(ein bisschen)
Hintergrundwissen RSA

1: Teilen mit Rest

Klar, oder?

10 / 4 = 2 Rest 2
8 / 7 = 1 Rest 1

2: Modulo-Operationen

"Restklassen"

$10 \equiv 2 \pmod 4$
$8 \equiv 1 \pmod 7$

3: größter gemeinsamer Teiler (ggT)

ggT(a,b) > 0 ist Teiler von a und von b,
mit: jeder andere Teiler von a und b
ist auch Teiler von ggT(a,b)

4: Euler-Phi-Funktion

(Anzahl der Zahlen, die relativ prim zu n sind)

$\Phi(n) := |\{ m < n: ggT(m,n) = 1 \}|$

5: Satz von Euler-Fermat

(Wichtige Eigenschaft von Φ)

ggT(a,b) = 1 $\Longrightarrow$ a^Φ(b) ≡ 1 (mod b)

Schließlich:

- $\Phi(p) = p-1$
- $\Phi(pq) = (p-1)(q-1)$
- $ggT(a,pq) = p$

  $\Longrightarrow a^{\Phi(pq)} \equiv 1 \pmod{pq}$

Der RSA-Algorithmus

Alice möchte Bob eine Nachricht schicken.

Dazu braucht sie:
Bobs öffentlichen Schlüssel.

Bob braucht zum Entschlüsseln seinen privaten Schlüssel.

Schlüsselpaar

Bob sucht sich 2 (große) Primzahlen p und q,
damit m := pq, sowie
eine weitere Zahl e mit ggT(e,m)=1
(üblicherweise auch eine nicht zu kleine Primzahl).

Da Bob p und q bekannt sind, kann er mit Hilfe des Euklidischen Algorithmus die "arithmetische Inverse" (mod $\Phi(m)$) d ausrechnen, d.h.

$ed \equiv 1 \pmod{\Phi(m)}$

Damit:
Öffentlicher "Schlüssel": (e,m)
Privater "Schlüssel": (d,m)

Klartext K
(muss < m sein, sollte dringend > 1 sein)
Alice berechnet
$C = K^{e} \pmod{m}$
(das geht effizient mit dem
binären Exponential-Algorithmus)

Bob empfängt C.
Er berechnet
$C^d = (K^e)^d$
$= K^{de} \equiv K^{(\Phi(m)+1)} \pmod m$

Aus Euler-Fermat folgt:

$K^{\Phi(m)+1} \equiv K \pmod{m}$

(zumindest falls ggT(K,m)=1.
Falls ggT(K,m)=p gilt das trotzdem,
Hausaufgabe!)

Weitere Anwendung:

Signatur (quasi "umgekehrt", d.h.
Alice veschlüsselt die Signatur mit Ihrem privaten Schlüssel, Bob empfängt die Signatur und kann Sie mit öffentlichen Schlüssel von Alice dekodieren).

Fazit

Die Sicherheit des Algorithmus beruht darauf, dass nur dem Besitzer des Geheimen Schlüssels die Primfaktorzerlegung von m (bzw. das arithmetische Inverse d) bekannt sind, und sich diese Information praktisch nicht einfach aus m ergibt (theoretisch natürlich schon, sogar sehr einfach. Nur eben nicht in kurzer Zeit).