יסודות הקריפטוגרפיה תרגול #8

פירוק - המשך:

הסיכוי שמספר בסד"ג של n יתפרק לגורמים ראשוניים שכל אחד מהם קטן מ-$n^{\frac{1}{a}}$ הוא בערך a^{-a}.

רוצים למצוא a,b לא קשורים אחד לשני כך ש-$a^2 = b^2 \bmod n$. אז נקח: $\Pi_i p_i^{e_i} \equiv r^2 \pmod n$, ונרצה למצוא r_i^2 שיחליף את האגף השמאלי. נגריל כאלה ונקבל רשימה: $r_1^2 = \Pi_i p_i^{e_{i_1}} \bmod n, \ldots, r_k^2 = \Pi_i p_i^{e_{i_k}}$. מעל קבוצת הראשוניים $B = \{p_1, \ldots, p_m\}$. אפשר למצוא תת קבוצה תלויה לינארית $\{e_{1_i} \bmod 2, \ldots, e_{m_i} \bmod 2\}$.

<u>סיבוכיות</u>:

נניח שבדיקה האם ראשוני נמצא בקבוצה שלנו B עולה לנו $O(m)$. את B אנחנו לוקחים כרצוננו, כאשר סביר שראשוניים קטנים יופיעו במספר שנרצה (למשל 2 מאוד נפוץ כגורם). כדי למצוא מספיק r-ים צריך לבצע a^a נסיונות וכל אחד יעלה m. בשביל לאזן את פתרון המערכת ומציאת היחסים (משהו מהצורה $r_j^2 = \Pi_i p_i^{e_{i_j}}$) לוקחים $m = e^{\sqrt{\ln n \cdot \ln \ln n}}$ ($n^{\frac{1}{4}} = e^{\frac{1}{4}\ln n}, \sqrt{n} = e^{\frac{1}{2}\ln n} \ldots$). לבסוף, מציאת התלות הלינארית מעל וקטורים באורך m תעלה לנו בערך m^3 (מערכת משוואות גאוסיאנית).

נרצה $r^2 (\bmod n)$ שיהיה "קטן" כדי שיתפרק בקלות.

$r = x + \lfloor \sqrt{n} \rfloor \ (small\ x)$

$r^2 \cong \left(x + \sqrt{n}\right)^2 = x^2 + n + 2x\sqrt{n} \underset{\bmod n}{\Longrightarrow} x^2 + 2x\sqrt{n}$

וכעת r^2 בסד"ג $\sqrt{n}$ ולא n.

כעת $r^2 - n = \Pi_{i=1}^m p_i^{e_i}$ אמ"מ $p \in B$ אז $p | r^2 - n$ אמ"מ $n = r^2 \bmod p$; n הוא QR ב-$\mathbb{Z}_p$. אם n אינו QR מודולו p, לא נכניס אותם ל-B.

כיוון ש-n-אז $p | r^2 - n$ למשוואה $p | (r+p)^2 - n = r^2 + p^2 + 2rp - n$. יש שני פתרונות r', r''. לכן $\begin{cases} r' + c \cdot p \\ r'' + c \cdot p \end{cases}$ הם כל המספרים המקיימים $p | x^2 - n$.

נאתחל מערך M כך ש-$M[x] = \left(x + \lfloor \sqrt{n} \rfloor\right)^2 - n$ עבור כל ה-x-ים איתם רוצים לעבוד. כעת לכל $p \in B$ נפתור את המשוואה $r^2 = n \bmod p$ לקבלת r', r''. נלך לכפולות $r' + cp, r'' + cp$ ונחלק אותן ב-p. נחזור על תהליך זה עם כל ראשוני. אם בסיום התהליך $M[x] = 1$ אז $\left(x + \lfloor \sqrt{n} \rfloor\right)^2 \bmod n$ מתפרק בדיוק למכפלת ראשוניים ב-B ($r = x + \lfloor \sqrt{n} \rfloor$). יש לטפל בנפרד במקרים כמו $p^2 | \left(x + \lfloor \sqrt{n} \rfloor\right)^2 - n$.

יש כיום אלגוריתמים טובים יותר, למשל *NFS* (קיצור של משהו עם הרבה אלגברה).