Kryptografie

– "Vertrauen verpflichtet"

Christian Hofer

Was ist Kryptografie ?

Als Kryptografie bezeichnet man die Wissenschaft davon, wie man Nachrichten verschlüsselt. Die Ergebnisse dieser Forschungen werden heute, außer in Softwarepaketen zur Datenverschlüsselung, zum Beispiel auch zur Absicherung von Bankomatkarten und GSM-Telefongesprächen genutzt.

Wozu benötige ich kryptografische Systeme ?

Verschlüsselungstechniken sollen Informationen vor unberechtigtem Zugriff und vor Manipulation schützen. Dazu einige Beispiele aus der Praxis:

- Untersuchungsergebnisse von Forschergruppen an unterschiedlichen Orten sollen ausgetauscht werden können, ohne dass konkurrierende Forscher die Daten zu sehen bekommen.
- Medizinische Untersuchungsergebnisse eines Patienten sollen, ohne dass sie publik werden, an einen Experten zur Begutachtung geschickt werden.
- Die Mitarbeiter einer Firma an verschiedenen Orten wollen Daten mit der gleichen Sicherheit austauschen können, als wären sie im lokalen Netzwerk.
- Internetanbieter wollen sicherstellen, dass eine Bestellung von demjenigen kommt, der sich als Absender ausgibt und sowohl Anbieter als auch Kunde wollen sicher sein, dass die Bestellung nicht von Dritten manipuliert wird.
- Bei Bestellungen mit Kreditkarte erwartet der Kunde, dass seine Daten nicht in falsche Hände geraten.
- Sehr viele Viren werden per e-mail Anhang verbreitet – Daher sollte man besonders bei solchen Nachrichten sicher sein, dass die e-mail auch wirklich von einem vertrauenswürdigen Freund stammt und der Absender nicht gefälscht ist.
- Die Geheimdienste der USA, GB und Australien können über das Lauschsystem "Echelon" europäische Unternehmen, Organisationen und Privatpersonen ausspionieren, wenn diese Daten unverschlüsselt senden.

Die Ziele der Kryptografie sind also das Erreichen von größtmöglicher

- **Vertraulichkeit** – Unberechtigte dürfen eine Nachricht nicht entschlüsseln können.
- **Authentizität** – Der Urheber eines Textes muss einwandfrei feststellbar sein.
- **Integrität** – Die Veränderung einer Nachricht muss erkennbar sein.

Verfahren zur Gewährleistung von Vertraulichkeit

Schon Julius Caesar verwendete Verschlüsselung für seine Nachrichten. Dabei ersetzte er die Buchstaben der Nachricht durch jene, die drei Stellen weiter im Alphabet stehen. Dieses Verfahren hieße heute "Algorithmus" (allgemeine Vorschrift), die Anzahl der zu versetzenden Stellen wäre der "Schlüssel" (Key). Damit ist ein Text mit einem "Kryptosystem" verschlüsselt worden. Heute unterscheidet man zwischen Verfahren mit geheimem Schlüssel und Verfahren mit öffentlichem Schlüssel sowie deren Kombination.

