WIKIPEDIA

RSA-Kryptosystem

RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann.[1] Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

Inhaltsverzeichnis

Geschichte

Nachdem Whitfield Diffie und Martin Hellman im Jahr 1976 eine Theorie zur Public-Key-Kryptografie veröffentlicht hatten[2], versuchten die drei Mathematiker Rivest, Shamir und Adleman am MIT, die Annahmen von Diffie und Hellman zu widerlegen. Nachdem sie den Beweis bei verschiedenen Verfahren durchführen konnten, stießen sie schließlich auf eines, bei dem sie keinerlei Angriffspunkte fanden. Hieraus entstand 1977 *RSA*, das erste veröffentlichte asymmetrische Verschlüsselungsverfahren. Der Name RSA steht für die Anfangsbuchstaben ihrer Familiennamen.

Bereits Anfang der 1970er Jahre war in den britischen GCHQ von Ellis, Cocks und Williamson ein ähnliches asymmetrisches Verfahren entwickelt worden, welches aber keine große praktische Bedeutung erlangte und aus Geheimhaltungsgründen nicht wissenschaftlich publiziert wurde.[3] RSA konnte daher 1983 zum Patent angemeldet werden[4], obgleich es nicht das erste Verfahren dieser Art war. Das Patent erlosch am 21. September 2000.

Verfahren

Das Verfahren ist mit dem Rabin-Verschlüsselungsverfahren verwandt. Da es deterministisch arbeitet, ist es anfällig für einfache Angriffe. In der Praxis wird RSA daher mit dem Optimal Asymmetric Encryption Padding kombiniert.

Einwegfunktionen

→ *Hauptartikel: Einwegfunktion*

Funktionen, bei denen eine Richtung leicht, die andere (Umkehrfunktion) schwierig zu berechnen ist, bezeichnet man als *Einwegfunktionen* (engl. *one-way function*). Beispielsweise ist nach aktuellem Wissensstand die Faktorisierung einer großen Zahl, also ihre Zerlegung in ihre Primfaktoren, sehr aufwändig, während das Erzeugen einer Zahl durch Multiplikation von Primzahlen recht einfach und schnell möglich ist. Spezielle Einwegfunktionen sind Falltürfunktionen (engl. *trapdoor one-way function*), die mit Hilfe einer Zusatzinformation auch rückwärts leicht zu berechnen sind.

Die Verschlüsselung und die Signatur mit RSA basiert auf einer Einwegpermutation mit Falltür (engl. *trapdoor one-way permutation*, kurz *TOWP*), einer Falltürfunktion, die gleichzeitig bijektiv, also eine Permutation, ist. Die Einwegeigenschaft begründet, warum die Entschlüsselung (bzw. das Signieren) ohne den geheimen Schlüssel (die Falltür) schwierig ist.

Erzeugung des öffentlichen und privaten Schlüssels

Der öffentliche Schlüssel (public key) ist ein Zahlenpaar (e, N) und der private Schlüssel (private key) ist ebenfalls ein Zahlenpaar (d, N), wobei N bei beiden Schlüsseln gleich ist. Man nennt N den *RSA-Modul*, e den *Verschlüsselungsexponenten* und d den *Entschlüsselungsexponenten*. Diese Zahlen werden durch das folgende Verfahren erzeugt:

1. Wähle zufällig und stochastisch unabhängig zwei Primzahlen $p \neq q$. Diese sollen die gleiche Größenordnung haben, aber nicht zu dicht beieinander liegen, so dass der folgende Rahmen ungefähr eingehalten wird: $0{,}1 < |\log_2 p - \log_2 q| < 30$.[5] (In der Praxis erzeugt man dazu so lange Zahlen der gewünschten Länge und führt mit diesen anschließend einen Primzahltest durch, bis man zwei Primzahlen gefunden hat.)
2. Berechne den RSA-Modul

$$N = p \cdot q$$

3. Berechne die Eulersche φ-Funktion von N

$$\varphi(N) = (p-1) \cdot (q-1)$$

4. Wähle eine zu $\varphi(N)$ teilerfremde Zahl e, für die gilt $1 < e < \varphi(N)$.
5. Berechne den Entschlüsselungsexponenten d als Multiplikatives Inverses von e bezüglich des Moduls $\varphi(N)$. Es soll also die folgende Kongruenz gelten

$$e \cdot d \equiv 1 \pmod{\varphi(N)}$$

Die Zahlen p, q und $\varphi(N)$ werden nicht mehr benötigt und können nach der Schlüsselerstellung gelöscht werden. Es ist jedoch relativ einfach, diese Werte aus e, d und N zu rekonstruieren. Aus Effizienzgründen wird e klein gewählt, üblich ist die 5. Fermat-Zahl $2^{16} + 1 = 65537$. Kleinere Werte von e können zu Angriffsmöglichkeiten führen, etwa in Form des von Johan Håstad publizierten „Broadcast"-Angriffs, bei dem der Versand einer Nachricht an mehrere Empfänger zu einer Dechiffrierung über den chinesischen Restsatz führen kann.[6] Bei Wahl eines d mit weniger als einem Viertel der Bits des RSA-Moduls kann d – sofern nicht bestimmte Zusatzbedingungen erfüllt sind – mit einem auf Kettenbrüchen aufbauenden Verfahren effizient ermittelt werden.[7]

