RSA - Verfahren

Arno Fehringer , Mai 2017

Quellen:

Dobrowolski, Manfred : Mathematische Exkursionen: Gödel, Escher und andere Spiele Oldenbourg Verlag , München, 2010

Padberg, Friedhelm : Elementare Zahlentheorie, Spektrum Akademischer Verlag , 2. Aufl. 1990

Fehringer, Arno : Grundlegendes zur Zahlentheorie (AF) , 2012 , pdf-Dokument download bei URL: http://mathematikgarten.npage.de/ [08.05.2017]

Fehringer, Arno : Endliche und periodische Dezimalbrüche (AF) , 2017, pdf-Dokument download bei URL: http://mathematikgarten.npage.de/ [08.05.2017]

Die RSA - Verschlüsselung beruht wesentlich auf folgenden zahlentheoretischen Sätzen :

1. Der größte gemeinsame Teiler $(a;b)$ zweier Zahlen a , $b \in \mathbb{N}$ kann über den Euklidischen Algorithmus gefunden werden nebst einer entsprechenden Darstellung in der Form

   $$h \cdot a + i \cdot b = (a;b) \quad ,$$

   wobei die Zahlen h , $i \in \mathbb{Z}$ eindeutig bestimmt sind .

2. **Satz von Euler**

   $(m;n) = 1 \quad \Rightarrow \quad m^{\varphi(n)} \equiv 1 \mod n$.

   Die Funktion $\varphi(n)$ ist gleich der Anzahl der zu n teilerfremden vorhergehenden Zahlen .

   Wenn speziell $n = pq$, p , $q \in \mathbb{P}$ ist, folgt $\varphi(n) = (p-1)(q-1)$.

Die RSA - Verschlüsselung

Empfänger

Der Empfänger wählt Primzahlen $p , q \in IP$ mit jeweils mehren Hundert Stellen und bildet die Zahl

$n := pq$.

Dann ist $\varphi(n) = (p-1)(q-1)$.

Er wählt er eine weitere Primzahl $r \in IP$

mit $\max(p,q) < r < \varphi(n)$, $r \nmid p-1$, $r \nmid q-1$,

also $r \nmid \varphi(n)$ und $(\varphi(n);r) = 1$

Der Euklidischer Algorithmus liefert eindeutige Zahlen $h , i \in \mathbb{N}$ mit

$h \cdot \varphi(n) + i \cdot r = 1$

$i \cdot r = h \cdot \varphi(n) + 1$

$i \cdot r \equiv 1 \mod \varphi(n)$

Öffentlich bekannt sind die Zahlen n , r .

Geheim bzw. nur dem Empfänger bekannt ist die Zahl i .

Sender

Der Sender möchte die Zahl m senden und **verschlüsselt** sie über

$c \equiv m^r \mod n$

Empfänger

Der Empfänger **entschlüsselt** die übermittelte Zahl c durch c^i bzw.

$c^i \equiv m \mod n$

Beweis für die korrekte Entschlüsselung von c **zu** m **:**

$$c^i \equiv \left(m^r\right)^i \quad \text{mod } n$$
$$c^i \equiv m^{i \cdot r} \quad \text{mod } n$$

$$i \cdot r = h \cdot \varphi(n) + 1$$

$$c^i \equiv m^{h \cdot \varphi(n) + 1} \quad \text{mod } n$$
$$c^i \equiv m^{h \cdot \varphi(n)} \cdot m \quad \text{mod } n$$
$$c^i \equiv \left(m^{\varphi(n)}\right)^h \cdot m \quad \text{mod } n$$

Satz von Euler :

$$m^{\varphi(n)} \equiv 1 \quad \text{mod } n \quad , \quad (m;n) = 1$$
$$\left(m^{\varphi(n)}\right)^h \equiv 1 \quad \text{mod } n$$

$$c^i \equiv 1 \cdot m \quad \text{mod } n$$
$$c^i \equiv m \quad \text{mod } n$$

q.e.d.

