Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 06.06.2005, 14h

Kryptografie
Übungsblatt 7

Aufgabe 22:
Mehrere Brauereien verdächtigen sich gegenseitig, gegen das bayerische Reinheitsgebot zu verstoßen. Techniker haben eine Sonde entwickelt, die fest in einem Biertank installiert werden kann, das dortige Bier auf verbotene Inhaltsstoffe analysiert, und eine daraus berechnete Nachricht per Funk an eine Überwachungszentrale übermittelt. Entwickeln Sie ein Protokoll, das den folgenden Anforderungen genügt.

1. Keine Brauerei kann die Nachricht einer Sonde so manipulieren, dass sie „Alles O.K." lautet, obwohl das nicht stimmt.
2. Jede Brauerei will den Klartext der Nachrichten der Sonden in ihren Tanks wissen, um eventuell rechtzeitig Verbesserungsmaßnahmen einzuleiten.
3. Behauptet die Überwachungsstelle fälschlicherweise, eine Nachricht „Bier ist nicht O.K." erhalten zu haben, so soll jede Brauerei in der Lage sein festzustellen, dass eine solche Nachricht nie gesendet wurde.
4. Alle Sonden sollen identisch sein und ihr Aufbau soll allen Parteien bekannt sein.

Aufgabe 23:
Zwei Parteien A und B verwenden das Diffie-Hellman-Protokoll zur Schlüsselvereinbarung. Sie einigen sich auf $p = 3602561$. Partei A wählt $a = 1082389$ und erhält $g^b = 983776$ von B zugeschickt. Mit dem resultierenden Schlüssel $k \in \mathbb{Z}/p\mathbb{Z}$ soll folgendes Kryptosystem angewendet werden.

1. Für eine Zahl $l \geq k$ sei $\bar{l}$ ihr nichtnegativer Rest modulo 26^4. Schreibe $\bar{l}$ in der Form $\bar{l} = a \cdot 26^3 + b \cdot 26^2 + c \cdot 26 + d$ mit $a, b, c, d \in \{0, \ldots, 25\}$ und bilde die Matrix $M(l) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Sei $l \geq k$ die kleinste Zahl, für die die von $M(l)$ definierte Abbildung $(\mathbb{Z}/26\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/26\mathbb{Z})^2$ invertierbar ist.
2. Klartext– und Geheimtexteinheiten sind Buchstabenpaare, die in Elemente von $(\mathbb{Z}/26\mathbb{Z})^2$ übersetzt werden.
3. Die Verschlüsselungsabbildung ist die Multiplikation mit $M(l)$.

a) Finden Sie die zwischen A und B vereinbarte Matrix $M(l)$.

b) Bestimmen Sie die Entschlüsselungsmatrix und dechiffrieren Sie $VHNHDOAM$.

Aufgabe 24:
Bei einem RSA-Kryptosystem mit $n = pq$ und öffentlichem Schlüssel e sei der Klartext $m \in \{0, \ldots, n-1\}$ gegeben. Wir definieren $c_0 := m$ und $c_i := c_{i-1}^e \bmod n$ für $i \geq 1$. Dann heißt die Zahl $s_m = \min\{i \geq 1 \mid c_i = m\}$ der *Wiederherstellungsexponent* von m. Es ist klar, dass man bei der Wahl von e im RSA-Kryptosystem unbedingt beachten muss, dass sich ein großer Wiederherstellungsexponent für hinreichend viele Klartexte m ergibt.

a) Was ist der Wiederherstellungsexponent von $m = 518$ für $(n, e) = (2773, 17)$?

b) Finden Sie den maximalen Wiederherstellungsexponenten im Fall $(n, e) = (2773, 17)$ und im Fall $(n, e) = (55, 7)$.

c) Beweisen Sie, dass s_m stets ein Teiler von $\mathrm{kgV}(\frac{p-3}{2}, \frac{q-3}{2})$ ist.

d) Eine Primzahl p heißt *sicher*, wenn $(p-1)/2$ wieder eine Primzahl ist, und *doppelt sicher*, wenn auch $(p-1)/2$ eine sichere Primzahl ist. Erklären Sie, warum bei doppelt sicheren Faktoren p, q von n das zugehörige RSA-Kryptosystem sehr sicher ist, und finden Sie 10 doppelt sichere Primzahlen.