Übungsaufgaben zur Vorlesung Kryptologie

Helmut-Schmidt-Universität — Universität der Bundeswehr Hamburg
Professur für Allgemeine Nachrichtentechnik — Prof. Dr.-Ing. Udo Zölzer
Dr.-Ing. Martin Holters, Raum: H3 - R115, Tel.: 040 / 6541 - 3468

M.Sc. Patrick Nowak, Raum: H3 - R116, Tel.: 040 / 6541 - 3650

Übungsaufgaben zu Kap. 8: Schlüsselaustausch und öffentliche Schlüssel und Kap. 9: Rechnergestützte Blockchiffren

---

Aufgabe 1 — Unizitätslänge

Bestimmen Sie die Unizitätslänge bei Verschlüsselung mit einer kommerziellen Enigma! (Der Schlüssel umfasst die Lage der drei Rotoren sowie deren Anfangsstellung und die Stellung der Umkehrwalze.)

Aufgabe 2 — Diffie-Hellman-Schlüsselaustausch

Alice und Bob verwenden das Diffie-Hellman-Verfahren, um einen Schüssel auszuhandeln. Alice wählt $p = 11$, $g = 2$, $a = 6$, Bob wählt $b = 7$.

a) Welche Nachrichten tauschen Alice und Bob aus, um einen gemeinsamen Schlüssel zu ermitteln?

b) Wie lautet dieser Schlüssel K?

c) Warum wäre $g = 10$ eine schlechte Wahl gewesen?

Aufgabe 3 — ELGAMAL-Verschlüsselung

Alice und Bob verwenden das ELGAMAL-Verfahren, um mit Hilfe öffentlicher Schlüssel zu kommunizieren. Insbesondere sei der Fall untersucht, dass Bob eine geheime Nachricht in Form der Zahl $x = 5$ an Alice senden will. Alice wählt wie oben $p = 11$, $g = 2$, $a = 6$ zur Erzeugung des Schlüsselpaars, Bob wählt für die Verschlüsselung $b = 7$.

a) Wie lautet Alice' öffentlicher Schlüssel?

b) Wie lautet die verschlüsselte Nachricht, die Bob an Alice sendet?

Aufgabe 4 — RSA-Verschlüsselung

Wieder will Bob eine Nachricht unter Benutzung eines asymmetrischen Verfahrens an Alice senden. Dieses Mal soll jedoch das RSA-Verfahren zum Einsatz kommen. Alice wählt $p' = 7$, $p'' = 11$ und $e = 17$.

a) Wie lautet Alice' öffentlicher Schlüssel?

b) Wie lautet Alice' geheimer Schlüssel?

c) Wie lautet die verschlüsselte Nachricht, die Bob an Alice sendet, wenn die unverschlüsselte Nachricht $x = 2$ ist?

Aufgabe 5 — Elliptische Kurven

Es sei die elliptische Kurve

$$y^2 \equiv x^3 + x + 2 \mod 11, \quad x, y \in \mathbb{Z}_{11}$$

betrachtet. Berechnen Sie $5 \cdot P$ mit $P = (2, 1)$.

Aufgabe 6 — Galois-Fields

Es sei das Galois-Field GF(2^8), das mit dem Polynom $\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1$ erzeugt wird, betrachtet.

a) Berechnen Sie das multiplikative Inverse zu $\alpha^5 + \alpha^2$ mit Hilfe des erweiterten euklidischen Algorithmus.

b) Überprüfen Sie Ihr Ergebnis, indem Sie es mit $\alpha^5 + \alpha^2$ multiplizieren.