9. April 2025

8. Übungsblatt Kryptologie

Aufgabe 1:

Der Rechenaufwand von Faktorisierungsalgorithmen sowie von Algorithmen zur Berechnung diskreter Logarithmen für eine Zahl n ist oft ungefähr von der Form

$$L_n(\alpha, c) = e^{c(\log n)^\alpha (\log \log n)^{1-\alpha}}$$

mit $\alpha \in [0, 1]$ und $c > 0$.

- Wie sieht diese Funktion in den Grenzfällen $\alpha = 0$ und $\alpha = 1$ aus?
- Zeigen Sie: Für $\alpha < \beta$ ist $L_n(\alpha, c) < L_n(\beta, c)$!
- Der Aufwand für das Zahlkörpersieb ist ungefähr $L_n(\frac{1}{3}, c)$ mit $c = \sqrt[3]{\frac{64}{9}}$, der für eine gute Implementierung des quadratischen Siebs liegt bei $L_n(\frac{1}{2}, 1)$. Ab welcher Größe von n ist das Zahlkörpersieb schneller?

Aufgabe 2:

- Bestimmen Sie für $g = 2, 3, 5$ das Bild der Abbildung $x \mapsto g^x \bmod 23$ und stellen Sie jeweils eine Tabelle der diskreten Logarithmen der Bildelemente auf!
- Finden Sie alle Elemente von $\mathbb{F}_{11}$, die die multiplikative Gruppe dieses Körpers erzeugen!
- p sei eine Primzahl der Form $p = 2p' + 1$ mit p' prim. Welche Ordnungen kann ein Element der multiplikativen Gruppe von $\mathbb{F}_p$ haben, und wie viele Elemente der jeweiligen Ordnung gibt es?

Aufgabe 3:

Das folgende Verfahren soll für eine beliebige Anzahl n von Teilnehmern $A_1, \dots, A_n$ zur Vereinbarung eines gemeinsamen Konferenzschlüssels führen. Der Operator $\oplus$ steht dabei für die Addition modulo n , wobei die Null mit n identifiziert wird, und $\ominus$ entsprechend für die Subtraktion modulo n .

Die n Teilnehmer einigen sich auf eine hinreichend große Primzahl p und ein $a \in \mathbb{Z}/p$, das eine hinreichend große multiplikative Ordnung in $(\mathbb{Z}/p)^\times$ hat. Sodann wählt jeder Teilnehmer A_i eine Zufallszahl $x_i \in \{2, \dots, p-2\}$, berechnet $u_i = a^{x_i} \bmod p$ und schickt diese Zahl an alle anderen Teilnehmer. Danach berechnet er $m_i = (u_{i \oplus 1} u_{i \ominus 1}^{-1})^{x_i} \bmod p$ und schickt auch diese Zahl an alle anderen Teilnehmern. Schließlich berechnet A_i noch die Zahl $s_i = u_{i \ominus 1}^{n x_i} m_i^{n-1} m_{i \oplus 1}^{n-2} \cdots m_{i \ominus 2}^1 \bmod p$.

- Wie vergleicht sich dieses Verfahren im Falle $n = 2$ mit dem Schlüsselaustausch nach DIFFIE-HELLMAN?
- Zeigen Sie, daß alle s_i gleich $a^{x_1 x_2 + x_2 x_3 + \cdots + x_{n-1} x_n + x_n x_1}$ sind!

Aufgabe 4:

Ihr geheimer ELGAMAL-Schlüssel ist 32; das System arbeitet mit der Basis $a = 2$ und modulo der Primzahl $p = 100\,003$.

- Welchen öffentlichen Schlüssel müssen Sie bekanntgeben?
- Entschlüsseln Sie die an Sie gerichtete Nachricht (23 094, 72 676)!

Abgabe und Besprechung am Mittwoch, dem 30. April 2025, um 15.30 Uhr