (m - rx)k^{-1}\ mod\ p-1$. לכן: $sk + rx = m\ mod\ p-1$. בגלל ש-$r = g^k$ אז $r^s = g^{ks}$. כיוון ש-$y = g^x$ אז $y^r = g^{rx}$. מכן: $y^r \cdot r^s = g^{rx} \cdot g^{ks} = g^{sk+rx} = g^m$.

<u>תכונות</u>:

כיוון שהחתימה היא ראנדומית, להודעה מסויימת יכולות להיות כמה הצפנות. אבל, אם נבחר את אותו k בכמה הודעות, זה יכול להוביל לשבירה. כמו כן, בחירת k תלויים אחד בשני זה גם בעייתי. עוד כמה תכונות...

זיוף צריך לכלול r, s כך ש-$y^r \cdot r^s = g^m (mod\ p)$ ונראה שדורש discrete log (אך טרם הוכח כשקול לו).

***

נושא חדש: חלוקת סוד: n out of n secret sharing:

- נניח נתון סוד חשוב s.
- קיים trusted dealer המחזיק בסוד.
- רוצים לחלק את הסוד בין n משתתפים כך ש:
  - רק יחד יוכלו לשחזר את הסוד.
  - אף תת קבוצה של $n-1$ מתוכם (או פחות) לא תוכל להסיק דבר מהחלקים שלה על s.

הדילר מחזיק בפונ' $F(S,r) \to (p_1,\dots,p_n)$ כאשר r הוא חלק אקראיות; המשתתף ה-i מקבל את p_i.

דרישת הסודיות: $\forall x.\forall i.Pr[S=x]=Pr[S=x|\{p_1,\dots,p_n\}\backslash\{p_i\}]$, כלומר כל $n-1$ חלקים לא מגלים דבר על הסוד המקורי.

<u>פתרון בהקשר הפשוט ביותר</u>:

הסוד הוא ביט s, עם התפלגות כלשהי: הדילר בוחר $n-1$ ביטים אקראיים לחלוטין ובת"ל $p_1,\dots,p_{n-1}$, והביט האחרון $p_n = s \oplus_{i=1}^{n-1} p_i$.

<u>טענה</u>: זו סכמה n-out-of-n לחלוקת סוד:

<u>1. שחזור</u>: $s = \oplus_{i=1}^{n} p_i$.

<u>2. לא לומדים כלום מתת קבוצה</u>: נראה שלכל בחירה של $n-1$ מהביטים $p_1,\dots,p_n$ הביטים מתפלגים אחיד ובאופן ב"ת, ללא קשר מהו s (ואז לא יכול להיות שההסתברות למצוא את s שונה מאשר קודם). נראה למשל עבור $p_2,\dots,p_{n-1},p_n$: $p_n = s \oplus_{i=1}^{n-1} p_i$. נראה שהביטים הללו ב"ת ע"י כך שנראה שלכל קונפיגורציה של $n-1$ ביטים $b_2,\dots,b_n$ הסיכוי שהביטים $p_2,\dots,p_n$ יקבלו את הערכים $b_2,\dots,b_n$ היא בדיוק $\frac{1}{2^{n-1}}$.

עבור הביטים $p_2,\dots,p_{n-1}$ ע"פ הבניה; נתונה הקונפיגורציה $p_2,\dots,p_{n-1}$ ורוצים להראות שבהסתברות $\frac{1}{2}$ יהיה לנו $p_n = b_n$ בהינתן כל היתר.

$p_1 \oplus \underbrace{[s \oplus_{i=2}^{n-1} p_i]}_{const\ at\ this\ point}$ - כאשר p_1 טרם נקבע, נבחר אחיד וב"ת, לכן בהסתברות $\frac{1}{2}$ יכה ב-b_n.

לו היינו מטפלים במרחב סופי אחר של סודות (לאו דווקא $\mathbb{Z}_2$), היינו ממפים אותם ל-$\mathbb{Z}_m$ כאשר m הוא מספר הסודות, ואז החלק ל-$p_1,\dots,p_{n-1}$ יהיה $r_i \in \mathbb{Z}_m$ שנבחר באקראי ו-$p_n = s - \sum_{i=1}^{n-1} p_i \ mod\ m$ (XOR הוא סכום מודולו 2; - או + לא משנה למודולו 2, יותר מכך זה משנה).