Beispiel

1. Wir wählen $p = 11$ und $q = 13$ für die beiden Primzahlen.
2. Der RSA-Modul ist $N = p \cdot q = 143$.
3. Die eulersche φ-Funktion nimmt damit den Wert $\varphi(N) = \varphi(143) = (p-1)(q-1) = 120$ an.
4. Die Zahl e muss zu 120 teilerfremd sein. Wir wählen $e = 23$. Damit bilden $e = 23$ und $N = 143$ den öffentlichen Schlüssel.
5. Berechnung der Inversen zu e bezüglich $\mod \varphi(N)$:
   Es gilt: $e \cdot d + k \cdot \varphi(N) = 1 = ggT(e, \varphi(N))$
   bzw. im konkreten Beispiel: $23 \cdot d + k \cdot 120 = 1 = ggT(23, 120)$. Mit dem erweiterten euklidischen Algorithmus berechnet man nun die Faktoren $d = 47$ und $k = -9$, so dass die Gleichung aus dem Beispiel wie folgt aussieht: $23 \cdot 47 + (-9) \cdot 120 = 1$
   d ist der geheime Entschlüsselungsexponent, während k nicht weiter benötigt wird.

Verschlüsseln von Nachrichten

Um eine Nachricht m zu verschlüsseln, verwendet der Absender die Formel

$$c \equiv m^e \pmod{N}$$

und erhält so aus der Nachricht m den Geheimtext c. Die Zahl m muss dabei kleiner sein als der RSA-Modul N.

Verschlüsselung

Beispiel

Es soll die Zahl 7 verschlüsselt werden. Der Sender benutzt den veröffentlichten Schlüssel des Empfängers $N = 143$, $e = 23$ und rechnet

$$2 \equiv 7^{23} \pmod{143}$$

Das Chiffrat ist also $c = 2$.

Entschlüsseln von Nachrichten

Der Geheimtext c kann durch modulare Exponentiation wieder zum Klartext m entschlüsselt werden. Der Empfänger benutzt die Formel

$$m \equiv c^d \pmod{N}$$

mit dem nur ihm bekannten Wert d sowie N.

Entschlüsselung

Beispiel

Für gegebenes $c = 2$ wird berechnet

$$7 \equiv 2^{47} \pmod{143}$$

Der Klartext ist also $m = 7$.

Signieren von Nachrichten

Um eine Nachricht m zu signieren, wird vom Sender auf die Nachricht die RSA-Funktion mit dem eigenen privaten Schlüssel d angewendet. Zum Prüfen wendet der Empfänger auf die Signatur $m^d \bmod N$ mit Hilfe des öffentlichen Schlüssels des Senders e die Umkehrfunktion an und vergleicht diese mit der zusätzlich übermittelten unverschlüsselten Nachricht m. Wenn beide übereinstimmen, ist die Signatur gültig und der Empfänger kann sicher sein, dass derjenige, der das Dokument signiert hat, auch den privaten Schlüssel besitzt und dass niemand seit der Signierung das Dokument geändert hat. Es wird also die Integrität und Authentizität garantiert, vorausgesetzt, der private Schlüssel ist wirklich geheim geblieben. Aufgrund der Homomorphieeigenschaft von RSA kann mit diesem Verfahren nur eine Nachricht signiert werden. Liegen nämlich zwei Signaturen m_1^d, m_2^d vor, so kann ein Angreifer daraus durch Multiplizieren die Signatur der Nachricht $m_1 m_2$ berechnen.

Dieses Problem kann umgangen werden, indem nicht die Nachricht selbst signiert wird. Stattdessen wird mit einer zusätzlich zum Signaturverfahren spezifizierten kollisionsresistenten Hashfunktion H der Hash-Wert $H(m)$ der Nachricht berechnet. Dieser wird mit dem privaten Schlüssel signiert, um die eigentliche Signatur zu erhalten. Der Empfänger kann die so erhaltene Signatur mit dem öffentlichen Schlüssel verifizieren und erhält dabei einen Hashwert $H(m)'$. Diesen vergleicht er mit dem von ihm selbst gebildeten Hashwert $H(m)$ der ihm vorliegenden Nachricht m. Wenn die beiden Hash-Werte übereinstimmen, kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass die Nachricht fehlerfrei übertragen wurde und nicht gefälscht ist. Auch diese Modifikation erfüllt allerdings nicht die modernen Sicherheitsanforderungen, daher werden Verfahren wie RSA-PSS verwendet um mit RSA zu signieren.

Siehe auch: Elektronische Unterschrift und Full-Domain-Hash

RSA mit dem Chinesischen Restsatz

Mit Hilfe des Chinesischen Restsatzes können Nachrichten effizienter entschlüsselt oder signiert werden. Weil der Modul N sehr groß ist, sind auch die im Rechner verwendeten Bitdarstellungen der Zahlen sehr lang. Der Chinesische Restsatz erlaubt es, die Berechnungen statt in einer Gruppe der Größe N gleichzeitig in den zwei kleineren Gruppen der Größe p und q auszuführen und das Ergebnis danach wieder zusammenzusetzen. Da hier die Zahlen wesentlich kleiner sind, ist diese Berechnung insgesamt schneller. Diese Variante wird nach der englischen Bezeichnung des Chinesischen Restsatzes CRT (Chinese remainder theorem) auch CRT-RSA genannt.

