SMS1 für MC, FHS Hagenberg
12. Übungsblatt für den 19. Jänner 2006

Diffie-Hellman Schlüsseltausch:

1. Für eine Primzahl p heißt $\alpha \in \mathbb{Z}_p$ ein Generator (Erzeuger) der zyklischen Gruppe $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, wenn zu jedem $x \in \mathbb{Z}_p^*$ eine natürliche Zahl n existiert, sodass $x = \alpha^n$. D.h., jedes $x \in \mathbb{Z}_p, x \neq 0$, ist eine Potenz von α.

   Finden Sie zwei Generatoren von $\mathbb{Z}_7^*$.

2. Finden Sie einen Generator von $\mathbb{Z}_{27701}^*$. Siehe [1, 4.80].

3. Beschreiben Sie das Verfahren von Diffie-Hellman zum Schlüsseltausch (siehe [1, 12.47]):

   (a) Worauf müssen sich Alice und Bob im Setup einigen?

   (b) Welche Nachrichten werden ausgetauscht?

   (c) Wie ergibt sich der gemeinsame Schlüssel?

   (d) Kann man den gemeinsamen Schlüssel bestimmen, wenn man die zwischen Alice und Bob ausgetauschten Nachrichten kennt?

4. Alice und Sie wollen sich mit dem Verfahren von Diffie-Hellman auf einen gemeinsamen Schlüssel einigen. Sie verwenden die Primzahl $p = 1728439$ und den Generator $\alpha = 27318$ von $\mathbb{Z}_p^*$.

   Von Alice erhalten Sie die Nachricht $a = 580170$. Was antworten Sie? Wie lautet der gemeinsame Schlüssel?

Literatur

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.