Wiederholung

Die Eulersche ϕ-Funktion

$$\phi : n \mapsto \begin{cases} |(\mathbb{Z}/n\mathbb{Z})^\times| & n > 1 \\ 1 & n = 1 \end{cases}$$

Lemma 4.4: Sei $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$

Dann ist die Funktion

$$f_a : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$$
$$[b]_n \mapsto [a]_n [b]_n$$

eine Bijektion.

Bemerkung: Wegen Lemma 3.13 ist f_a tatsächlich eine Funktion von $(\mathbb{Z}/n\mathbb{Z})^\times$ nach $(\mathbb{Z}/n\mathbb{Z})^\times$

Beweis: Injektion

$$[a]_n [b_1]_n = [a]_n [b_2]_n \Rightarrow ([a]_n)^{-1} [a]_n [b_1]_n = ([a]_n)^{-1} [a]_n [b_2]_n$$
$$\Rightarrow [b_1]_n = [b_2]_n$$

Surjektion: $[b]_n = [a]_n \left(([a]_n)^{-1} [b]_n \right)$ □

Satz 4.5 (Satz von Euler-Fermat)

Sei $n \in \mathbb{N}^+$, $a \in \mathbb{Z}$ und $(a, n) = 1$

Dann gilt $a^{\phi(n)} \equiv 1 \mod n$

(kleiner Fermatscher Satz) insbesondere gilt für $p \in \mathbb{P}$, $p \nmid a \in \mathbb{Z}$

$$a^{p-1} \equiv 1 \mod p.$$

Beweis: Wegen Lemma 4.4 ist

$$\prod_{[b]_m \in (\mathbb{Z}/m\mathbb{Z})^\times} [b]_m = \prod_{[b]_m \in (\mathbb{Z}/m\mathbb{Z})^\times} [a]_m [b]_m$$

$$= [a]_m^{\phi(m)} \prod_{[b]_m \in (\mathbb{Z}/m\mathbb{Z})^\times} [b]_m$$

da alle $[b]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$ invertierbar sind, gelt

$$[a]_m^{\phi(m)} = [1]_m$$

$$\Rightarrow \quad a^{\phi(m)} \equiv 1 \mod m. \qquad \square$$

Korollar 4.6: Sei $(a,m) = 1$. Dann ist $a^{\phi(m)+1} \equiv a \mod m$

Sei $p \in \mathbb{P}$, $p \nmid a$, dann ist $a^p \equiv a \mod p$.

Sei $n = pq$, $p, q \in \mathbb{P}$ $p \neq q$

Dann ist $\phi(n) = (p-1)(q-1)$

Sei s teilerfremd zu $(p-1)(q-1)$ und $t \in \mathbb{N}$ sodass $ts \equiv 1 \mod (p-1)(q-1)$

und $a \in \mathbb{Z}$ sodass $(a,n) = 1$

Dann ist $(a^s)^t = a^{k\phi(n)+1} \equiv a \mod n$

Gegeben a, s und n, dann kann man $a^s \mod n$ leicht ausrechnen

Aber gegeben a^s, s und n, was ist a?

schwierig ohne t.

Das RSA - Verfahren

(Rivest, Shamir, Adleman, 1978)

Das RSA - Verfahren ist eine „Public-Key Verschlüsselung", d.h. ein kryptographisches Verfahren sodass jeder Benutzer verschlüsseln kann, aber nur ausgewählte Benutzer entschlüsseln können.

So wie ein Briefkasten - jeder kann einwerfen, nur ich habe den Schlüssel.

1. Man wähle zwei (große, unterschiedliche) Primzahlen p, q und eine (große) Zahl s teilerfremd zu $(p-1)(q-1)$
   Sei $t \in \mathbb{N}$ sodass $st \equiv 1 \mod (p-1)(q-1)$ und $n = pq$

2. Man veröffentliche n und s
   p, q und t bleiben geheim

3. Sei $a \in \mathbb{N}^+$ eine (Teil-)Nachricht
   a wird als $b \equiv a^s \mod n$ verschlüsselt

4. Zum entschlüsseln nehme man $b^t \mod n$
   $\equiv (a^s)^t \mod n$
   $\equiv a \mod n$.

Öffentliche Information

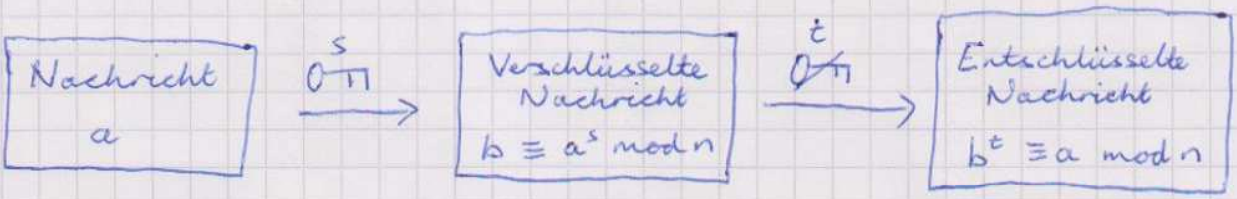
n, s

öffentlicher Schlüssel

Geheime Information

p, q, t

geheimer Schlüssel



Sehr einfaches Beispiel:

