Das RSA-Verfahren

Vorbemerkungen

Das RSA-Verfahren erzeugt einen öffentlichen und einen geheimen Schlüssel zur Ver- und Entschlüsselung von Daten. Insbesondere bei der eMail-Verschlüsselung wird das RSA-Verfahren verwendet. Es ist auch geeignet, eMails mit digitalen Unterschriften zu signieren und damit die Identität des eMail-Erstellers und die Integrität (= Unverfälschtheit) der eMail zu bestätigen.

Das RSA-Verfahren wurde 1977 von den Ronald Rivest, Adi Shamir und Leonard Adleman erfunden. Die Anfangsbuchstaben der Nachnamen gaben dem Verfahren seinen Namen.

Die folgende Beschreibung zeigt das RSA-Verfahren mit kleinen Zahlen, um das Grundprinzip verständlich zu machen. Im letzten Abschnitt dieser Beschreibung wird skizziert, an welchen Stellen unser Beispiel von dem in der Praxis angewendete Verfahren abweicht. Es kann vorkommen, dass die folgende Beschreibung zuhunster der Algemeinverständlichkeit nicht immer die mathematisch korrekten Begriffe verwendet.

Erzeugung des öffentlichen Schlüssels eines RSA-Schlüsselpaars

Nr.	Verfahrensschritt	Formel	Beispiel
(1)	Zwei Primzahlen p und q zufällig auswählen.	p ist Primzahl q ist Primzahl	p = 5 q = 11
(2)	Produkt r aus p und q bilden (r = RSA-Modul).	r = p * q	r = 55
(3)	Eulersche Phi-Funktion f bilden.	f = (p - 1) * (q - 1)	f = 4 * 10 f = 40
(4)	Suche einer zufälligen Zahl e, die folgende Eigenschaften besitzt: • e ist kleiner als f aus (3) • e ist teilerfremd zu f aus (3) 'e teilerfremd zu f' = es gibt keine Zahl außer 1, die durch e und f gleichermaßen ohne Rest teilbar wäre. Umgangssprachlich ausgedrückt: ein Bruch zweier teilerfremder Zahlen kann nicht gekürzt werden. Mathematischer Nachweis: der größte gemeinsame Teiler von e und f ist 1.	e < f e ⊥ f *Nachweis:* *ggT(e, f) = 1*	1 < e < 40 e ⊥ 40 *e: 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39*

	Wir wählen für e die Zahl 3 aus.		e = 3
(5)	**Der öffentliche Schlüssel ö besteht aus e und r.** *(die Primzahlen p und q werden nicht mehr benötigt)*	**ö: e, r**	**ö: 3, 55**

Berechnung des geheimen Schlüssels eines RSA-Schlüsselpaars

Nr.	Verfahrensschritt	Formel	Beispiel
(6)	Berechnung der Zahl d, für die gilt: (e * d) mod f = 1 *(zur Vereinfachung wird Produkt u aus e und d eingeführt; f ist aus (3) bekannt)*	u = e * d u mod f = 1	f = 40 u mod 40 = 1 *das gilt für u = 41, 81, 121, 161, usw.*
(7)	Das richtige u ist gefunden, wenn u durch e ohne Rest teilbar, also u mod e = 0	u = i * f + 1 mit i = 1, 2, 3 .. n solange bis u mod e = 0	Ergebnis: u = 2 * 40 + 1 u = 81
(8)	Aus u (siehe (6) und (7)) muss d berechnet werden.	u = e * d d = u / e	u = 81 d = 81 / 3 = 27
(9)	**Der geheime Schlüssel g besteht aus d und r.**	**g: d, r**	**g: 27, 55**

Der geheime und der öffentliche Schlüssel

"d,r" ist für uns der geheime und "e,r" der öffentliche Schlüssel. Wir hätten das auch umkehren können und "e,r" zum geheimen und "d,r" zum öffentlichen Schlüssel erklären können. Es ist also keine Eigenschaft des Schlüssels 'öffentlich' oder 'geheim' zu sein, sondern eine willkürliche Festlegung.

Wichtig ist nur, dass der geheime Schlüssel auch tatsächlich **immer** geheim bleibt, also nur der Schlüsselerzeuger den geheimen Schlüssel kennt.

