Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Aufgabe 7.1 K15+4+8

a) Berechnen Sie alle Untergruppen von $\mathbb{Z}_{13}^*(\cdot, 1)$.

b) Welche Elemente von $\mathbb{Z}_{13}^*(\cdot, 1)$ generieren die Gruppe selbst? Warum sind diese Elemente von besonderem Interesse für den diskreten Logarithmus?

c) Führen Sie den Diffie-Hellman Schlüsselaustausch mit $p = 13$ und $g = 11$ durch.

d) Skizzieren Sie, wie der Angreifer Mallory einen Man-in-the-Middle-Angriff durchführen kann. Welche Möglichkeiten hat der Angreifer durch diesen Angriff? Welche Schutzziele könnte er verletzen?

Aufgabe 7.2

Sie nehmen in dieser Aufgabe die Rolle von Mallory ein und möchten den gemeinsamen Schlüssel von Bob und Alice ermitteln. Ihnen sind folgende (öffentliche) Werte aus dem entsprechenden Diffie-Hellman Schlüsselaustausch bekannt:
$p = 13, g = 2, a = 8$ und $b = 10$.

Hinweis: Nutzen Sie die Untergruppen von $\mathbb{Z}_p^*(\cdot, 1)$ für Ihre Überlegungen.

a) Welche Möglichkeiten kommen für den gemeinsamen Schlüssel $k_1 = k_2$ von Alice und Bob in Betracht?

b) Wie kommt diese Verwundbarkeit zustande?

c) Wie könnte diese Verwundbarkeit vermieden werden?

Hinweis Zur Lösung der folgenden Aufgabe ist eine selbstständige Recherche notwendig, um ein genaues und über die Vorlesung hinausgehendes Verständnis zu entwickeln. Lesetipps:
- RFC 3447: https://www.rfc-editor.org/rfc/rfc3447
- Freiermuth et al. [2014]
- Menezes et al. [2001]

Aufgabe 7.3 K20+15

Betrachten Sie den RSA-Algorithmus.

a) Seien die beiden Primzahlen $p = 41$ und $q = 17$ gegeben.

(i) Welcher der beiden Parameter $e_1 = 32$, $e_2 = 49$ ist ein gültiger RSA-Exponent? Begründen Sie Ihre Antwort.

(ii) Berechnen Sie den zugehörigen privaten Schlüssel $K_{pr} = (n, d)$. Benutzen Sie den erweiterten Euklidschen Algorithmus und geben jeden Berechnungsschritt an.

b) Verschlüsseln und Entschlüsseln Sie mit Hilfe des RSA-Algorithmus und nachfolgenden Werten. Benutzen Sie dazu nur einen Taschenrechner.

(i) $p = 3, q = 11, d = 7, m = 5$

(ii) $p = 5, q = 11, d = 3, m = 9$

Literatur

Karin Freiermuth, Juraj Hromkovič, Lucia Keller, and Björn Steffen. *Einführung in die Kryptologie – Lehrbuch für Unterricht und Selbststudium*. 2nd edition, 2014. doi: 10.1007/978-3-8348-2269-7.

Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001. ISBN 0849385237. URL https://cacr.uwaterloo.ca/hac/.