1.1 Beschreibung des Verfahrens

Parameter

$n =$ Modul,
$e =$ öffentlicher Exponent,
$d =$ privater Exponent.

mit der Eigenschaft

$$(\star) \quad m^{ed} \equiv m \pmod n \qquad \text{für alle } m \in [0 \ldots n-1].$$

Naive Beschreibung

In „erster Näherung“ setzt man

$$M = C = \mathbb{Z}/n\mathbb{Z}, \quad K \subseteq [1 \ldots n-1] \times [1 \ldots n-1].$$

Für $k = (e, d)$ ist

$$E_k : M \longrightarrow C, \qquad m \mapsto c = m^e \bmod n,$$
$$D_k : C \longrightarrow M, \qquad c \mapsto m = c^d \bmod n.$$

Diese Beschreibung ist naiv, weil n variabel und zwar (sogar zwingend, wie sich später zeigen wird) Teil des öffentlichen Schlüssels ist. Insbesondere sind sogar die oben verwendeten Mengen M und C variabel.

Genauere Beschreibung

Um zu einer Beschreibung zu kommen, die auf die allgemeine Definition einer Chiffre passt, gibt man als Parameter vor:

$l =$ Länge des Moduls in Bit („Schlüssellänge“),
$l_1 < l$ Bitlänge der Klartextblöcke,
$l_2 \geq l$ Bitlänge der Geheimtextblöcke.

Es wird eine Block-Chiffre über dem Alphabet $\Sigma = \mathbb{F}_2$ mit

$$M = \mathbb{F}_2^{l_1} \subseteq \mathbb{Z}/n\mathbb{Z} \subseteq \mathbb{F}_2^{l_2} = C$$

konstruiert. Dabei wird ein Schlüssel $k = (n, e, d) \in \mathbb{N}^3$ gewählt mit

$$\ell(n) := \lfloor {}^2\!\log n \rfloor + 1 = l, \quad 1 \leq e \leq n-1, \quad 1 \leq d \leq n-1,$$

so dass die obige Eigenschaft $(\star)$ erfüllt ist. Dabei ist $\ell(n)$ die Zahl der Bits, das heißt, die Länge der binären Darstellung von n.

Ein Klartextblock m der Länge l_1 wird als Binärdarstellung einer natürlichen Zahl $< n$ gedeutet und kann so mit E_k verschlüsselt werden; das Ergebnis c, wieder eine natürliche Zahl $< n$, wird mit l_2 Bits – eventuell mit führenden Nullen – binär dargestellt.

Der Geheimtextblock c lässt sich zum Entschlüsseln wieder als Zahl $c < n$ deuten und in $m = c^d \bmod n$ transformieren.

Ganz genaue Beschreibung

Siehe PKCS = 'Public Key Cryptography Standard' bei RSA – `http://www.rsasecurity.com/rsalabs/pkcs/`.

Zu beantwortende Fragen

- Wie findet man geeignete Parameter n, d, e, so dass $(\star)$ erfüllt ist?
- Wie implementiert man das Verfahren hinreichend effizient?
- Wie weist man die Sicherheit nach?

Geschwindigkeit

Siehe Vorlesung „Datenschutz und Datensicherheit“, `http://www.uni-mainz.de/~pommeren/DSVorlesung/KryptoBasis/RSA.html`