Verschlüsseln

Nr.	Verfahrensschritt	Formel	Beispiel
(10)	Mit dem RSA-Verfahren können nur Zahlen verschlüsselt werden. Jedes Zeichen x ist also in eine Zahl y umzuwandeln. Die zu verschlüsselnde Zahl y muss kleiner sein als das RSA-Modul r. r ist Teil des öffentlichen und geheimen Schlüssels. r bestimmt also den Umfang des Zeichencodes.	x ⇒ y 0 ≤ y ≤ (r-1)	r = 55 0 ≤ y ≤ 54

(11)	Wir wollen das zu verschlüsselnde Zeichen x (z.B. den Buchstaben 'D') verschlüsseln. Zum Umwandeln in eine Zahl y nehmen wir einfach die Positionsnummer im Alphabet: 'D' steht an vierter Stelle des Alphabets; wir wandeln also 'D' in 4 um.	x ⇒ y	x = 'D' y = 4
(12)	Die Verschlüsselung verwendet den öffentlichen Schlüssel ö (siehe (5)) bestehend aus e und r. Die zu verschlüsselnde Zahl y wird mit e potenziert. Der verbleibende Rest aus der Division mit r ist die verschlüsselte Zahl z.	z = y ** e mod r *y, e und r sind bekannt.*	y = 4 e = 3 r = 55 z = 4**3 mod 55 z = 64 mod 55 z = 9
(13)	**Zusammenfassung:** Den Buchstaben 'D' haben wir in die Zahl 4 umgewandelt. Die Verschlüsselungsformel verschlüsselt 4 in 9.	**x ⇒ y ⇒ z**	**'D' ⇒ 4 ⇒ 9**

Exkurs: Methode des fortgesetzten Quadrierens (Exkurs)

Bei der Verschlüsselung und später bei der Entschlüsselung wird in der Regel mit hohen Exponenten potenziert (Verschlüsselung siehe (12)).
Dabei entstehen sehr sehr große Zahlen, die nur schwer zu berechnen sind. Die Methode des fortgesetzten Quadierens (= Potenzieren mit dem Exponenten 2) hilft, die Potenzen zu berechnen.
Aus Vereinfachungsgründen wählen wir ein Beispiel mit einem kleinen Exponenten:

7 ** 4 = 2.401

Der Exponent 4 kann im Beispiel auch durch 2 ** 2 gebildet werden:

7 ** 4 = (7 ** 2) ** 2 = 49 ** 2 = 2.401

Lässt sich der Exponent nicht durch 2-er-Exponenten ausdrücken, kann durch die Multiplikation mit der Basis ergänzt werden:

7 ** 5 = ((7 ** 2) ** 2) * 7 = 16.807

Das fortgesetzte Quadrieren erleichtert das Potenzieren mit großen Exponenten. Als Ergebnis entsteht wie beim "normalen" Potenzieren letztlich eine große Zahl, die schwer zu handhaben ist.
Bei der Ver- und Entschlüsselung wird aber nicht die große Zahl selbst, sondern immer nur der Rest aus einer Division benötigt. Diese Modulo-Berechnung kann auch auf die Teilergebnisse des fortgesetzten Quadrierens angewendet werden:

7 ** 5 mod 3 = 16.807 mod 3 = 5602 * 3 Rest 1

Die Formel unter Anwendung des fortgesetzten Quadrierens:

7 ** 5 mod 3 = (((7 ** 2) ** 2) * 7) mod 3

Bei der Division mit Rest kann die Division mit Rest auf die Teilergebnisse des fortgesetzten Quadrierens statt auf das Endergebnis angewendet werden (die Teilergebnisse werden der Übersicht halber in geschweiften statt in runden Klammern gesetzt):

(((7 ** 2) ** 2) * 7) mod 3
= (((((7 ** 2) mod 3) ** 2) mod 3) * 7) mod 3
= ((((49 mod 3) ** 2) mod 3) * 7) mod 3
= (((1 ** 2) mod 3) * 7) mod 3
= ((1 mod 3) * 7) mod 3
= (1 * 7) mod 3
= 7 mod 3
= 1

Die Teilergebnisse können nie größer als das Quadrat der Basis sein, so dass die Division mit Rest auch bei sehr großen Exponenten leicht zu berechnen ist.

Entschlüsseln

Nr.	Verfahrensschritt	Formel	Beispiel
(14)	Die Verschlüsselung verwendet den geheimen Schlüssel g (siehe (9)) bestehend aus d und r. Die zu entschlüsselnde Zahl z (siehe (13)) wird mit d potenziert. Der verbleibende Rest aus der Division mit r ist die entschlüsselte Zahl y. Für hohe Potenzen (z ** d) setzen wird das fortgesetzte Quadrieren ein.	y = z ** d mod r *z, d und r sind bekannt.*	z = 9 d = 27 r = 55 y = 9**27 mod 55 y = 4
(15)	**Zusammenfassung:** Die verschlüsselte Zahl '9' haben wir mit dem Ergebnis '4' entschlüsselt. Der vierte Buchstaben im Alphabet (siehe (11)) ist das 'D'.	**z ⇒ y ⇒ x**	**9 ⇒ 4 ⇒ 'D'**

Signieren und Verifizieren

Neben dem Ver- und Entschlüsseln von Mails können wir mit dem geheimen und dem öffentlichen Schlüssel auch Mails signieren (also digital unterschreiben) und verifizieren (also die Unterschrift überprüfen).