Der private Schlüssel besteht dann im Gegensatz zu dem, was im Rest dieses Artikels angenommen wird, aus folgenden Komponenten:

- N, der *RSA-Modul*,
- d, der *Entschlüsselungsexponent*,
- p, die *erste Primzahl*,
- q, die *zweite Primzahl*,

- $d_p = d \bmod (p-1)$, häufig *dmp1* genannt,
- $d_q = d \bmod (q-1)$, häufig *dmq1* genannt und
- $q_{Inv} = q^{-1} \bmod p$, häufig *iqmp* genannt.

Eine Signatur einer Nachricht m wird dann wie folgt durchgeführt.

- $m_1 = m^{d_p} \bmod p$
- $m_2 = m^{d_q} \bmod q$
- $s = (q_{Inv}(m_1 - m_2) \bmod p)q + m_2$

Aus der letzten Gleichung sieht man sofort, dass $s \bmod q = m_2$ und $s \bmod p = q_{Inv}q(m_1 - m_2) + m_2 \bmod p = m_1$. Die Signatur s stimmt also sowohl $\bmod p$ als auch $\bmod q$ mit m^d überein, daher ist nach dem Chinesischen Restsatz $s = m^d \bmod N$.

RSA ist kein Primzahltest

Wenn $p \neq q$ Primzahlen sind, funktioniert das RSA-Verfahren. Umgekehrt kann aber aus dem funktionierenden RSA-Verfahren nicht geschlossen werden, dass der Modul N aus zwei Primzahlen p und q zusammengesetzt ist, denn bei Carmichael-Zahlen funktioniert das Verfahren, obwohl Carmichael-Zahlen nicht der Standardform entsprechen.

Sicherheit

Public-Key-Verschlüsselungs-Verfahren wie RSA werden in der Praxis immer als hybride Verfahren in Verbindung mit symmetrischen Verfahren verwendet. Bei der Analyse der Sicherheit im praktischen Einsatz müssen die Sicherheit des Public-Key-Verfahrens und die praktische Sicherheit des Gesamtsystems betrachtet werden. Angriffe auf das RSA-Verfahren erfolgen oft über Seitenkanäle. Das Gesamtsystem kann unsicher sein, wenn nur eine Komponente, beispielsweise ein Computer, kompromittiert wurde.

Beziehung zwischen RSA und dem Faktorisierungsproblem

Bei der Kryptanalyse des RSA-Verfahrens unterscheidet man zwischen zwei Problemen:

- RSA-Problem (RSAP): Gegeben sind der öffentliche Schlüssel (N, e) sowie der Geheimtext c. Gesucht wird der Klartext m wobei gilt: $m^e \equiv c \pmod N$

  > Das Problem liegt hier in der Schwierigkeit, e-te Wurzeln modulo N zu ziehen, was zur Bestimmung der Nachricht m notwendig ist.

- RSA-Schlüsselproblem ($\mathrm{RSAP^*}$): Gegeben ist der öffentliche Schlüssel (N, e). Gesucht wird der geheime Schlüssel d wobei gilt: $ed \equiv 1 \pmod{\varphi(N)}$

  > Das Problem liegt hier in der Schwierigkeit, die Eulersche φ-Funktion von N *ohne* Kenntnis der Faktoren *p* und *q* zu berechnen.

Folgende Beziehungen zwischen den RSA-Problemen und $\mathrm{FACTORING}$, dem Faktorisierungsproblem, sind bekannt:

$$\mathrm{RSAP} \leq_p \mathrm{RSAP^*} =_p \mathrm{FACTORING}$$

Die Beziehung $\mathrm{RSAP} \leq_p \mathrm{RSAP^*}$ ist trivial, denn wenn man den privaten Schlüssel hat, kann man damit wie oben jeden beliebigen Geheimtext entschlüsseln. Ob die Umkehrung gilt, ist zurzeit unbekannt.

Auch die Beziehung $\mathrm{RSAP^*} \leq_p \mathrm{FACTORING}$ ist trivial, denn wenn man $N = pq$ faktorisiert hat, kann man damit leicht $\varphi(N) = (p-1)(q-1)$ berechnen, und dann mit dem euklidischen Algorithmus zu gegebenem öffentlichen Schlüssel den zugehörigen privaten Schlüssel effizient berechnen, wie in der Schlüsselerzeugung.

Für die Beziehung $\mathrm{FACTORING} \leq_p \mathrm{RSAP^*}$ ist schon lange ein *probabilistischer* Polynomialzeitalgorithmus bekannt. Vor kurzem wurde gezeigt, dass sich diese Reduktion im balancierten RSA (d. h. p und q haben gleiche Bitlänge) auch *deterministisch* durchführen lässt. Der Beweis verwendet das Coppersmith-Verfahren zur Bestimmung von Nullstellen eines irreduziblen bivariaten Polynoms mit ganzzahligen Koeffizienten, welches sich auf eine Gitterbasenreduktion zurückführen lässt.