Verfahren mit geheimem Schlüssel: DES, IDEA und AES

Dabei verwendet der Absender den Schlüssel zur Erzeugung des Geheimtextes und der Empfänger muss ihn zur Entschlüsselung ebenfalls verwenden. Auf Grund dieser Symmetrie werden solche Verfahren auch **symmetrische Verfahren** genannt und der Schlüssel muss verständlicherweise auf sichere Art zwischen den beiden Partnern ausgetauscht werden. Moderne Kryptosysteme ersetzen nicht jedes einzelne Zeichen, so wie Julius Caesar, durch andere, sondern es wird in jedem Verschlüsselungsschritt ein längerer Block von Zeichen verarbeitet und durch einen anderen ersetzt, wobei jedes Klartextzeichen eines Blocks das gesamte Ergebnis beeinflusst. (Blockverschlüsselungen) Regelmäßigkeiten in den Klartextzeichen werden dabei über mehrere Zeichen hinweg verteilt und verringern die Spuren die sich für die Analyse nutzen ließe.
An der Entwicklung von **DES** (**D**ata **E**ncryption **S**tandard) waren sowohl IBM als auch die NSA (National Security Agency) der USA beteiligt und es ist das wohl am häufigsten eingesetzte Verfahren, so auch zur Abwicklung von Bargeldauszahlungen mit einer eurocheque-Karte. Es verwendet 56-Bit lange Schlüssel und 64-Bit Blöcke. DES arbeitet mit der Produktverschlüsselung, eine Kombination aus Substitutionen und Transpositionen. Zwar ist DES ein ANSI-Standard und wird in vielen Applikationen verwendet, es ist aber wegen der zu geringen Schlüssellänge nicht mehr sicher. Eine internationale "Brute Force Attack", bei der ein Spezialrechner und Tausende Rechner via Internet teilgenommen haben, benötigte nur 23 Stunden zur Entschlüsselung einer Testnachricht. Durch eine geänderte Krypto-Exportregelung der US-Regierung ist es jetzt allerdings möglich, den Netscape Communicator 4.7 und den Internet Explorer 5 mit 128-Bit Verschlüsselung (statt 56-Bit) zu erhalten und somit sichere Übertragungen im Internet durchzuführen.
1990 wurde in der Schweiz das **IDEA** Verfahren (**I**nternational **D**ata **E**ncryption **A**lgorithm) entwickelt. IDEA weist viele Schwachstellen von DES nicht auf, so verwendet es 128-Bit lange Schlüssel, die einzelnen elementaren Operationen haben unterschiedliche mathematische Eigenschaften und es werden nie zwei gleiche Operationen hintereinander durchgeführt. Außerdem sind reine Software-Lösungen für IDEA cirka doppelt so schnell wie für DES. Mehrere unterschiedliche Forschergruppen versuchen zurzeit einen Nachfolger für DES zu finden. Dieser wird als **AES** (**A**dvanced **E**ncryption **S**tandard) vorgesehen und soll sowohl schneller als DES sein, frei verfügbar und öffentlich nachprüfbar sowie in Chipkarten einsetzbar sein.

Verfahren mit öffentlichem Schlüssel: RSA (Public-Key-Verfahren)

Dadurch, dass beim symmetrischen Verfahren zwei Mail-Partner mit dem gleichen Schlüssel zum ver- und entschlüsseln arbeiten entsteht das Problem, dass eine Anzahl von n Mail-Partnern n*(n-1)/2 Schlüssel benötigt, die irgendwie auszutauschen sind. Die große Schlüsselanzahl kann zwar von einem immer erreichbaren Keyserver verwaltet werden, der aber einer zentralen Meldestelle = "Großer Bruder" gleichkommt. Daher haben 1976 W. Diffie und M. E. Hellman ein anderes System vorgeschlagen: In einem **asymmetrischen** System gibt es für jeden Teilnehmer ein Schlüssel*paar*, bestehend aus einem geheimen und einem öffentlichen Schlüssel. Nur der Besitzer der Schlüssel kennt auch den geheimen, der öffentliche kann frei verteilt werden. Sendet nun Mail-Partner A eine vertrauliche Mail an B, dann verschlüsselt er diese mit dem öffentlichen Schlüssel des Empfängers B. Nur B kann die E-Mail mit seinem dazu passenden geheimen Schlüssel wieder entschlüsseln. Es reicht nicht aus, den öffentlichen Schlüssel zu kennen, um die E-Mail zu entschlüsseln und der geheime Schlüssel lässt sich nicht aus dem Öffentlichen berechnen. Daher ist die Verbreitung des öffentlichen Schlüssels ohne einen sicheren Übertragungsweg möglich. Man benötigt bei einer solchen asymmetrischen Lösung gleich viele Schlüssel(paare) wie Mail-Partner miteinander kommunizieren. Damit dieses System funktioniert ist es allerdings notwendig, dass zwischen dem öffentlichen und privaten Schlüssel eine sehr enge, formelmäßig erfassbare Beziehung besteht. Diese würde allerdings einem Angreifer wieder die Möglichkeit geben, das entsprechende Gleichungssystem zu lösen. Abhilfe schaffen z.B.: Primfaktorenzerlegungen.

Die große Bedeutung von Primzahlen in der Kryptografie liegt in der Tatsache, dass es schwierig und zeitaufwändig ist, herauszufinden ob es sich um eine Primzahl handelt, sowie die Primfaktoren einer Zahl zu finden: Sind zum Beispiel p und q zwei große Primzahlen und werden sie multipliziert (n=p*q), so sind p und q per Definition die einzigen Primfaktoren vom Produkt n. Wird diese Zahl n nun verschickt und abgefangen, so können die Primfaktoren nicht schnell errechnet werden. Das Problem besteht nun darin, schnell viele große Primzahlen zu ermitteln, weil bei jeder Transaktion mit einem kryptografischen Protokoll neue Primzahlen verwendet werden. Eine praktische Implementation da-

für ist das RSA-Verfahren. Wie alle asymmetrischen Verfahren hat dieses den Nachteil, dass die Berechnungen aufwändig sind.

