RSA: Das Verfahren

Das nach seinen Autoren Rivest, Shamir und Adleman benannte *RSA-Verfahren* ist ein asymmetrisches Verschlüsselungsverfahren, das in sehr vielen weit verbreiteten Systemen angewendet wird.

Bob (B) soll eine Nachricht an *Alice* (A) schicken.

Vorbereitungen durch Alice:

Wähle große Primzahlen p und q mit $p < q$.
(Das ist möglich, wie wir später sehen werden.)

Berechne $n = p \cdot q$.

Setze $\varphi(n) = (p-1)(q-1)$, wähle $e > 1$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$.

Berechne Zahl $s < n$ mit $e \cdot s \equiv 1 \bmod \varphi(n)$. (Benutze hierbei den Euklidischen) Algorithmus!)

Alice veröffentlicht das Paar (n, e).

RSA: Bob sendet Nachricht

Die Zahlen n und e sind also nun öffentlich bekannt.
Dagegen müssen p, q und s absolut geheim bleiben!

Bobs Nachricht an Alice muss als eine Zahl im Bereich $\{0, \ldots, n-1\}$ gewählt werden. Die Nachricht sei x.

Bob macht nun Folgendes:

Berechne $y = x^e \bmod n$. (Mit schneller Exponentiation – Folie 28.6)

Sende y über einen beliebigen Kanal zu Alice.

Alice berechnet schließlich den Wert $x' = y^s \bmod n$ und geht davon aus, dass $x = x'$ gilt, d.h. dass sie Bobs Nachricht korrekt entschlüsselt hat.

Es muss also gelten: $(x^e)^s \bmod n = x$. Das zeigen wir gleich!

RSA: Ein Beispiel

Bob möchte die Nachricht 42 an Alice senden.

Vorbereitungen durch Alice:

Wähle $p = 11$ und $q = 13$.

Es gilt $11 < 13$ und p und q sind große Primzahlen!

Berechne $n = 11 \cdot 13 = 143$.

Setze $\varphi(n) = (11 - 1)(13 - 1) = 120$ und wähle $e > 1$.

1. Versuch: $e = 21$, es folgt aber $\mathrm{ggT}(21, 120) = 3$.
2. Versuch: $e = 7$, nun gilt $\mathrm{ggT}(7, 120) = 1$.

Mit Euklids Algorithmus erhalten wir $s = 103$, denn

$7 \cdot 103 = 721 \equiv 1 \bmod 120$

RSA-Beispiel (Fortsetzung)

Alice veröffentlicht das Paar $(143, 7)$.

Bob verschlüsselt die Nachricht 42 durch 42^7 mod 143:

$$42 \cdot 42 = 1764 \equiv 334 \equiv 48 \bmod 143$$
$$48 \cdot 48 = 2304 \equiv 874 \equiv 16 \bmod 143$$
$$42^7 \equiv 16 \cdot 48 \cdot 42 = 48 \cdot 672 \equiv 48 \cdot 100 = 4800 \equiv 510 \equiv 81$$

Bob sendet die verschlüsselte Nachricht 81 an Alice.

Alice berechnet y^s mod 143:

$$81^{103} = 3^{412} = 3^{27 \cdot 15} \cdot 3^7 = (3^{15})^{27} \cdot 9 \cdot 243 \equiv 9 \cdot 100 = 900 = 6 \cdot 143 + 42 \equiv 42$$

Es wurde benutzt, dass $3^{15} = (3^5)^3 = 243^3 \equiv 100^3 = 1000^2 \equiv (-1)^2 = 1 \bmod 143$.

Also hat Alice den Wert 42 korrekt berechnet.

RSA: Korrektheit

Wir müssen zeigen, dass $(x^e)^s \equiv x \bmod n$ gilt.

Da p und q teilerfremd sind, genügt es zu zeigen,
dass $(x^e)^s \equiv x \bmod p$ und $(x^e)^s \equiv x \bmod q$ gilt.

Beide Behauptungen sind nach dem selben Muster zu beweisen.
Es genügt also, die Behauptung modulo p zu prüfen:

Falls x durch p teilbar ist, gilt $(x^e)^s \equiv 0 \bmod p$, aber auch $x \equiv 0 \bmod p$.

Wenn aber x nicht durch p teilbar ist, haben wir $\mathrm{ggT}(x, p) = 1$, und folglich nach Fermats kleinem Satz $x^{p-1} \equiv 1 \bmod p$. Damit folgt:

$$(x^e)^s = x^{es} = x^{1+k(p-1)(q-1)} =$$
$$x \cdot (x^{p-1})^{k(q-1)} \equiv x \cdot 1^{k(q-1)} \equiv x \bmod p$$

Korrektheit (Forts.)

Wir haben gesehen, dass $(x^e)^s \equiv x \bmod p$ gilt.

Auf die gleiche Weise erhalten wir auch $(x^e)^s \equiv x \bmod q$.

Da p und q teilerfremd sind, erhalten wir mit $n = pq$:

$$(x^e)^s \equiv x \bmod n.$$

Damit ist die Korrektheit der Entschlüsselung nachgewiesen.