Da alle gängigen Implementierungen balanciertes RSA verwenden, ist in der Praxis das Brechen des geheimen Schlüssels nur mit der Kenntnis des öffentlichen Schlüssels genau so schwer wie das Faktorisieren von N. Wegen $\mathrm{RSAP} \leq_p \mathrm{FACTORING}$ ist im Fall der zusätzlichen Kenntnis eines Geheimtexts die Schwierigkeit des Faktorisierungsproblems von zentralem Interesse.

Schwierigkeit des Faktorisierungsproblems

Man möchte $N = pq$ für sehr große Primzahlen p und q faktorisieren. Diese Primfaktorzerlegung ist für große Zahlen mit den heute bekannten Verfahren praktisch nicht durchführbar. Es ist aber nicht bewiesen, dass es sich bei der Primfaktorzerlegung um ein prinzipiell schwieriges Problem handelt.

Mit dem Quadratischen Sieb wurde 1994 die Zahl RSA-129 mit 129 Dezimalstellen in 8 Monaten von ca. 600 Freiwilligen faktorisiert. Mit der Methode des Zahlkörpersiebs wurde im Jahr 2005 von Wissenschaftlern der Friedrich-Wilhelms-Universität Bonn die im Rahmen der RSA Factoring Challenge von RSA Laboratories vorgegebene 200-stellige Dezimalzahl RSA-200 in ihre zwei großen Primfaktoren zerlegt[8]. Die ersten RSA-Zahlen bis RSA-500 wurden entsprechend der Anzahl der Dezimalstellen benannt, weitere RSA-Zahlen nach der Anzahl der Binärstellen. Die Faktorisierung begann Ende 2003 und dauerte bis Mai 2005. Unter anderem kam ein Rechnerverbund von 80 handelsüblichen Rechnern an der Universität Bonn zum Einsatz. Im November 2005 zahlten RSA Laboratories für die Faktorisierung von RSA-640, einer Zahl mit 640 Bits bzw. 193 Dezimalstellen, eine Prämie von 20.000 US-Dollar.[9] Obwohl mittlerweile für das Faktorisieren der RSA-Challenge-Zahlen keine Prämien mehr gezahlt werden, wurde im Dezember 2009 die Zahl RSA-768 faktorisiert.[10]

Für die Faktorisierung von RSA-1024 (309 Dezimalstellen) oder gar RSA-2048 (617 Dezimalstellen) waren 100.000 $ bzw. 200.000 $ ausgelobt; die RSA Laboratories haben im Mai 2007 das RSA Factoring Challenge beendet, nachdem die o. g. Wissenschaftler der Universität Bonn im selben Monat eine 1039-Bit Mersennezahl (312 Dezimalstellen) faktorisiert hatten.[11] Aufgrund der ungleichen Stellenzahl der Faktoren war das aber wesentlich leichter, als eine RSA-Zahl gleicher Länge zu faktorisieren. Die wachsende Rechenleistung moderner Computer stellt für die kurzfristige Sicherheit von RSA im Wesentlichen kein Problem dar, zumal diese Entwicklung vorhersehbar ist: Der Nutzer kann bei der Erzeugung seines Schlüssels darauf achten, dass der während der Dauer der beabsichtigten Verwendung nicht faktorisiert werden kann. Nicht vorhersehbare Entwicklungen wie die Entdeckung deutlich schnellerer Algorithmen oder gar Schaffung eines leistungsfähigen Quantencomputers, der die Faktorisierung von Zahlen durch Verwendung des Shor-Algorithmus' effizient durchführen könnte, bergen zumindest für die mittel- und langfristige Sicherheit der verschlüsselten Daten gewisse Risiken.

Zum konkreten Sicherheitsniveau bestimmter Schlüssellängen gibt es unterschiedliche Aussagen.[12] Laut Bundesnetzagentur sind für RSA-basierte Signaturen bis Ende 2020 Schlüssel mit einer Mindestlänge von 1976 Bit geeignet (Empfehlung 2048 Bit). Für Signaturverfahren nach den Anforderungen aus § 17 Abs. 1 bis 3 SigG, „für die die besten bekannten Angriffe auf dem Problem der Faktorisierung großer Zahlen oder auf dem Problem der Berechnung diskreter Logarithmen in endlichen Körpern beruhen (RSA und DSA), werden Schlüssellängen von mindestens 3 000 Bit verpflichtend werden“, um perspektivisch mindestens ein Sicherheitsniveau von 120 Bit zu etablieren.[5]

Schwierigkeit des RSA-Problems

In einigen Spezialfällen kann man das RSA-Verfahren brechen, ohne das Faktorisierungsproblem gelöst zu haben. Der Angriff von Wiener bei balanciertem RSA löst das RSA-Schlüsselproblem effizient unter der Annahme, dass der private Schlüssel nur eine geringe Bitlänge aufweist, genauer $d < \frac{1}{3}\sqrt[4]{N}$. Wiener verwendete dabei die Tatsache, dass unter der Abschätzung für d der Bruch $\frac{k}{d}$ (für eine ganze Zahl k) in der Kettenbruchentwicklung von $\frac{e}{N}$ auftaucht. Die Schranke wurde mit Mitteln der Gitterbasenreduktion auf $d < N^{0{,}292}$ verbessert.

