יסודות הקריפטוגרפיה תרגול 7#

אלגוריתם *Polard*:

$f: S \to S$ "מקרית", $x_0 \in S$, $x_{i+1} = f(x_i)$: האיברים מתחלקים לשתי קבוצות. הראשונה היא כל האיברים עד תחילת המחזור, השניה היא האיברים במחזור (ρ של פולארד). גודל ה-ρ עצמו הוא בערך $2\sqrt{|S|}$ - $\sqrt{|S|}$ בחלק לפני המחזור, ו-$\sqrt{|S|}$ במחזור עצמו.

אם $n = pq$, $f(\alpha) = x^2 + c \bmod n$: ניתן להסתכל על סדרת הערכים כסדרה מודולו n וגם כסדרה ב-$\mathbb{Z}_p$ וגם $\mathbb{Z}_q$. נסתכל על הסדרות הבאות:

- x_i - מודולו n
- y_i - מודולו p
- z_i - מודולו q

מתקיים: $x_i = \alpha y_i + \beta z_i$. רוצים למצוא את הנקודה בה מחזור אחד התחיל, נגיד p, והשני עוד לא התחיל, נגיד q. אם מתקיים $y_i = y_j$ וגם $z_i \neq z_j$ אז אם נסתכל על $x_i - x_j = \alpha(y_i - y_j) + \beta(z_i - z_j) = \beta(z_i - z_j)$ ומתקיים $p|x_i - x_j$, כלומר p מחלק את זה: $\gcd(x_i - x_j, n) = p$ (זו α איזושהי כפולה של p אך לא של q). הזמן שלוקח למצוא שני x_i, x_j שווים מודולו p הוא בערך $2\sqrt{p}$ (פעם אחת להגיע לתחילת המחזור, פעם נוספת להתקדם מחזור שלם). זמן הריצה הוא לפיכך בערך $O(\sqrt[4]{n})$.

רוצים למצוא את כל האיברים הראשוניים עד n. אופציות:

- לבדוק כ"א בזמן $O(\log^3 n)$, סה"כ נקבל $n \cdot \log^3 n$ זמן ריצה.
- *Sieve of Eratosthenes*: מתחילים עם רשימת כל המספרים; שלב ראשון מסמנים את 2 כראשוני ומוחקים את כל הזוגיים; מסמנים את 3 ראשוני ומוחקים את כל הכפולות של 3; ממשיכים כך כאשר 4 מחוק ו-5 ראשוני. המספר הבא תמיד יהיה ראשוני כי מחקנו את כל אלו שיש להם מחלקים קטנים מהם שאינם 1. זמן הריצה: עבור ראשוני p מחקנו $\frac{n}{p}$ מהאיברים. זמן הריצה סה"כ: $n \cdot \sum_{p \leq n} \frac{1}{p} = n \cdot \ln \ln n$.
- עבור $n = pq$, אם נתונים לנו x, y כך ש-$x \neq \pm y$ אז $x^2 = y^2 \bmod n$, $n \mid (x-y)(x+y)$ ו-p מחלק את $(x-y)$ ו-q לא מחלק את $(x+y)$, ולכן $p = \gcd(x-y, n)$. נגריל x ונחשב $z \coloneqq x^2 \bmod n$. אם במקרה $z = y^2$ (בשלמים) סיימנו. אם $x_1^2 = z_1 = y^2 \cdot t, x_2^2 = z_2 = t^3$ אז $(x_1 x_2)^2 = (yt^2)^2$. $x_j^2 = z_j = \Pi_{i=1}^{k} p_i^{e_{ij}}$, ורוצים: $z_1 \cdot z_{20} \cdot z_{100} = \Pi p_i^{some\ even}$. נסתכל על מטריצת $e_{ij} \bmod 2$ ומחפשים קומבינציה לינארית שלהם:

$$(e_{ij}) \begin{pmatrix} 1/0 \\ 1/0 \\ \dots \\ 1/0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

אם נמצא קומבינציה לינארית כזו של השורות שמאפסת את המטריצה אז מאחר ויש לנו k ראשוניים שונים, מספיק שנאסוף $k+1$ זים (טורים), אז יש תלות. נצטרך להגריל הרבה xים ונצטרך לבדוק האם $x^2 \bmod n$ מתפרק יפה; בחרנו מראש k ראשוניים $p_1, \dots, p_k$ קבועים לכל התהליך. $x^2 \bmod n$ מתפרק יפה אם הוא מתפרק לראשוניים האלה, ואם המטריצה ....