$n = 33$, $s = 7$

Nachricht 5

Verschlüsseln: $5^1 \equiv 5 \mod 33$

$5^2 \equiv 25 \equiv -8 \mod 33$

$5^3 \equiv -40 \equiv -7 \mod 33$

$5^4 \equiv -35 \equiv -2 \mod 33$

$5^5 \equiv -10 \mod 33$

$5^6 \equiv -50 \equiv -17 \equiv 16 \mod 33$

$5^7 \equiv 80 \equiv 14 \mod 33$

verschlüsselte Nachricht 14

Entschlüsseln: ?

oder verschlüsselte Nachricht 16

Entschlüsseln: ?

$n = 3 \cdot 11$

$\phi(n) = 2 \cdot 10 = 20$

$\phi(n) + 1 = 21 = 7 \cdot 3 \qquad t = 3$

Entschlüsseln: $14^1 \equiv 14 \mod 33$

$14^2 \equiv 196 \equiv -2 \mod 33$

$14^3 \equiv -28 \equiv 5 \mod 33$

$16^1 \equiv 16 \mod 33$

$16^2 \equiv 256 \equiv -8 \mod 33$

$16^3 \equiv -128 \equiv 4 \mod 33$

Bei Textnachrichten wird der Text in Buchstabengruppen aufgeteilt, jede Gruppe als Zahl kodiert und einzeln verschlüsselt

z.B.

A	B	C	D	E	...	S	T	...	X	Y	Z	Ä	Ö	Ü	ß
01	02	03	04	05		19	20		24	25	26	27	28	29	30

Nachricht T E X T kodiert: 2005|2420

2005 2420

Verschlüsselung: x|y $\qquad x \equiv 2005^5 \mod n$

$y \equiv 2420^5 \mod n$

Leerzeichen, Sonderzeichen und Ziffern können natürlich ähnlich behandelt werden

Varianten und Erweiterungen von RSA werden für viele Anwendungen benutzt

z.B. Online Banking

PGP

Webseite Zertifikat

⋮

Ist das sicher?

Die Sicherheit des RSA-Verfahrens basiert darauf, dass Primzahltests schneller sind, als in Primfaktoren zu zerlegen.

D.h. wir können zwei große Primzahlen p und q (relativ) leicht finden, aber $n=pq$ ist schwer zu zerlegen, ohne p und q vorher zu wissen.

p und q sollten in der Regel mindestens 300 Ziffern haben.

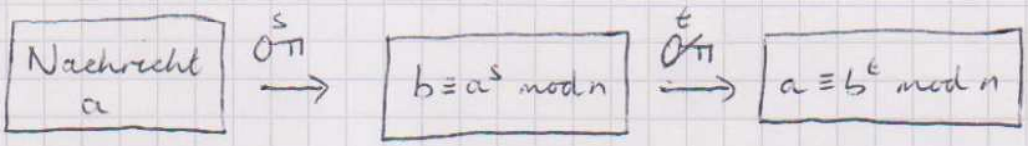
Allerdings ist es bisher nicht bekannt, ob Zerlegen wirklich schwieriger ist, als Primheit zu testen, oder ob Mathematiker bisher nur nicht die richtigen Ideen hatten.

Weitere Varianten

<u>Signatur</u>: Wie können wir wissen, dass eine Nachricht tatsächlich vom angegebenen Sender kommt?

Öffentliche Information: n, t

Geheime Information: p, q, s



Jeder kann entschlüsseln

Nur ich kann verschlüsseln

Sichere Kommunikation über unsicheren Kommunikationsweg

Ein Freund und ich wollen geheim kommunizieren, auch wenn ein Dritter jede verschickte Nachricht lesen kann.

Grundidee: Ich errichte einen Briefkasten und behalte den Schlüssel

Der Freund errichtet einen Briefkasten, behält einen Schlüssel und wirft einen zweiten in meinen Briefkasten.

Ich verwende das RSA-Verfahren mit $n' = p'q'$, s' und t'

öffentlich n', s' geheim p', q', t'

Der Freund wählt eine zweite RSA-Verschlüsselung mit $n = pq$, s und t.

Er veröffentlicht n, s, t mit (n', s') verschlüsselt

d.h. $n^{s'} \bmod n'$

$s^{s'} \bmod n'$

$t^{s'} \bmod n'$

Ich entschlüssele n, s und t, die jetzt unser Geheimnis sind.

Es gibt mathematisch raffiniertere Möglichkeiten

Nächstes Mal: Diffie-Hellman Schlüssel-Austausch