Auch das RSA-Problem kann unter einigen Annahmen effizient ohne Faktorisieren gelöst werden. Der Angriff von Håstad ermittelt einen Klartext, der mit kleinem Verschlüsselungsexponent (etwa $e = 3$) für mehrere Empfänger vor dem Verschlüsseln speziell aufbereitet wurde, etwa wenn die Nummer des Empfängers in den Klartext codiert wurde. Dieser Angriff verwendet die Coppersmith-Methode, um kleine Nullstellen eines Polynoms in einer Unbestimmten zu berechnen, welche wiederum auf Gitterbasenreduktion beruht.

Angriffe gegen das unmodifizierte RSA-Verfahren

In der Praxis wird das RSA-Verfahren wie oben beschrieben nicht eingesetzt, da es mehrere Schwächen hat.

Die RSA-Verschlüsselung ist deterministisch. Das erlaubt es einem Angreifer, einen Klartext zu raten, ihn mit dem öffentlichen Schlüssel zu verschlüsseln und dann mit einem Chiffrat zu vergleichen. Da der Angreifer eine große Tabelle solcher Klartext-Chiffratpaare anlegen kann, darf der Klartext nicht leicht zu raten sein. Das bedeutet, dass unmodifiziertes RSA nicht IND-CPA sicher ist, heute eine Mindestanforderung an public-key Verschlüsselungsverfahren.

Wenn der Klartext m und der Verschlüsselungsexponent e so klein sind, dass $c = m^e < N$ ist, dann kann ein Angreifer die e-te Wurzel von c ziehen und das Chiffrat auf diese Weise entschlüsseln. Wurzelziehen ist nur modulo einer großen Zahl schwierig, in diesem Fall kann c aber als in den ganzen Zahlen liegend betrachtet werden.

Wenn dieselbe Nachricht m zu mehreren Empfängern geschickt wird, die zwar alle unterschiedliche (und teilerfremde) Moduli N_i benutzen, aber als öffentlichen Schlüssel den gleichen Exponenten e, dann kann aus e Nachrichten $m^e \mod N_1, \ldots, m^e \mod N_l$ mit dem Chinesischen Restsatz $m^e \mod \prod N_i$ berechnet werden. Weil $m^e < \prod N_i$ (nach Voraussetzung ist $m < N_i$ für alle i), kann diese Zahl wieder als in den ganzen Zahlen liegend aufgefasst werden und Wurzelziehen ist dort einfach. Dieser Angriff wird nach seinem Entdecker Johan Håstad als „Håstads Angriff“ bezeichnet.[13]

Da die RSA-Funktion $x \mapsto x^d \mod N$ multiplikativ ist (d. h. $(xy)^d = x^d y^d \mod N$ gilt), kann man aus jedem Chiffrat m^e ein weiteres gültiges Chiffrat $m^e r^e = (mr)^e$ erzeugen. Wenn man den Besitzer des zugehörigen geheimen Schlüssels davon überzeugen kann, diese Zahl zu entschlüsseln oder zu signieren, kann man aus dem Ergebnis mr leicht m gewinnen.

Dieselbe Eigenschaft erlaubt auch einen Angriff auf das Signaturverfahren. Aus bekannten Klartext-Signaturpaaren $s_1, = m_1^d \ldots, s_k = m_k^d$ lassen sich weitere gültige Signaturen

$$s = \prod s_i \mod N \text{ zu Nachrichten } m = \prod m_i \mod N$$

berechnen.

Padding

Um solche Angriffe zu verhindern, werden bei RSA-Verschlüsselung und RSA-Signatur sogenannte Padding-Verfahren eingesetzt. Standards für Padding-Verfahren für RSA werden z. B. in PKCS#1 oder ISO 9796 definiert. Diese nutzen aus, dass die Länge des Klartextes bzw. Hash-Wertes deutlich kleiner als die Länge von N ist, und fügen

dem Klartext bzw. dem Hash-Wert vor der Verschlüsselung oder Signatur eine Zeichenfolge R mit vorgegebener Struktur an, die unter mehreren möglichen zufällig gewählt wird und dadurch das Chiffrat randomisiert. Es wird also die RSA-Funktion nicht auf die Nachricht M oder auf den Hash-Wert $h(M)$ angewendet, sondern auf den Klartext (bzw. seinem Hashwert) mit angehängtem R. In der Regel enthält R eine Angabe über die Länge der Nachricht oder des Hash-Wertes oder eine eindeutige Zeichenfolge, die den Beginn von R kennzeichnet. Dies erleichtert nicht nur die Dekodierung, sondern erschwert auch Angriffe. Padding-Verfahren können für die Berechnung von R auch Zufallszahlen und Hashfunktionen verwenden. Einige moderne Paddingverfahren – beispielsweise das Optimal Asymmetric Encryption Padding (OAEP) oder das Probabilistic Signature Scheme (PSS) – verwenden kryptographische Hashfunktionen um den Klartext vor der Verschlüsselung weiter zu randomisieren und sind unter idealisierenden Annahmen an die verwendete Hashfunktion beweisbar sicher unter der RSA-Annahme.[14][15]