Einfaches Beispiel für die RSA - Verschlüsselung

Empfänger

$p=11 \quad , \quad q=13$

$n = 143$

$\varphi(143) = 120 \quad .$

$r=23$

$120 = 5 \cdot 23 + 5$

$23 = 4 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$(120;23) = 1$

Allgemein

$a_1 = v_2 \cdot a_2 + a_3 \qquad \Rightarrow \qquad a_3 = -v_2 \cdot a_2 + a_1$

$a_2 = v_3 \cdot a_3 + a_4 \qquad \Rightarrow \qquad a_4 = -v_3 \cdot a_3 + a_2$

$a_3 = v_4 \cdot a_4 + a_5 \qquad \Rightarrow \qquad a_5 = -v_4 \cdot a_4 + a_3$

$a_4 = v_5 \cdot a_5 + a_6 \qquad \Rightarrow \qquad a_6 = -v_5 \cdot a_5 + a_4$

$a_5 = v_6 \cdot a_6 + 0$

$a_6 = -v_5 \cdot a_5 + a_4$

$a_6 = -v_5 \cdot (-v_4 \cdot a_4 + a_3) + a_4$

$a_6 = (v_5 v_4 + 1) a_4 - v_5 a_3$

$a_6 = (v_5 v_4 + 1)(-v_3 \cdot a_3 + a_2) - v_5 a_3$

$a_6 = -(v_5 v_4 + 1) v_3 \cdot a_3 + (v_5 v_4 + 1) a_2 - v_5 a_3$

$a_6 = -((v_5 v_4 + 1) v_3 + v_5) \cdot a_3 + (v_5 v_4 + 1) a_2$

$a_6 = ((v_5 v_4 + 1) v_3 + v_5) v_2 \cdot a_2 - ((v_5 v_4 + 1) v_3 + v_5) a_1 + (v_5 v_4 + 1) a_2$

$a_6 = - ((v_5 v_4 + 1) v_3 + v_5) a_1 + (((v_5 v_4 + 1) v_3 + v_5) v_2 + (v_5 v_4 + 1)) a_2$

Mit $v_5 = 1$, $v_4 = 1$, $v_3 = 4$, $v_2 = 5$ folgt

$$a_6 = -\left(\left(v_5 v_4 + 1\right) v_3 + v_5\right) a_1 + \left(\left(\left(v_5 v_4 + 1\right) v_3 + v_5\right) v_2 + \left(v_5 v_4 + 1\right)\right) a_2$$

$$a_6 = -9 \cdot a_1 + 47 \cdot a_2$$

Mit $a_6 = (120;23) = 1$, $a_1 = 120$, $a_2 = 23$ folgt

$$1 = -9 \cdot 120 + 47 \cdot 23$$

$$47 \cdot 23 = -9 \cdot 120 + 1$$

$$47 \cdot 23 \equiv 1 \mod 120$$

$$i = 47$$

Öffentlich bekannt sind die Zahlen $n = 143$, $r = 23$

Geheim bzw. nur dem Empfänger bekannt ist die Zahl $i = 47$.

Sender

Der Sender möchte die Zahl $m = 7$ senden und **verschlüsselt** sie über

$$c = m^r \equiv 7^{23} \mod 143$$

$$7 \equiv 7 \mod 143$$

$$7^2 \equiv 49$$

$$7^3 \equiv 49 \cdot 7 \equiv 57$$

$$7^4 \equiv 57 \cdot 7 \equiv 113$$

$$7^5 \equiv 113 \cdot 7 \equiv 76$$

$$7^6 \equiv 76 \cdot 7 \equiv 103$$

$$7^7 \equiv 103 \cdot 7 \equiv 6$$

$$7^{21} \equiv 6 \cdot 6 \cdot 6 \equiv 73$$

$$7^{22} \equiv 73 \cdot 7 \equiv 82$$

$$7^{23} \equiv 82 \cdot 7 \equiv 2$$

$$c \equiv 2 \mod 143$$

$$c = 2$$

Empfänger

Der Empfänger **entschlüsselt** c nach m durch

$m \equiv c^i \mod n$

$m \equiv 2^{47} \mod 143$

$2^8 \equiv 256 \equiv 113 \mod 143$

$2^9 \equiv 113 \cdot 2 \equiv 83$

$2^{10} \equiv 83 \cdot 2 \equiv 23$

$2^{20} \equiv 23 \cdot 23 \equiv 100$

$2^{21} \equiv 100 \cdot 2 \equiv 57$

$2^{23} \equiv 57 \cdot 2^2 \equiv 85$

$2^{46} \equiv 85 \cdot 85 \equiv 75$

$2^{47} \equiv 75 \cdot 2 \equiv 7$

$m \equiv 7 \mod 143$

$m = 7$