Beim Signieren wird ein Hashwert (also ein digitaler Fingerabrduck) der Mail berechnet. Dieser Hashwert wird mit dem **geheimen Schlüssel des Absenders** verschlüsselt und zum Empfänger gesendet.

Der Empfänger entschlüsselt den verschlüsselten Hashwert mit dem **öffentlichen Schlüssel des Absenders**. Anschließend bildet er mit der selben Hashwert-Berechnungsmethode einen eigenen Hashwert der Mail und vergleicht den entschlüsselten Hashwert mit seinem eigenen Hashwert. Stimmen beide überein, ist die Mail unverändert übertragen worden und der Absender hat seine Identität bestätigt, weil nämlich nur er in der Lage war, den Hashwert passend zu seinem öffentlichen Schlüssel mit seinem geheimen Schlüssel zu verschlüsseln.

Das Signieren und Verfizieren wird also mit den selben Berechnungsverfahren durchgeführt wie das Verschlüsseln und das Entschlüsseln. Sie unterscheiden sich nur dadurch, wann und von wem die geheimen und die öffentlichen Schlüssel zum Einsatz kommen. Das Dokument **'Signieren und Verifizieren'** beschreibt den Vorgang detaillierter.

RSA in der Praxis

Das Berechnungsverfahren für den geheimen und den öffentlichen Schlüssel erweckt so wie oben dargestellt den Eindruck, nicht besonders sicher zu sein, denn von den drei relevanten Werten e, d und r sind e und r als öffentlicher Schlüssel bekannt.

Es muss eigentlich nur noch d ermittelt werden, um auch an den geheimen Schlüssel zu kommen. Wenn die beiden Primzahlen p und q, die das Produkt r ($r = p * q$) bilden, ermittelt werden könnten, wären alle Schlüsselbestandteile des RSA-Verschlüsselungsverfahrens bekannt.

In unserem Beispiel war $r = 55$; r ist 2 Dezimalstellen lang. Es wäre einfach gewesen, durch Versuch und Irrtum zwei Primzahlen zu finden, die als Produkt 55 ergeben. In der Praxis werden Schlüssellängen von aktuell 2^{2048} bit verwendet: das sind $2048 * \log_{10}(2) \leq 617$ Dezimalstellen.

Wir können davon ausgehen, dass die beiden Primzahlen bis zu 300 Dezimalstellen lang sein können, da sie in etwa die gleiche Größenordnung haben und nicht zu eng beieinander liegen sollten. Nach dem heutigen Stand der Technik würden mit sehr großem Rechnereinsatz immer noch mehrere Jahre vergehen, bis die richtigen Primzahlen gefunden wären.

Das oben dargestellte RSA-Verfahren wäre durch andere mathematische Verfahren trotzdem leicht zu knacken, so dass es in dieser originären Form in der Praxis nicht zum Einsatz kommt. So werden beispielsweise nicht nur einzelne Zeichen verschlüsselt, sondern lange Zeichenketten. Das RSA-Verfahren verlangt dabei, dass die Bitlänge dieser Zeichenketten kürzer als die Bitlänge des Schlüsselbestandteils r ist.

Um das Entschlüsseln durch Versuch und Irrtum weiter zu erschweren, werden zusätzlich in den Zeichenketten nutzlose zufällige andere Füllzeichen eingebaut, die den Eindruck erwecken, Nutzzeichen zu sein (das so genannte Padding).

Das RSA-Verfahren ist ein langsames Verschlüsselungsverfahren. Es wird daher häufig in Kombination mit schnelleren symmetrischen Verschlüsselungsverfahren verwendet. Dabei wird z.B. nur der ad-hoc gebildetete symmetrische Schlüssel durch das RSA-Verfahren asymmetrisch verschlüsselt.

Ein detailliertes Verständnis aktueller Verschlüsselungsverfahren setzt umfassende Mathematikkenntnisse voraus. Die Weiterentwicklung der Krypthographie wird weltweit öffentlich vorangetrieben, so dass der "Normalbürger" davon ausgehen darf, dass die aktuellen Verfahren sicher sind bzw. Lücken schnell erkannt und geschlossen werden.

Weiterführende Links

- **https://de.wikipedia.org/wiki/RSA-Kryptosystem**