Hybridverfahren

Daher werden in aktuellen Verschlüsselungsprogrammen vielfach Hybridverfahren eingesetzt, wobei das Public-Key-System als abhörsicheres "Transportsystem" für den Schlüssel des symmetrischen Verfahrens dient.
Die Verschlüsselung der eigentlichen Nachricht erfolgt also zum Beispiel über das effizientere IDEA und nur ein Sitzungsschlüssel wird per RSA erzeugt. Ein solches Hybridverfahren wird zum Beispiel im Verschlüsselungsprogramm PGP (Pretty Good Privacy) eingesetzt.

Verfahren zur Sicherstellung von Integrität und Authentizität

Wenn sich ein Angreifer aktiv in die Kommunikation einschaltet und eine Nachricht manipuliert, versucht man dies mit der Erstellung eines "Fingerabdrucks" der übermittelten Daten zu erkennen. Prüfsummern, wie sie zum Beispiel von Modems bekannt sind schützen allerdings nicht gegen *absichtliche* Änderung einer Nachricht. Deshalb muss ein solcher Prüfsummen-Algorithmus (Hashfunktion) für beliebig lange Nachrichten einen kleinen Wert vordefinierter Länge liefern, von jedermann leicht berechenbar sein und es soll ausgeschlossen sein, dass aus dem Hashwert eine Nachricht mit diesem Hashwert generierbar ist. Beispiele für Verfahren die solche Hashwerte liefern sind MD5 (in PGP verwendet), SHA-1 oder RIPEMD-160. Letztere werden heute wegen der 160-Bit langen Hashwerte als sicher eingestuft. Alle Verfahren basieren auf den oben erwähnten Blockverschlüsselungsalgorithmen. Der Forderung nach eindeutiger Authentifizierung des Absenders kann mit elektronischen Unterschriften (Signaturen) nachgekommen werden. Beim Einsatz symmetrischer Verfahren benötigt man einen vertrauenswürdigen Vermittler, ein so genanntes Trust Center, welches mit jedem Teilnehmer einen geheimen Schlüssel vereinbart. Sendet A eine Nachricht an den Empfänger B, verschlüsselt A diesen Text mit dem geheimen Schlüssel und schickt die Nachricht an das Trust Center. Dort wird die Nachricht entschlüsselt und mit dem geheimen Schlüssel von B an denselben versandt. Sowohl der hohe Aufwand im Trust Center als auch die notwendige hohe Vertauenswürdigkeit lassen vor allem für die private Kommunikation Verfahren auf Basis der Public-Keys angebrachter erscheinen. Dabei benutzt A den eigenen geheimen Schlüssel zur Verschlüsselung des Hash-Wertes der Nachricht. Das Ergebnis wird mit der Nachricht an B gesendet, der mit dem öffentlichen Schlüssel von A den Hash-Wert rekonstruiert und ihn mit dem selbst für den Text berechneten vergleicht.

Zertifizierung von Schlüsseln

Sowohl die Verschlüsselung als auch die Anwendung von Signaturen hängen entscheidend von der Zugehörigkeit des Schlüsselinhabers und des Schlüssels ab. Dazu gibt es zwei Vorgehensweisen:

Das Modell der **C**ertification **A**uthority (**CA**) stellt ein, dem Trust Center ähnliches, System dar, bei dem die Beglaubigung durch offizielle Autoritäten erfolgt. Das Vorweisen des Reisepasses bei der CA oder einem Vertreter (z.B.: Postamt) wäre eine solche Beglaubigung. Die CA stellt dann im täglichen Betrieb zertifizierte Informationen über die registrierten Kunden zur Verfügung.

Im Privaten Bereich reicht es allerdings meist aus, wenn man ein Vertrauensnetz ("Web of Trust") aufbaut, indem man sich der Vertrauenswürdigkeit eines Freundes sicher ist. Die Gewissheit beruht darauf, dass vertrauenswürdige Personen ihre Einschätzung über die Identität und Vertrauenswürdigkeit anderer Menschen weiterreichen. Dieses "Web of Trust" ist vor allem durch den Einsatz im Programm PGP weit verbreitet.

