Verschlüsselungsverfahren

Christoph Schöpf

4. Juni 2014

Inhaltsverzeichnis

1 Einführung

Jeder nutzt täglich Geräte und Anwendungen, die irgendeine Form der Verschlüsselung verwenden. Sei es zum Schutz der Privatsphäre bei der Nutzung von Telekommunikation oder zum Schutz von persönlichen Daten, wie Bankinformationen beim Online-Shopping oder Netbanking.

Dieses Dokument bietet einen Überblick über die verschiedenen Arten von Verschlüsselungsverfahren und deren Funktionsweisen. Bei den *asymmetrischen* Verfahren wird noch genauer auf das RSA-Verfahren eingegangen.

Um die Lesbarkeit zu erleichtern, wird auf die zusätzliche Formulierung der weiblichen Form verzichtet. Die männliche Form soll als geschlechtsneutral verstanden werden.

2 Begriffserklärung

- Kryptographie - Wissenschaft der Verschlüsselung und Entschlüsselung von Daten.
- Kryptosystem - Verschlüsselungsverfahren
- Kryptoanalytiker - Codebrecher, der den Geheimtext unbefugt entziffern will.
- Klartext - Der zu verschlüsselnde Text.
- Geheimtext - Der verschlüsselte Text.
- Chiffrierung - Der Verschlüsselungsvorgang
- Dechiffrierung - Der Entschlüsselungsvorgang
- mod - Modulo-Operator, dessen Ergebnis der Rest einer Division ist. ($5 \bmod 3 = 2$)

3 Anwendungsbereich

In den verschiedensten Bereichen ist eine sichere Verschlüsselung notwendig.
Einige werden nachfolgend aufgezählt [3]:

1. Kommunikation: Verschlüsselte Verbindungen werden bei Handynetzen und Internettelefonie verwendet.
2. Online Banking: Für die sichere Durchführung einer Online Überweisung muss der Login zu Ihrem Konto über eine verschlüsselte Verbindung erfolgen.
3. Internet-Shopping: Beim Einkaufen von zu Hause werden an mehreren Stellen Verschlüsselungstechnologien benötigt. Login und Übermittlung von sicherheitskritischen Daten (z. B. Kreditkartennummern) erfordern eine verschlüsselte Verbindung. Das Speichern dieser Daten am Web-Server muss auch verschlüsselt erfolgen.
4. Identifikation: Wird durchgeführt um den Zugriff auf Informationen zu erlauben.
5. Zertifizierung: Man benötigt sie, um sicher zu stellen, ob eine Person berechtigt ist, einen bestimmten Schlüssel zu verwenden.
6. Pay-TV: Der Anbieter sendet ein verschlüsseltes Fernsehsignal, das vom Empfänger mit Hilfe des richtigen Schlüssels (elektronischer Schlüssel per Chipkarte) entschlüsselt wird.

4 Arten von Verschlüsselungen

Verschlüsselungsverfahren lassen sich in drei Gruppen einteilen: *Symmetrische*, *asymmetrische* und *hybride* Verschlüsselungsverfahren.

4.1 Symmetrische Verschlüsselung

Die *symmetrische* Verschlüsselung wird auf Basis eines einzigen Schlüssels durchgeführt. Dieser Schlüssel muss mittels einer „sicheren“ Verbindung übertragen werden. Dazu kann ein *asymmetrisches* Verschlüsselungsverfahren (Kapitel 4.2) oder eine persönliche Übergabe angewandt werden. Sobald Sender und Empfänger einen Schlüssel haben, kann ein verschlüsselter Datenaustausch erfolgen. Der Schlüssel sollte aber in periodischen Abständen ausgewechselt werden, weil mit jedem neuen Geheimtext die Wahrscheinlichkeit steigt, dass der Kryptoanalytiker den Code entziffert.
Einige Beispiele für *symmetrische* Verschlüsselungsverfahren [2] sind:

1. DES (Data Encryption Standard) oder Lucifer: bis Oktober 2000 der Verschlüsselungsstandard der USA; Lucifer, das Verfahren, wurde 1974 von IBM entwickelt.
2. AES (Advanced Encryption Standard) oder Rijndael: der US-amerikanische Verschlüsselungsstandard, Nachfolger des DES; von Joan Daemen und Vincent Rijmen
3. Twofish: Blockverschlüsselungsverfahren[1], vom Counterpane Team; wird u. a. in Microsoft Windows eingesetzt
4. Blowfish: 1993 von Bruce Schneier entwickeltes Blockverschlüsselungsverfahren

