

Der RSA - Algorithmus

Inhalt

- Einführung
- Schlüsselerzeugung
- Verschlüsseln
- Entschlüsseln

Einführung

In diesem Tutorial möchte ich euch etwas über den RSA Algorithmus berichten. Wenn ihr wenig, oder gar keine Ahnung von der Kryptographie habt, empfehle ich euch zuerst andere Kryptographietuts zu lesen, in denen einige Grundlagen erläutert sind.

Der RSA Algorithmus ist nach seinen Erfindern benannt: Ron **R**ivest, Adi **S**hamir und Len **A**dleman.

Der RSA Algorithmus war das erste Public Key Verfahren und ist bis heute noch das wichtigste.

Die Schwierigkeit der Entschlüsselung des RSA-Algorithmus beruht darauf, dass es sehr schwierig ist 2 grosse Primzahlen zu faktorisieren. Im Normalfall sind die Primzahlen häufig 1024 Bit lang. Das heisst sie haben mindestens 100 Stellen.

Schlüsselerzeugung

In diesem Abschnitt möchte ich erläutern, wie man seinen privaten, und seinen öffentlichen Schlüssel erzeugt. Die Schlüsselerzeugung läuft in 4 Schritten ab:

1. Man wählt 2 Primzahlen: **p** und **q**

2. Man bildet das Produkt dieser Primzahlen: **n = p * q**

3. Man wählt eine Zahl **e**, die grösser ist als 1, kleiner als **n** und keine gemeinsamen Faktoren mit dem Produkt **(p - 1) * (q - 1)** hat. Ausserdem muss

gcd(e, (p-1)*(q-1)) = 1 sein und **e** muss ungerade sein. (gcd = greatest common divisor = Grösster gemeinsamer Teiler)

4. Man berechnet eine Zahl **d**, die grösser ist als 1 und kleiner ist als **(p-1)*(q-1)** und **d * e = 1 mod (p - 1) * (q - 1)**. Diese Zahl kann mit dem erweiterten euklidischen Algorithmus berechnet werden. Oder man versucht eine Zahl **x** zu finden, für die gilt: **d = (x(p-1)(q-1)+1)/e** ist ein ganzzahliges Ergebnis. Diese Zahl ist durch probieren herauszufinden..

Nun haben wir zwei Primzahlen **p** und **q**, das Produkt **n**, die Zahl **e** und die Zahl **d**. Das Paar **(n,e)** bildet den **öffentlichen Schlüssel** und **d** den **privaten Schlüssel**. Man nennt die Zahl

n : RSA - Modul,

e : Verschlüsselungsexponent

d : Entschlüsselungsexponent.

Damit haben wir unsere Schlüssel erzeugt und können uns der Verschlüsselung widmen. Aber zuvor zur Veranschaulichung noch ein Beispiel:

1. Man wählt 2 Primzahlen : **p = 11** und **q = 23**

2. Das Produkt **n** ist dann : **253**

3. Die Rechnung **(p-1)*(q-1)** ergibt: **10 * 22 = 220**. In **Primfaktoren** zerlegt ist diese Zahl:

4 * 5 * 11. Das einfachste **e** das wir wählen können ist **e=3**. **e** erfüllt auch die bedingung dass: **gcd(e,(p-1)*(q-1)) = 1** ist.

4. Nun brauchen wir die Zahl **d** mit **d = (x(p-1)(q-1)+1)/e** oder **d*e = 1 mod (p - 1)*(q - 1)**. Wir berechnen **d** und kommen auf:

d = 147

Fassen wir nun unsere Zahlen einmal zusammen:

p = 11

q = 23

n = 253

e = 3

d = 147

Der öffentliche Schlüssel ist: **(253 , 3)**

Jeder der diesen Schlüssel kennt kann Nachrichten verschlüsseln.

Der private Schlüssel lautet : **d = 147**

Somit können wir nun zur Verschlüsselung kommen.

Verschlüsselung

Im folgenden steht

c für Chiffre

m für Klartext

N für die Länge eines angenommen Alphabets

k für die Blocklänge

Einen Klartext verschlüsselt man folgendermaßen:

$$c = m^e \bmod n$$

Wir erstellen uns nun ein Alphabet der Länge **N**. Wie nehmen:

0	a	b	c
0	1	2	3

Diese Alphabet hat die Länge **N = 4**. Wir berechnen $k = \log_4 253 = 3$. Die Zahl **k=3** ist unsere Klartextblocklänge.

Wir werden nun den Klartextblock "**abb**" verschlüsseln. Aus unserer Alphabetstabelle entnehmen wir das "**abb**" der Zahl **122** entspricht.

$$\text{Nun können wir } m \text{ berechnen: } m = 1 * 4^2 + 2 * 4^1 + 2 * 4^0 = 26$$

$$\text{Daraus folgt } c = 26^3 \bmod 253 = 119.$$

Die Zahl müssen wir nun zur Basis **N = 4** schreiben. Die Quadratzahlen von 4 lauten:

$$1 ; 4 ; 16 ; 64$$

$$\text{Wir teilen nun } 119 \text{ durch } 64: 119/64 = 1 \text{ Rest } 55$$

$$\text{Nun teilen wir } 55 \text{ durch } 16: 55/16 = 3 \text{ Rest } 7$$

$$\text{Nun teilen wir } 7 \text{ durch } 4: 7/4 = 1 \text{ Rest } 3$$

$$\text{Schliesslich teilen wir noch } 4 \text{ durch } 1 : 4/1 = 4 \text{ rest } 0$$

Die Zahl 119 lautet zur Basis 4 geschrieben also: **1313**

Wenn wir uns nun unsere Alphabetstabelle anschauen sehen wir das 1313 der Buchstaben kombination:

"**acac**" entspricht. Jeder der den Public Key " (253 ; 3) kennt kann beliebige Nachrichten verschlüsseln.

Aber nur derjenige der den privaten Schlüssel $d = 147$ kennt kann diese Nachricht auch wieder entschlüsseln

.Dies wird im nächsten Abschnitt gezeigt.

Entschlüsselung

Entschlüsselt wird nach folgender Rechnung:

$$m = c^d \bmod n$$

Auf den Beweis des Satzes werde ich hier nicht näher eingehen.

Er hängt damit zusammen das : **$e \cdot d \text{ kongruent zu } 1 \text{ mod } (p - 1)(q - 1)$** ist.

Wir werden nun als Beispiel unser im letzten Abschnitt verschlüsselten Klartext wieder entschlüsseln.

Wir hatten im letzten Abschnitt:

$$n = 253$$

$$e = 3$$

$$d = 147$$

$$c = 119$$

Wir setzten nun diese zahlen in unsere Entschlüsselungsformel ein:

$$119^{147} \text{ mod } 253 = 26$$

Tatsächlich haben wir im letzten Abschnitt **$m = 26$** berechnet.