Wolfgang K. Seiler
Tel. 2515

B6, B4.08

3. November 2022

9. Übungsblatt Kryptologie

Aufgabe 1:

Das folgende Verfahren soll für eine beliebige Anzahl n von Teilnehmern $A_1, \ldots, A_n$ 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 $\left(\mathbb{Z}/p\right)^\times$ hat. Sodann wählt jeder Teilnehmer A_i eine Zufallszahl $x_i \in \{2, \ldots, p-2\}$, berechnet $u_i = a^{x_i} \bmod p$ und schickt diese Zahl an alle anderen Teilnehmer. Danach berechnet er $m_i = \left(u_{i\oplus 1} u_{i\ominus 1}^{-1}\right)^{x_i} \bmod p$ und schickt auch diese Zahl an alle anderen Teilnehmern. Schließlich berechnet A_i noch die Zahl $s_i = u_{i\ominus 1}^{nx_i} m_i^{n-1} m_{i\oplus 1}^{n-2} \cdots m_{i\ominus 2}^{1} \bmod p$.

a) Wie vergleicht sich dieses Verfahren im Falle $n = 2$ mit dem Schlüsselaustausch nach Diffie-Hellman?

b) Zeigen Sie, daß alle s_i gleich $a^{x_1x_2+x_2x_3+\cdots+x_{n-1}x_n+x_nx_1}$ sind!

Aufgabe 2:

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

a) Welchen öffentlichen Schlüssel müssen Sie bekanntgeben?

b) Entschlüsseln Sie die an Sie gerichtete Nachricht $(23\,094,\ 72\,676)$!

Aufgabe 3:

Finden Sie die kleinste vierstellige Primzahl, die kongruent eins modulo elf ist!

Besprechung am Mittwoch, dem 9. November 2022, um 15.30 Uhr