LU06g - RSA-Verfahren im Detail

Siehe auch http://de.wikipedia.org/wiki/RSA-Kryptosystem

Entstehung

Whitfield Diffie und Martin Hellman hatten in den 1970er Jahren eine Theorie zur Public-Key-Krytographie veröffentlicht. Die drei Mathematiker Rivest, Shamir und Adleman versuchten diese Theorie zu widerlegen. Dabei stiessen sie auf ein Verfahren, bei dem sie keine Angriffspunkte fanden.

Aus diesem Verfahren entstand 1977 RSA, das erste veröffentlichte Verschlüsselungsverfahren.

Funktionsweise

RSA basiert auf einem privaten Schlüssel (private key) und einem öffentlichen Schlüssel (public key). Beide Schlüssel bestehen aus jeweils zwei Zahlen, die mit den Variablen `d`, `e` und `N` bezeichnet werden:

- Der public key besteht aus `e` und `N`
- Der private key besteht aus `d` und `N`
- **`N`** ist bei beiden Schlüsseln gleich und wird `RSA-Modul` genannt.

Um die Schlüssel zu berechnen, geht man wie folgt vor:

1. Wähle zwei unabhängige, unterschiedliche Primzahlen `p` und `q`.
   - Zum Beispiel: `p = 11` und `q = 13`
2. Berechne das RSA-Modul: `N = p * q`.
   - N = 11 * 13 = 143
3. Berechne die Eulersche ϕ-Funktion von `N`: `ϕ(N) = (p-1) * (q-1)`
   - ϕ(N) = 10 * 12 = 120
4. Wähle eine Zahl `e` die keinen gemeinsamen Teiler mit `ϕ(N)` hat. Man bezeichnet dies als teilerfremd
   - e = 23
5. Berechne die Zahl `d` mit Hilfe des erweiterten euklidischen Algorithmus anhand der Formel `e * d + k * ϕ(N) = 1`.
   - 23 * 47 + (-9) * 120 = 1

Somit erhalten wir den private key (47, 143) und den public key (23, 143).

Verschlüsseln

Der Absender möchte die Klartext-Nachricht `t` verschlüsseln und dabei den Chiffre-Text `c` erhalten. Er berechnet $c = (t^e) \bmod N$

Beispiel

Der Absender möchte die Zahl 7 verschlüsselt senden.

- Der public key ist (e=23, N=143)
- $c = (7^{23}) \bmod 143 = 2$

Entschlüsseln

Der Empfänger erhält den Chiffre-Text c und möchte den Klartext t erhalten. Er berechnet $t = (c^{d}) \bmod N$.

Beispiel

Der Empfänger erhält den Chiffre-Text 2.

- Der private key ist (d=47, N=143)
- $t = (2^{47}) \bmod 143 = 7$