PD Dr. Martin Kreuzer
Fakultät für Mathematik
Universität Regensburg

Regensburg, den 15.6.2000

Übungen zur Vorlesung "Kryptographie"

Blatt 5

(Abgabetermin: 29.6.2000)

Aufgabe 21. Zwei Parteien A und B vereinbaren, das folgende Public-Key-Kryptosystem zu verwenden.

1) Partei A wählt $a, b \in \mathbb{Z}$ und berechnet $M = ab - 1$. Dann wählt A noch zwei Zahlen $a', b' \in \mathbb{Z}$ und berechnet $e = a'M + a$ sowie $d = b'M + b$ und $n = (ed-1)/M$.

2) Partei A veröffentlicht das Paar (n, e). Der geheime Schlüssel sei d.

3) Will B eine Nachricht $m \in \{0, \dots, n-1\}$ an A senden, so soll er $c = e\, m \pmod n$ berechnen und an A übertragen.

4) A entschlüsselt die Nachricht, indem er $c\, d \pmod n$ berechnet.

a) Zeigen Sie, daß A die Nachricht m zurückerhält.

b) Wie kann man dieses Kryptosystem für digitale Signaturen verwenden?

c) Finden Sie einen Algorithmus, der dieses Kryptosystem knackt. Zeigen Sie, daß man das Kryptosystem genau dann knacken kann, wenn man diesen Algorithmus kennt.

Aufgabe 22. Briefmarkensammler A liegt im Krankenhaus und kann an der monatlichen Briefmarkenauktion nicht teilnehmen. Sein Bekannter B vom Briefmarkenclub bietet an, gegen ein Entgelt von 3% der Kaufsumme für A bei der Auktion mitzubieten. Beide besitzen leistungsstarke Notebook-Computer, die eine schnelle Kommunikation über das Internet ermöglichen.

a) Entwickeln Sie ein Protokoll, das den folgenden Anforderungen genügt.

1) A will sicher sein, daß B nur dann kauft, wenn ihn A mit einer verschlüsselten Nachricht dazu ermächtigt hat. Es soll nicht möglich sein, daß B ohne Erlaubnis kauft und eine fingierte Ermächtigung als Beleg vorweist.
2) B will sicher sein, daß A nach dem Kauf nicht plötzlich behaupten kann, er habe gar keine Ermächtigung geschickt.
3) Im Fall eines Streites soll ein Richter, dem alle Schlüssel vorgelegt werden müssen, den Fall eindeutig entscheiden können.

b) Schreiben Sie *CoCoA* Programme, die die verschiedenen Teile des Protokolls implementieren. Demonstrieren Sie die Korrektheit dieser Programme an einigen Beispielen.

Aufgabe 23. 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 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 24. 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 $\ell \geq k$ sei $\bar{\ell}$ ihr nichtnegativer Rest modulo 26^4. Schreibe $\bar{\ell}$ in der Form $\bar{\ell} = a \cdot 26^3 + b \cdot 26^2 + c \cdot 26 + d$ mit $a, b, c, d \in \{0, \ldots, 25\}$ und bilde die Matrix $M(\ell) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Sei $\ell \geq k$ die kleinste Zahl, für die die von $M(\ell)$ 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 $M(\ell)$.

a) Finden Sie die zwischen A und B vereinbarte Matrix $M(\ell)$.
b) Bestimmen Sie die Entschlüsselungsmatrix und dechiffrieren Sie $VHNHDOAM$.

Aufgabe 25. (Der Wiederholungsangriff auf das RSA Kryptosystem)
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 $c_i := c_{i-1}^e \pmod{n}$ 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 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.