RSA-KRYPTOSYSTEM

ULRICH THIEL

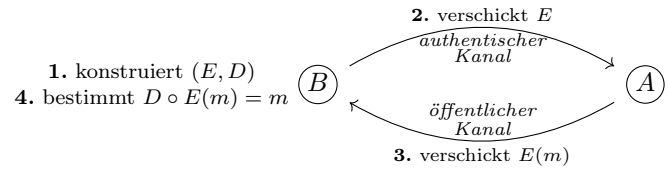
Zusammenfassung. Dies ist ein Transkript eines Kurz-Vortrags (15 Minuten) über das RSA-Kryptosystem, den ich für Studierende der Mathematik im 2. Semester gehalten habe.

Ziel. Person A möchte Person B geheime Nachrichten $m \in \mathcal{M}$ über einen öffentlichen Kanal schicken.[1]

Idee. A nimmt eine injektive Funktion $E\colon \mathcal{M} \to \mathcal{M}'$ (*Verschlüsselung*) und verschickt $E(m)$ an B. Da E injektiv ist, gibt es eine Funktion $D\colon \mathcal{M}' \to \mathcal{M}$ mit $D \circ E = \mathrm{id}_{\mathcal{M}}$ (*Entschlüsselung*).

Problem. B muss D kennen, aber niemand sonst darf D kennen.

Idee von Diffie–Hellman (1976). Angenommen: 1) es existiert ein authentischer Kanal zwischen A und B (abhörbar, aber nicht veränderbar); 2) man kann "leicht" Paare (E, D) erzeugen, aber von E allein lässt sich D nur "schwer" finden. Dann gibt es folgendes 4-stufiges Kryptosystem, das obiges Problem löst:



(0.1)

Annahme 1 kann man z.B. durch eine vertraute Instanz erreichen, mit der A und B direkt kommunizieren. Aber wie erreicht man Annahme 2?

Idee von Rivest–Shamir–Adleman (1978). Betrachte den Ring $\mathbb{Z}/n\mathbb{Z}$ für ein $n > 1$. Es sei $(\mathbb{Z}/n\mathbb{Z})^\times$ die Menge der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$. Es gilt

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{0 < m < n \mid m \text{ koprim zu } n\} \,. \tag{0.2}$$

Definiere $\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. Angenommen, es gilt $n = pq$ für *verschiedene* Primzahlen p und q. Nach dem Chinesischen Restsatz haben wir einen Ringisomorphismus

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \,, \quad x \mapsto (x \bmod p, x \bmod q) \,. \tag{0.3}$$

Folglich haben wir einen Gruppenisomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ und daher

$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) \,, \tag{0.4}$$

Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

E-mail address: thiel@mathematik.uni-kl.de.

Datum: 17. Mai 2021.

[1] Ich werde bewusst einige Begriffe nicht mathematisch präzise definieren.

wobei wir benutzen, dass $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/q\mathbb{Z}$ Körper sind, d.h. alle Elemente ungleich Null sind invertierbar.

Lemma 0.1. *Ist $l \equiv 1 \bmod \phi(n)$, so ist die Abbildung*

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,, \quad x \mapsto x^l\,, \tag{0.5}$$

die Identität.

Beweis. Nach Annahme ist $l = 1 + k\phi(n)$ für ein $k \in \mathbb{Z}$. Sei ψ der Isomorphismus des Chinesischen Restsatzes (0.3), d.h. $\psi(x) = (x \bmod p, x \bmod q)$. Da ψ ein Ringmorphismus ist, gilt

$$\psi(x^l) = \psi(x)^l = \big((x \bmod p)^l, (x \bmod q)^l\big)\,.$$

Für die 1. Komponente ergibt sich

$$\begin{aligned}(x \bmod p)^l &= (x \bmod p)^{1+k\phi(n)} = (x \bmod p)^{1+k(p-1)(q-1)}\\ &= (x \bmod p) \cdot \big(\big((x \bmod p)^{p-1}\big)\big)^{k(q-1)}\\ &= (x \bmod p) \cdot \begin{cases} 1 & \text{falls } x \not\equiv 0 \bmod p \text{ (kleiner Satz von Fermat)}\\ 0 & \text{falls } x \equiv 0 \bmod p \end{cases}\\ &= x \bmod p\,.\end{aligned}$$

Analog ergibt sich $(x \bmod q)^l = x \bmod q$ in der 2. Komponente. Da ψ ein Isomorphismus ist, schließen wir $x^l = x$. □

RSA-Kryptosystem.

