Beispiel RSA

7. November 2016

Im ersten Schritt führen wir das RSA-Setup durch und geben kleine RSA-Parameter an.

Öffentlicher Schlüssel

Für die Primzahlen p und q wählen wir $p = 11$ und $q = 17$.
Hieraus ergibt sich die RSA-Zahl $n = p \cdot q = 11 \cdot 17 = 187$. Nun müssen wir den öffentlichen Verschlüsselungsexponenten e bestimmen.

Hierbei gilt die Voraussetzung $1 < e < \varphi(n)$ mit $\varphi(n) = (p-1)(q-1)$.

Der öffentliche Exponent muss teilerfremd zu $\varphi(n)$ sein, d.h. $ggT(e, \varphi(n)) = 1$ erfüllen.

Um diese Bedingungen prüfen zu können, geben wir die Primfaktorisierung von $\varphi(n)$ an:

$$\varphi(n) = (11-1) \cdot (17-1) = 10 \cdot 16 = 2^5 \cdot 5. \tag{1}$$

Für $e = 3$, $e = 7$, $e = 9$ usw. ist die Bedingung erfüllt. Wir wählen $e = 7$.
Damit ist die Erstellung des öffentlichen Schlüssels (n, e) abgeschlossen.

Privater Schlüssel

Als nächstes muss der private Exponent d berechnet werden. Dieser erfüllt nach Gleichung **??** die Kongruenz

$$7 \cdot d \equiv 1 \bmod 160. \tag{2}$$

In der Praxis verwendet man zur Berechnung von d den *erweiterten Euklidischen Algorithmus*.

Dieser liefert $d = 23$. Wir prüfen das nach und erhalten

$$7 \cdot 23 = 161 \equiv 1 \bmod 160. \tag{3}$$

Damit erhalten wir für das Schlüsselpaar:

- Public Key: $(n, e) = (187, 7)$.

- Private Key $(p, q, d) = (11, 17, 23)$.

Nachdem der öffentliche Schlüssel $(187, 7)$ an den Sender der Nachricht übertragen wurde, verschlüsselt dieser die Nachricht $m = kryptographie$.

Jedes Klartextzeichen stellt er entsprechend der folgenden Tabelle als eine Zahl dar:

a	3	h	10	o	17	v	24
b	4	i	11	p	18	w	25
c	5	j	12	q	19	x	26
d	6	k	13	r	20	y	27
e	7	l	14	s	21	z	28
f	8	m	15	t	22		
g	9	n	16	u	23		

Der mittels Dezimalzahlen kodierte Klartext lautet dann

$$m_{dec} = 13202718221792031810117. \tag{4}$$

Der Sender verschlüsselt jedes Zeichen mittels der RSA-Verschlüsselung $c_i = m_i^e \bmod n$.

Für den Klartextbuchstaben k ergibt sich beispielsweise das Geheimtextzeichen

$$c_0 \equiv 13^7 = 13^1 \cdot 13^2 \cdot 13^4 \equiv 106 \bmod 187. \tag{5}$$

Der resultierende Geheimtext lautet

$$c = 106147124171448570147130171175881 82. \tag{6}$$

Für die Entschlüsselung der Nachricht wird für jedes Zeichen $m_i \equiv c_i^d \bmod n$ berechnet.