4.2 Asymmetrische Verschlüsselung

Bei *asymmetrischen* Kryptosystemen werden zum ver- und entschlüsseln jeweils zwei verschiedene Schlüssel verwendet. Einer dieser Schlüssel wird „Public-Key“ genannt, deshalb werden *asymmetrische* Verschlüsselungsverfahren oft als „Public-Key Verschlüsselungsverfahren“ bezeichnet. Der Public-Key ist öffentlich und für jeden zugänglich. Im Gegensatz zum „Private-Key“, der nur dem Empfänger bekannt ist. Im folgenden Kapitel wird nun auf das am häufigsten verwendete Kryptosystem, dem RSA-Verfahren, näher eingegangen.

[1] Eigenschaft von Kryptosystemen, bei denen sich der Schlüssel auf einen Block von Zeichen bezieht.

4.2.1 RSA-Verfahren

RSA steht für die Anfangsbuchstaben der Entwickler Rivest, Shamir und Adleman, die das RSA-Verfahren im Jahre 1977 entwickelten [1].
Beim RSA-Verfahren errechnet sich der Public-Key aus:

$$n = p \cdot q \tag{1}$$

$$m = (p-1) \cdot (q-1) \tag{2}$$

$$a \perp m \tag{3}$$

In (1) und (2) sind p und q Primzahlen. Weiters muss für m eine Zahl a gewählt werden, die teilerfremd[2] zu m ist. Zur Veranschaulichung wird nachfolgend ein Beispiel dargestellt.

Beispiel: Der Public-Key des Empfängers:

$$n = 3 \cdot 7 = 21 \tag{4}$$

$$m = (3-1) \cdot (7-1) = 12 \tag{5}$$

$$a = 5 \tag{6}$$

Der öffentliche Schlüssel setzt sich nun zusammen aus a und n. Auf der Senderseite wird der Klartext nun mit dem Public-Key des Empfängers verschlüsselt. Die Verschlüsselung mit dem öffentlichen Schlüssel gilt als sicher, weil die Modulo-Operation eine Einwegfunktion[3] ist. Daher lassen sich aus einem Ergebnis nicht die Eingangsparameter eindeutig zurückrechnen.

$$y = x^a \ mod \ n \tag{7}$$

In der Formel (7) stellt x den zu verschlüsselnden Klartext dar. Der Geheimtext y wird dem Empfänger übermittelt. Zur Vereinfachung wird in unserem Beispiel die Zahl 17 als Nachricht übertragen. In der Praxis werden Wörter als Zahlenfolgen mit Hilfe der ASCII-Tabelle [5] repräsentiert, die zur Berechnung des Geheimtextes dienen. Zusätzlich muss gelten, dass $x < n$ ist. Das ist bei der praktischen Anwendung kein Problem, weil für p und q sehr große Primzahlen ($\approx$ 300-stellig) verwendet werden.

Beispiel: Verschlüsselung des Klartexts auf der Senderseite:

$$y = 17^5 \ mod \ 21 = 5 \tag{8}$$

Der Empfänger ermittelt nun aus m und a seinen kombinierten Schlüssel zum Entschlüsseln der Nachricht. Dieser Schlüssel setzt sich zusammen aus a (Public-Key) und m (Private-Key).

$$b = a^{-1} \ mod \ m \tag{9}$$

Das Inverse von a kann mittels des erweiterten euklidischen Algorithmus [6] berechnet werden, sodass die Gleichung aus (10) gilt.

$$a \cdot b \ mod \ m = 1 \tag{10}$$

Beispiel: Der Empfänger errechnet b wie folgt:

$$b = 5^{-1} \ mod \ 12 = 5 \tag{11}$$

$$5 \cdot 5 \ mod \ 12 = 1 \tag{12}$$

Als nächstes kann der Empfänger den Geheimtext mit folgender Formel decodieren:

$$x = y^b \ mod \ n \tag{13}$$

[2] Zwei natürliche Zahlen sind teilerfremd, falls keine natürliche Zahl existiert, die beide Zahlen teilt (außer Eins).

[3] Bei einer Einwegfunktion f(x) lassen sich für alle x, f(x) leicht berechnen, aber für ein gegebenes y lässt sich schwer ein x finden.