Sicherheitsbewusste Organisation von Abläufen

Zum Aufbau eines *sicheren* kryptografischen Systems reicht es nicht aus, entsprechende Algorithmen und Schlüssel einzusetzen. Auch nichtkryptografische Angriffe müssen einkalkuliert und entsprechend dem Sicherheitsbedürfnis verhindert werden.

Schutz der Rechnerumgebung:
Neben so trivialen Angriffen wie dem Ausbau der Festplatte oder dem Stehlen von ausgedruckten Passwortlisten ist sicher die geeignete Wahl des Rechner,- Netz- und Verschlüsselungspasswortes entscheidend.
In Netzwerkumgebungen muss auch das Belauschen mit Hilfe von Packet Sniffer-Programmen durch geeignete Netztopologie und Protokollauswahl verhindert werden. Ebenso gefährlich sind Trojaner, die durch Ausspähen des Passwortes alle anderen Sicherungsmechanismen zunichte machen.

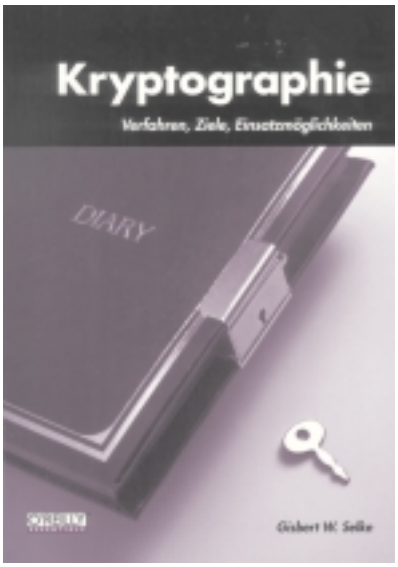
Sicheres Schlüsselmanagement:
Die Wahl der Schlüssellänge hängt vom verwendeten System ab. Symmetrische Verfahren gelten heute bei Schlüssellängen von 128-Bit als sicher, asymmetrische benötigen für die gleiche Sicherheit cirka 2300-Bit. Eine Kombination in Hybridverfahren ist daher nur so stark wie der schwächste Teil. In Hybridverfahren kommt außerdem der möglichst zufälligen Erzeugung des Sitzungsschlüssels grundlegende Bedeutung zu.
Aufbewahren von Schlüssel: Da sich kein Benutzer die Schlüssel wegen ihrer Länge auswendig merken kann, werden Schlüssel entweder durch ein zusätzliches Verschlüsselungspasswort abgesichert und möglichst sicher verwahrt. Oder eine Hälfte wird auf Chipkarte und die andere am PC gespeichert.

Schlüsselhinterlegung:
In großen Betrieben wird häufig die Möglichkeit eines Zweitschlüssels (key escrow) eingeführt, um beim Ausscheiden eines Mitarbeiters an dessen verschlüsselte Daten zu gelangen. Dabei entsteht zwangsläufig ein Konflikt zwischen dem Schutz der Privatsphäre des Mitarbeiters und den Interessen des Unternehmens. Viel gravierender sind die Konflikte allerdings, wenn Regierungen versuchen so Zugriff auf die Kommunikation von Firmen und Privaten zu erlangen.

Literatur

Neben den Kapiteln über kryptografische Verfahren und Protokolle sowie der Ablauforganisation, aus denen hier überblicksmäßig die wichtigsten Inhalte zusammengestellt sind, werden auch das Aufspüren von Hintertüren, die rechtlichen Rahmenbedingungen und die Standardisierung kryptografischer Systeme behandelt.

Im Buch wird bewusst auf die Vorstellung einzelner Programme zur Verschlüsselung verzichtet, da der Leser die Entscheidung über das richtige Softwarepaket oder Verfahren selbst anhand der Informationen im Buch treffen können soll.
Das Buch ist für Computerbenützer interessant, die sich eingehender mit dem Themenkreis Verschlüsselung beschäftigen wollen. Darüber hinaus bietet es allen, die in Unternehmen, Bildungseinrichtungen oder Organisationen für die Datensicherheit verantwortlich sind eine eingehende Orientierungshilfe in Sachen Datenschutzkonzepte.



Selke, Gisbert W.: Kryptographie - Verfahren, Ziele, Einsatzmöglichkeiten, 225 Seiten, O'Reilly Essentials 2000, ISBN 3-89721-155-6, ATS 212.-