Geheimschriften mit Computeralgebra

Prof. Dr. Wolfram Koepf
Fachbereich Mathematik/Informatik
Universität Gh Kassel

koepf@mathematik.uni-kassel.de

http://www.mathematik.uni-kassel.de/~koepf

Kryptographie

- Nachricht: N
- Verschlüsselungsfunktion: V
- Schlüssel zum Verschlüsseln: e
- Entschlüsselungsfunktion: E
- Schlüssel zum Entschlüsseln: d
- Es gilt dann die Gleichung $E_d(V_e(N)) = N$
- Effizienz: V und E lassen sich schnell berechnen.

Symmetrische Verschlüsselungsverfahren

- Bei diesen klassischen Verschlüsselungs-verfahren benutzen Sender und Empfänger dieselben Ver- und Entschlüsselungs-schlüssel *e* und *d*.
- Problem: Sender und Empfänger müssen diese Schlüssel austauschen, bevor Sie korrespondieren können. Was ist, wenn der Schlüsselaustausch abgehört wird?

Caesar-Verfahren

- Es ist bekannt, dass Caesar bei seinen Feldzügen Nachrichten gerne verschlüsselt hat.
- Er verwendete hierzu folgendes einfache Verfahren: Jeder Buchstabe wird durch den drittnächsten ersetzt:
- ABCDEFGHIJKLMNOPQRSTUVWXYZ

wird zu

- DEFGHIJKLMNOPQRSTUVWXYZABC

Rechnerisches Caesar-Verfahren

- Ersetzt man jeden Buchstaben durch seine Nummer A → 0, B → 1, C → 2, D → 3, ..., Z → 25, so läuft das Ersetzen durch den drittnächsten Buchstaben auf eine Addition hinaus:

$$V(B) = B + 3$$

- Damit aber auch X, Y und Z richtig ersetzt werden, müssen wir modulo 26 rechnen:

$$V(B) = B + 3 \bmod 26$$

Entschlüsselung bei Caesar

- Die Entschlüsselung beim Caesar-Verfahren ist herzlich einfach. Die Verschiebung um e Buchstaben wird durch die Verschlüsselungsfunktion

$$V_e(N) = N + e \bmod 26$$

- beschrieben und hat die Entschlüsselung

$$E_{-e}(N) = N - e \bmod 26$$

Asymmetrische Verschlüsselungsverfahren

- Im Jahr 1976 hatten Diffie und Hellman eine revolutionierende Idee.
- Bei den von ihnen erfundenen asymmetrischen Verschlüsselungsverfahren benutzen alle Teilnehmer dieselben Verschlüsselungs-funktionen V und E, aber jeder Teilnehmer hat seine eigenen Schlüssel e und d.
- Diese Verfahren heißen Public-Key-Verfahren, aus folgendem Grund.

Öffentlicher und privater Schlüssel

- Public Key: Jeder Teilnehmer macht seinen Verschlüsselungsschlüssel *e* öffentlich bekannt, beispielsweise in einer öffentlichen Schlüsselliste im Internet, damit ihm jeder andere Teilnehmer verschlüsselte Nachrichten senden kann.
- Private Key: Jeder Teilnehmer hält seinen privaten Entschlüsselungsschlüssel *d* dagegen absolut geheim.

Eigenschaften

- Damit ein Public-Key-Verfahren sicher ist, muss es folgende Eigenschaften haben:
- Da der Verschlüsselungsschlüssel bekannt ist, darf es (mit vertretbarem Aufwand) nicht möglich sein, hieraus den Entschlüsselungsschlüssel zu bestimmen.
- Da dies im Prinzip aus $E_d(V_e(N)) = N$ aber möglich ist, muss die Funktion $F : d \rightarrow e$ eine Einwegfunktion bzw. Falltürfunktion sein.

Das RSA-Verfahren

- Im Jahr 1968 haben Rivest, Shamir und Adleman zum ersten Mal ein asymmetrisches Verschlüsselungsverfahren angegeben.
- Hierbei ist

$$V_e(N) := N^e \bmod n$$

und

$$E_d(M) := M^d \bmod n$$

Wie wählt man n, e und d?

- Der Empfänger bestimmt seine Werte wie folgt:
- Wähle zwei Primzahlen p und q mit jeweils mindestens 100 Dezimalstellen.
- Berechne $n = p \cdot q$.
- Berechne die Hilfsgröße $\varphi = (p\text{-}1)\,(q\text{-}1)$.
- Wähle $1 < e < \varphi$ mit $\mathrm{ggT}(e, \varphi) = 1$.
- Bestimme $1 < d < \varphi$ mit $d \cdot e = 1 \bmod \varphi$. Dies geht mit dem euklidischen Algorithmus.

Sicherheit des RSA-Verfahrens

- Wegen $V_e(N) = N^e \bmod n$ und $E_d(M) = M^d \bmod n$ ist also das Paar (e,n) der öffentliche und d der private Schlüssel.
- Kennt man φ, p oder q, so kann man – wie gesehen – aus dem öffentlichen Schlüssel e den privaten d berechnen.
- Die Falltürfunktion des RSA-Verfahrens ist die Faktorzerlegung $n = p \cdot q$.

Funktionsweise des RSA-Verfahrens

- Das RSA-Verfahren basiert auf dem Kleinen Satz von Fermat.
- Dieser besagt, dass für Primzahlen $p \in \mathbb{P}$ und für zu p teilerfremde $a \in \mathbb{N}$ gilt:

$$a^{p-1} = 1 \bmod p$$

- Hieraus folgt mit der Definition von e und d

$$E_d(V_e(N)) = N$$