

**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- $a^2 = b^2 \pmod n$ . אז נקח:  $\prod_i p_i^{e_i} \equiv r^2 \pmod n$ , ונרצה למצוא  $r_i^2$  שיחליף את האגף השמאלי. נגדיל

כאלה ונקבל רשימה:  $r_k^2 = \prod_i p_i^{e_{ik}}, \dots, r_1^2 = \prod_i p_i^{e_{i1}} \pmod n$ . אפשר למצוא תת קבוצה תלויה לינארית  $B = \{p_1, \dots, p_m\}$ .  
 $\{e_1 \pmod 2, \dots, e_m \pmod 2\}$

סיבוכיות:

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  $r_j^2 = \prod_i p_i^{e_{ij}}$  לוקחים  $m = e^{\sqrt{\ln n \cdot \ln n}}$  (למשל  $\sqrt{n} = e^{\frac{1}{2} \ln n}, n^{\frac{1}{4}} = e^{\frac{1}{4} \ln n}$ ). לבסוף, מציאת התלות הלינארית מעל וקטורים באורך  $m$  תעלה לנו

בערך  $m^3$  (מערכת משוואות גאוסיאנית).

נרצה  $r^2 \pmod n$  שיהיה "קטן" כדי שיתפרק בקלות.

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

$$r^2 \equiv (x + \sqrt{n})^2 = x^2 + n + 2x\sqrt{n} \pmod n \implies x^2 + 2x\sqrt{n}$$

וכעת  $r^2$  בסד"ג  $\sqrt{n}$  ולא  $n$ .

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

כיוון ש- $n - p | r^2 - n$  אז  $p | r^2 - p^2 + 2rp - n = r^2 + p^2 + 2rp - n$ . למשוואה  $r^2 = n \pmod p$  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- $M[x] = (x + \lfloor \sqrt{n} \rfloor)^2 - n$  עבור כל ה- $x$  איתם רוצים לעבוד. כעת לכל  $p \in B$  נפתור את המשוואה  $r^2 = n \pmod p$  לקבלת

$r', r''$ . נלך לכפולות  $r' + cp, r'' + cp$  ונחלק אותן ב- $p$ . נחזור על תהליך זה עם כל ראשוני. אם בסיום התהליך  $M[x] = 1 \pmod n$  אז  $(x + \lfloor \sqrt{n} \rfloor)^2 \pmod n$

מתפרק בדיוק למכפלת ראשוניים ב- $B = \{p_1, \dots, p_m\}$ . יש לטפל בנפרד במקרים כמו  $p^2 | (x + \lfloor \sqrt{n} \rfloor)^2 - n$ .

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