Übungsaufgaben zur Bearbeitung **zu Hause** vor der Übungsstunde

Aufgabe 1

Beim Diffie-Hellman-Schlüsseltausch werden zwei öffentliche Zahlen benötigt: Eine Primzahl p sowie eine ganze Zahl $g \in \{2, 3, \ldots, p-2\}$.
Es seien $p = 19$ und $g = 3$.

a) Alice wählt nun als geheimen Exponenten die Zahl 3, Bob wählt 2.
   - Welche Zahl wird von Alice an Bob übertragen?
   - Welche Zahl wird von Bob an Alice übertragen?
   - Wie lautet der generierte Schlüssel?

b) Zeigen Sie: p ist keine sichere Primzahl.
c) Zeigen Sie: g ist eine primitive Wurzel modulo p.
d) Der berechnete Schlüssel wurde nun in binärer Form als One-Time-Pad verwendet. Empfangen wurde der Chiffretext 5 (dezimal). Wie lautet die Botschaft im Klartext?

Aufgabe 2

Beim RSA-Verfahren veröffentlicht jeder Teilnehmer einen Schlüssel (n, c), wobei n das Produkt zweier großer Primzahlen p und q ist und c ein Exponent. Bob wählt die Primzahlen $p=3$ und $q=11$.

a) Ermitteln Sie alle möglichen Zahlen, die für Bob als öffentliche Schlüssel c geeignet wären.
b) Bob verwendet als öffentlichen Schlüssel die zweitkleinste in Frage kommende Zahl. Berechnen Sie Bobs geheimen Schlüssel d.
c) Alice möchte an Bob die Nachricht „EI“ senden. Berechnen Sie die verschlüsselte Nachricht y. Dabei wird als numerische Kodierung der Buchstaben deren Position im Alphabet verwendet (A=1,…).
d) Bob hat die Nachricht „RGAM“ empfangen und möchte sie entschlüsseln. Wie rechnet er?

Aufgaben zur Bearbeitung während der Übungsstunde

Aufgabe 3

Ein Teilnehmer am RSA-Verfahren hat ein einzelnes verschlüsseltes Zeichen gesendet, das den Wert 128 hat. Der öffentliche Schlüssel des Teilnehmers ist (187, 7). Knacken Sie die Verschlüsselung, indem Sie den privaten Schlüssel berechnen. Welches Zeichen wurde übertragen, wenn man von einer bei eins beginnenden Nummerierung des Alphabets ausgeht?

Aufgabe 4

Bisher wurde beim RSA-Verfahren nur der Angriff durch Faktorisierung des öffentlichen Schlüssels betrachtet.
Eine weitere Möglichkeit ist der Angriff durch Iteration. Hierbei wird die verschlüsselte Nachricht iterativ immer wieder verschlüsselt, bis man wieder die ursprüngliche Nachricht erhält.
Es sei:
(c, n) der öffentliche Schlüssel
$e_0 = x$ der Klartextblock
$e_1 = x^c \bmod n$ der verschlüsselte Text
Man bildet nun
$e_{i+1} = e_i{}^c \bmod n$ (i = 1, 2, 3, …)
Das kleinste $k \geq 1$ mit $e_{k+1} = e_1$ nennt man Iterationsexponent, $k - 1$ Wiederherstellungsexponent (gültig diesen Klartextblock).

a) Der öffentliche Schlüssel sei (17, 2773). Es wurde der verschlüsselte Block 1787 empfangen. Wie lautet der Klartextblock? Bestimmen Sie den Wiederherstellungsexponenten.
b) Eine der beiden verwendeten Primzahlen war $p=47$. Ist 17 als Verschlüsselungsexponent in Ordnung?
c) Es wird nun der öffentliche Schlüssel (3, 55) bzw. (11,55) verwendet. Bestimmen Sie den Wiederherstellungsexponenten des Klartextblocks 15.