Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 30.05.2005, 14h

Kryptografie
Übungsblatt 6

Aufgabe 19:

a) Schreiben Sie eine Funktion `MillerRabin(...)`, die mit Hilfe des Miller–Rabin–Primzahltests entscheidet, ob eine gegebene Zahl n eine Primzahl ist, wobei die Wahrscheinlichkeit, dass eine zufällig gewählte zusammengesetzte Zahl als Primzahl akzeptiert wird, $< \frac{1}{2^{20}}$ sein soll.

b) Wenden Sie Ihre Funktion aus a) an, um ein Programm `RandomPrime(...)` zu schreiben, dass eine Zahl $N > 0$ als Argument erwartet und eine zufällige Primzahl zwischen 10^N und 10^{N+1} erzeugt.

c) Schreiben Sie ein Programm `GenerateRSA(...)`, das ein Tupel (p, q, n, e, d) generiert, welches den Angriffen aus Aufgabe 11 widersteht, und so dass n mehr als 200 Stellen besitzt.

Aufgabe 20:
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 $m \in \{0, \ldots, n-1\}$ an A senden, so soll er $c = em \pmod{n}$ berechnen und an A übertragen.
4. A entschlüsselt die Nachricht, indem er $cd \pmod{n}$ berechnet.

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

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

c) Knacken Sie dieses Kryptosystem.

Aufgabe 21:
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. 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, das 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.