Chosen-Ciphertext-Angriff

Daniel Bleichenbacher stellte 1998 einen Angriff auf die in PKCS#1 v1 spezifizierte RSA-Verschlüsselung vor. Dabei nutzte er aus, dass PKCS#1 v1 ein Nachrichtenformat vorgibt und einige Implementierungen nach dem Entschlüsseln Fehlermeldungen ausgeben, falls dieses Format nicht eingehalten wurde. Um den Angriff gegen ein Chiffrat c durchzuführen, wählt man eine Zahl s und berechnet daraus ein neues Chiffrat $s^e c$. Bei dem Nachrichtenformat sind die ersten zwei Bytes 00 und 02, wenn also keine Fehlermeldung kommt, weiß man, dass sowohl bei der ursprünglichen Nachricht m als auch bei der neuen Nachricht sm die ersten beiden Bytes 00 02 sind. Mehrfache Wiederholung mit geschickt gewählten s erlauben es, nach und nach den gesamten Klartext aufzudecken.[16] RSA nach PKCS#1 ab Version 2 ist immun gegen diesen Angriff.

Sicherheit hybrider Verfahren

RSA wird aus Effizienzgründen in der Regel in Hybridverfahren mit symmetrischen Verfahren kombiniert. Zur hybriden Verschlüsselung wird zufällig ein Sitzungsschlüssel für ein symmetrisches Verschlüsselungsverfahren generiert, der dann per RSA verschlüsselt und zusammen mit der Nachricht übertragen wird. Zum Signieren wird nicht die gesamte Nachricht, sondern nur ein Hash-Wert signiert.

Für die Sicherheit von RSA sind Primzahlen mit mehreren hundert Dezimalstellen (mindestens 2048 Bit) erforderlich. Damit können symmetrische Schlüssel jeder üblichen Länge verschlüsselt werden. Gängige Verfahren zur symmetrischen Verschlüsselung basieren beispielsweise auf der Blockchiffre AES mit einer Schlüssellänge von 128, 168 oder maximal 256 Bit.

Eine sichere Hashfunktion wie SHA-2 erzeugt Hashwerte mit einer Länge zwischen 256 und 512 Bit. Damit lassen sich Signaturverfahren mittels RSA realisieren, die nur einen Signaturschritt benötigen.

Die Sicherheit des Gesamtsystems hängt sowohl bei der Verschlüsselung als auch bei der Signatur von der Sicherheit beider verwendeten Verfahren ab. Da bei RSA für ein ähnliches Sicherheitsniveau wie beim symmetrischen Verfahren deutlich längere Schlüssel nötig sind, wird in der Praxis die Sicherheit des Hybridverfahrens von der Sicherheit des Public-Key-Verfahrens bestimmt.

Vollständiges Beispiel

Anmerkung

- RSA direkt auf Texte anzuwenden birgt erhebliche Risiken. RSA wird deshalb, anders als im Beispiel, in der Praxis praktisch nur in Kombination mit anderen Verfahren verwendet. (Siehe: Hybride Verschlüsselung und Angriffe gegen das unmodifizierte RSA-Verfahren)
- Um das Beispiel übersichtlich zu halten, wurden relativ kleine Primzahlen verwendet. Zur sicheren Verschlüsselung werden typischerweise mindestens 600-stellige N empfohlen.[17]

Vorarbeiten

Die oben genannten Schritte sollen nun an einem vollständigen Beispiel erläutert werden. Um einen Text zu verschlüsseln, müssen zunächst Buchstaben in Zahlen umgewandelt werden. Dazu verwendet man in der Praxis zum Beispiel den ASCII-Code. Hier sei willkürlich die folgende Zuordnung gewählt:

```
A=01 B=02 C=03 usw. (00 = Leerzeichen)
```

Darüber hinaus sei angenommen, dass jeweils drei Zeichen zu einer Zahl zusammengefasst werden. Die Buchstabenfolge AXT wird also zu 012420. Die kleinste zu verschlüsselnde Zahl ist dann 000000 (drei Leerzeichen), die größte 262626 (ZZZ). Der Modulus $N = p \cdot q$ muss also größer als 262626 sein.

```
Klartext:   W  I  K   I  P  E   D  I  A
Kodierung: 23 09 11  09 16 05  04 09 01
```

Schlüsselerzeugung

Zunächst werden geheim zwei Primzahlen gewählt, beispielsweise $p = 307$ und $q = 859$. Damit ergibt sich:

$N = p \cdot q = 263713$

$\varphi(N) = (p-1) \cdot (q-1) = 262548$

$e = 1721$ (zufällig, teilerfremd zu $\varphi(N)$)

$d = 1373$ (das multiplikative Inverse zu $e \pmod{\varphi(N)}$ mit Hilfe des erweiterten euklidischen Algorithmus)