Beispiel: In unserem Beispiel rechnet der Empfänger:

$$x = 5^5 \; mod \; 21 = 17 \tag{14}$$

Der Empfänger verwendet zum Dechiffrieren den Geheimtext des Senders, sein errechnetes b und den Public-Key n. Einem Krypotoanalytiker ist es nicht in praktikabler Zeit möglich b zu errechnen, weil ihm m unbekannt ist. Das RSA-Verfahren beruht auf dem mathematischen Problem der Faktorisierung[4] zweier großer Primzahlen p und q. Die Funktion (1) ist eine Einwegfunktion mit der Eigenschaft, dass f(p, q) = p · q schnell zu berechnen ist. Die Umkehrfunktion (Faktorisierung), bei der das Produkt zweier Primzahlen gegeben ist und man p und q berechnen will, aber nicht in praktikabler Zeit berechenbar ist.

4.3 Hybride Verschlüsselung

Die *hybride* Verschlüsselung kombiniert das *asymmetrische* und *symmetrische* Kryptoverfahren miteinander. Eine Kombination dieser beiden Verfahren bringt erhebliche Geschwindigkeitsvorteile gegenüber dem *asymmetrischen* Verschlüsselungsverfahren. Grundidee beim *hybriden* Verfahren ist es, den Klartext zuerst mit einem zufällig generierten Schlüssel zu verschlüsseln (*symmetrisch*). Dann wird nur der zufällig gernierte Schlüssel mit dem *asymmetrischen* Kryptoverfahren verschlüsselt. Der kodierte Schlüssel und der Geheimtext werden dann als Nachricht übermittelt. Erhebliche Geschwindigkeitsvorteile ergeben sich bei größeren Datenmengen, weil lediglich der Schlüssel mit dem langsamen *asymmetrischen* Verfahren verschlüsselt werden muss [2]. Nachfolgend die zwei bekanntesten *hybriden* Verschlüsselungsverfahren:

1. PGP [7] - Pretty Good Privacy wurde von Phil Zimmermann im Jahr 1991 für Verschlüsselung und Unterschreiben von Daten entwickelt.
2. GnuPG oder GPG [4] - Gnu Privacy Guard wurde im Jahr 1999 entwickelt von Werner Koch. Dient als Ersatz für PGP und stellt Funktionalitäten für Ver- und Entschlüsselung von Daten und das Erzeugen von elektronischen Signaturen zur Verfügung.

5 Schluss

Solange die mathematischen Probleme hinter den Verschlüsselungsverfahren nicht berechenbar werden, sind die *asymmetrischen* bzw. *hybriden* Verschlüsselungsverfahren in der Praxis wohl noch lange im Einsatz. Die stetige Verbesserung der Rechnerleistung ermöglicht immer schnelleres Lösen von mathematischen Problemen, aber die heutigen Kryptosysteme können dieser Verbesserung mittels längerer Schlüssel entgegenwirken. Das heute noch am häufigsten eingesetzte RSA-Verfahren wird vermutlich immer mehr von *hybriden* Kryptosystemen ersetzt werden, weil diese erhebliche Performancevorteile besitzen. Dennoch ist es erstaunlich, wie lange das RSA-Verfahren den enormen Sicherheitsstandards des heutigen Internets standhält.

Literatur

[1] Franz Embacher. RSA - Verschlüsselung. `http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/`.

[2] NetPlanet. Arten von Verschlüsselungsverfahren - NetPlanet. `http://www.netplanet.org/kryptografie/verfahren.shtml` [Online; Stand 24. Mai 2014].

[3] Netzwelt. Wo wird Verschlüsselung eingesetzt? `http://www.netzwelt.de/news/105101_3-netzwelt-wissen-verschluesselung.html` [Online; Stand 24. Mai 2014].

[4] GNU Privacy Team. Gnu privacy guard. `https://www.gnupg.org/` [Online; Stand 24. Mai 2014].

[5] Harald Zankl. Diskrete Mathematik, 2013. Skriptum zur Vorlesung Diskrete Mathematik, Universität Innsbruck, page: 136, 2. Auflage.

[6] Harald Zankl. Diskrete Mathematik, 2013. Skriptum zur Vorlesung Diskrete Mathematik, Universität Innsbruck, pages: 69-71, 2. Auflage.

[7] Phil Zimmermann. Pretty Good Privacy. `http://philzimmermann.com/EN/background/index.html` [Online; Stand 24. Mai 2014].

[4] Die Zerlegung eines Objekts in mehrere Faktoren.