(1) Wähle verschiedene Primzahlen p, q und setze $n \coloneqq pq$.
(2) Wähle ein e koprim zu $\phi(n) = (p-1)(q-1)$.
(3) Es gilt $e \in (\mathbb{Z}/\phi(n)\mathbb{Z})^\times$, d.h. es existiert ein d mit $ed \equiv 1 \bmod \phi(n)$. Berechne ein solches Element, z.B. mit dem Euklidischen Algorithmus.
(4) Betrachte die Funktionen

$$E\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,, \quad x \mapsto x^e\,, \tag{0.6}$$

$$D\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,, \quad y \mapsto y^d\,. \tag{0.7}$$

Es gilt $D \circ E = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$ nach Lemma 0.1.
(5) Verwende dieses (E, D) im Diffie–Hellman Kryptosystem.

Beobachtungen. Das Paar (E, D) ist "leicht" konstruierbar – wie gewünscht. Um D aus E, d.h. aus n und e, zu berechnen, muss man ein d mit $de \equiv 1 \bmod \phi(n)$ finden. Es wird *vermutet* (!), dass man dafür $\phi(n)$ kennen muss. Um $\phi(n)$ zu kennen, muss man bereits p und q kennen, denn es ist $\phi(n) = (p-1)(q-1) = pq - (p+q) + 1$ und damit $p + q = n - \phi(n) + 1$, d.h. p und q sind die Nullstellen des Polynoms $X^2 - (n - \phi(n) + 1)X + n$. Um also $\phi(n)$ zu kennen, muss man n faktorisieren. Es wird *vermutet* (!), dass Faktorisieren ein "schweres" Problem ist. Dafür muss man aber zumindest n sehr groß wählen, etwa einige tausend Dezimalstellen.

Nun stellt sich aber rückwirkend doch wieder die Frage: ist es wirklich "leicht", (E, D) zu konstruieren, d.h. zwei große Primzahlen zu finden? Die Antwort lautet: im Prinzip ja! Man wählt dazu eine große Zufallszahl k. Dann testet man, ob k eine Primzahl ist (das ist aber ebenfalls schwierig; in der Praxis begnügt man sich deshalb mit einem probabilistischen Test). Ist k keine Primzahl, so nimmt man $k+1$, testet, usw. Der Clou ist nun, dass es gar nicht so lange dauern wird, bis man einen Treffer hat, denn nach dem Primzahlsatz liegt die Wahrscheinlichkeit, dass

eine (genügend große) Zufallszahl k eine Primzahl ist bei $1/\ln(k)$, d.h. unter den Zahlen mit weniger als 1000 Dezimalstellen ist etwa eine von $\ln(10^{1000}) \approx 2302.6$ Zahlen eine Primzahl.

Zusammenfassung. Unter einigen mathematischen *Annahmen*, ist das RSA-Kryptosystem eine Lösung unseres urpsrünglichen Problems. Findet man eine schnelle Methode, um Zahlen zu faktorisieren (oder auch nur um ein d mit $ed \equiv 1 \bmod \phi(n)$ zu finden), ist das System hinfällig. In der Praxis wird man mit dem Lehrbuch-Algorithmus scheitern: es gibt darin sehr viele kritische Aspekte, z.B. muss man gewisse Typen von Primzahlen vermeiden, weil diese sich leicht als Faktor bestimmen lassen, etc.