Öffentlicher Schlüssel: $e = 1721$ und $N = 263713$

Privater Schlüssel: $d = 1373$ und $N = 263713$

Verschlüsselung

```
C_n = K_n^e mod N  für n=1,2,3(,...)
C_1 = 230911^1721 mod 263713 = 001715
C_2 = 091605^1721 mod 263713 = 184304
C_3 = 040901^1721 mod 263713 = 219983
```

Entschlüsselung

```
K_n = C_n^d mod N  für n=1,2,3(,...)
K_1 = 001715^1373 mod 263713 = 230911
K_2 = 184304^1373 mod 263713 = 091605
K_3 = 219983^1373 mod 263713 = 040901
```

Signatur

```
C_n = K_n^d mod N
C_1 = 230911^1373 mod 263713 = 219611
C_2 = 091605^1373 mod 263713 = 121243
C_3 = 040901^1373 mod 263713 = 138570
```

Verifikation

$K_n = C_n^e \bmod N$
$K_1 = 219611^{1721} \bmod 263713 = 230911$
$K_2 = 121243^{1721} \bmod 263713 = 091605$
$K_3 = 138570^{1721} \bmod 263713 = 040901$

Die Berechnung der modularen Exponentiation kann durch binäre Exponentiation (Square-and-multiply) beschleunigt werden.

$$7^{23} \bmod 143 = \left(\left(\left(7^2\right)^2 \cdot 7\right)^2 \cdot 7\right)^2 \cdot 7 \bmod 143 = 2$$

Dabei wendet man nach jedem Rechenschritt auf die zu handhabenden Zahlen die Modulo-Operation „mod“ an, um die Zwischenergebnisse möglichst klein zu halten. Aus dem Klartext „7“ erhalten wir somit den Geheimtext „2“.

Anwendung

Hybride Verfahren

→ *Hauptartikel: Hybride Verschlüsselung*

RSA ist im Vergleich zu Verfahren wie 3DES und AES mindestens um den Faktor 1000 langsamer. In der Praxis wird RSA daher meist nur zum Austausch eines Schlüssels für die symmetrische Verschlüsselung benutzt. Für die Verschlüsselung der Daten werden dann symmetrische Verfahren eingesetzt. Damit sind die Vorteile beider Systeme vereint: einfacher Schlüsselaustausch und effiziente Verschlüsselung.

Anwendungsgebiete

- Internet- und Telefonie-Infrastruktur: X.509-Zertifikate
- Übertragungs-Protokolle: IPsec, TLS, SSH, WASTE
- E-Mail-Verschlüsselung: OpenPGP, S/MIME
- Authentifizierung französischer Telefonkarten
- Kartenzahlung: EMV
- RFID Chip auf dem deutschen Reisepass
- Electronic Banking: HBCI

Literatur

- Johannes Buchmann: *Einführung in die Kryptographie*. Springer-Verlag, Berlin 1999, ISBN 3-540-66059-3.
- *Der Dialog der Schwestern*. In: *c't*. Nr. 25, 1999 (Liegt auch dem E-Learning-Programm CrypTool (http://www.cryptool.de/) bei).
- Alexander May: *Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring*. In: *Advances in Cryptology (Crypto 2004), Lecture Notes in Computer Science*. Band 3152. Springer Verlag, 2004, S. 213–219.
- Dan Boneh: *Twenty Years of Attacks on the RSA Cryptosystem*. In: *Notices of the American Mathematical Society (AMS)*. Band 46, Nr. 2, 1999, S. 203–213.

Weblinks

Wikibooks: Beweisarchiv: Korrektheit des RSA-Kryptosystems – Lern- und Lehrmaterialien

- Erklärung von RSA vom Fachbereich Mathematik der Universität Wuppertal (http://www.matheprisma.uni-wuppertal.de/Module/RSA/index.htm)
- Einfache Erklärung von RSA mit Online-Beispielen von Hans-G. Mekelburg (http://www.nord-com.net/h-g.mekelburg/krypto/mod-asym.htm#rsa)
- *Arbeit über RSA mit Schwerpunkt in der Informatik.* (https://web.archive.org/web/20120818180314/http://www.basement-softworks.de/dokumente/realisierung_und_anwendung_des_rsa-algorithmus_in_der_informatik.html) Archiviert vom Original (http://derefer.unbubble.eu?u=http://www.basement-softworks.de/dokumente/realisierung_und_anwendung_des_rsa-algorithmus_in_der_informatik.html) am 18. August 2012, abgerufen am 18. August 2012.
- RSA-Codebeispiel (http://mitpress.mit.edu/sicp/psets/ps3/readme.html) in Scheme vom Massachusetts Institute of Technology
- Beispiel zur RSA-Verschlüsselung vorgerechnet von Joachim Mohr (http://kilchb.de/bsp_rsa.php)
- Interaktive Präsentation des RSA-Verfahrens von CrypTool (http://www.cryptool.org/images/ct1/presentations/RSA/RSA-Flash-de/player.html)
- Whitfield Diffie and Martin E. Hellman: New Directions in Cryptography (https://www-ee.stanford.edu/~hellman/publications/24.pdf), IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976
- Video: *RSA: Einführung (https://av.tib.eu/media/19815)*. Christian Spannagel 2012, zur Verfügung gestellt von der Technischen Informationsbibliothek (TIB), doi:10.5446/19815 (https://dx.doi.org/10.5446%2F19815).
- Video: *RSA: Konstruktion der Schlüssel (https://av.tib.eu/media/19816)*. Christian Spannagel 2012, zur Verfügung gestellt von der Technischen Informationsbibliothek (TIB), doi:10.5446/19816 (https://dx.doi.org/10.5446%2F19816).
- Video: *RSA: Ver- und Entschlüsselung (https://av.tib.eu/media/19817)*. Christian Spannagel 2012, zur Verfügung gestellt von der Technischen Informationsbibliothek (TIB), doi:10.5446/19817 (https://dx.doi.org/10.5446%2F19817).
- Video: *RSA: Beispiel Teil 1 (https://av.tib.eu/media/19813)*. Christian Spannagel 2012, zur Verfügung gestellt von der Technischen Informationsbibliothek (TIB), doi:10.5446/19813 (https://dx.doi.org/10.5446%2F19813).
- Video: *RSA: Beispiel Teil 2 (https://av.tib.eu/media/19814)*. Christian Spannagel 2012, zur Verfügung gestellt von der Technischen Informationsbibliothek (TIB), doi:10.5446/19814 (https://dx.doi.org/10.5446%2F19814).

Einzelnachweise

1. R.L. Rivest, A. Shamir, and L. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. (mit.edu (http://people.csail.mit.edu/rivest/Rsapaper.pdf) [PDF]).
2. Whitfield Diffie, Martin E. Hellman: *New Directions in Cryptography*. (stanford.edu (https://www-ee.stanford.edu/~hellman/publications/24.pdf) [PDF]).
3. C. C. Cocks: *A note on 'non-secret encryption'.* 1973 (https://web.archive.org/web/20080227001905/http://www.cesg.gov.uk/site/publications/media/notense.pdf) (Memento vom 27. Februar 2008 im *Internet Archive*)
4. Patent US4405829 (http://worldwide.espacenet.com/publicationDetails/biblio?locale=de_EP&CC=US&NR=4405829): *Cryptographic communications system and method.* Veröffentlicht am 20. September 1983, Anmelder: Massachusetts Institute of Technology, Erfinder: Ronald L. Rivest, Adi Shamir, Leonard Adleman.
5. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 21. Januar 2014 (BAnz AT 20.02.2014 B4 (https://www.bundesanzeiger.de/ebanzwww/wexsservlet?genericsearch_param.start_date%3A0=20&genericsearch_param.start_date%3A1=02&genericsearch_param.start_date%3A2=2014&genericsearch_param.stop_date%3A0=20&genericsearch_param.stop_date%3A1=02&genericsearch_param.stop_date%3A2=2014&%28page.navid%3Ddetailsearchlisttodetailsearchlistupdateresetpage%29=Dokumente+anzeigen&genericsearch_param.fulltext=BAnz+AT+20.02.2014+B4))
6. D. Boneh: *Twenty Years of Attacks on the RSA Cryptosystem*. In: *Notes of the AMS*. Band 46, Nr. 2, Februar 1999, S. 203–213 (PDF (http://www.ams.org/notices/199902/boneh.pdf)).
7. MJ Wiener: *Cryptanalysis of short RSA secret exponents*. In: *IEEE Transactions on information theory*. Band 36, Nr. 3, Mai 1990, S. 553–558, doi:10.1109/18.54902 (https://dx.doi.org/10.1109%2F18.54902).
8. RSA Labs: *RSA-200 is factored!* (http://www.rsa.com/rsalabs/node.asp?id=2879)
9. MathWorld: *RSA-640 Factored* (http://mathworld.wolfram.com/news/2005-11-08/rsa-640/)
10. RSA Labs: *RSA-768 is factored!* (http://www.emc.com/emc-plus/rsa-labs/historical/rsa-768-factored.htm)
11. http://www.crypto-world.com/announcements/m1039.txt
12. [1] (http://www.keylength.com/en/compare/)
13. Johan Håstad: *Solving Simultaneous Modular Equations of Low Degree*. In: *SIAM Journal on Computing*. Band 17, Nr. 2, 1988, S. 336–341 (Solving Simultaneous Modular Equations of Low Degree (http://www.nada.kth.se/~johanh/papers.html)).
14. What is OAEP? (http://www.rsa.com/rsalabs/node.asp?id=2346) (englisch)
15. What is PSS/PSS-R? (http://www.rsa.com/rsalabs/node.asp?id=2350) (englisch)

16. Daniel Bleichenbacher: *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1 (http://link.springer.com/chapter/10.1007/BFb0055716)*. In: *CRYPTO '98*. 1998, S. 1–12.
17. *Kryptographische Verfahren: Empfehlungen und Schlussellängen.* (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.pdf?__blob=publicationFile) In: *BSI.* Bundesamt für Sicherheit in der Informationstechnik, 10. Februar 2014, S. 15, 28, abgerufen am 13. Juli 2014 (PDF 1.4 (830kiB), Tabelle 1.2 und Tabelle 3.1 empfehlen Schlüssellängen von 2000Bit für RSA).
