Bernhard Esslinger
(Direktor Deutsche Bank,
Leiter Cryptography Competence Center;
Dozent Uni Siegen,
Institut für Wirtschaftsinformatik)

mit Unterstützung durch

Prof. Dr. Rüdiger Grimm, Anastasia Meletiadou
und Helge Hundacker
(Universität Koblenz, Forschungsgruppe
IT-Risk-Management, Institut für Wirtschafts-
und Verwaltungsinformatik)

Erstellt im Rahmen der Initiative
Deutschland sicher im Netz

Kryptologie für Jedermann

Kryptologie für Jedermann

Einführung in sichere Ver- und Entschlüsselungsverfahren

SAP Pocketseminar

Kryptoverfahren verstehen und richtig anwenden

Bernhard Esslinger – Kryptologie für Jedermann –
Einführung in sichere Ver- und Entschlüsselungsverfahren

SAP Pocketseminar

Eine Schriftenreihe der SAP AG

Bernhard Esslinger

Kryptologie für Jedermann

Einführung in sichere Ver- und Entschlüsselungsverfahren

Bei der Zusammenstellung der Texte, Verweise und Abbildungen wurde mit größter Sorgfalt vorgegangen; trotzdem ist ein vollständiger Fehlerausschluss nicht möglich. Die nachfolgende Dokumentation erfolgt daher ohne Gewähr für Richtigkeit und Vollständigkeit der gemachten Angaben, für deren Verifizierung allein der Anwender die Verantwortung trägt.

SAP übernimmt für aus der Verwendung dieser Dokumentation entstehende Schäden, gleich aus welchem Rechtsgrund, eine Haftung nur im Falle vorsätzlichen oder grob fahrlässigen Handelns; im übrigen ist die Haftung von SAP ausgeschlossen. SAP übernimmt keine Verantwortung für die Inhalte von Seiten oder Veröffentlichungen Dritter, auf welche wir durch Links verweisen.

50 085 038 (07/09)

Vorwort

Kryptologie bezeichnet die Wissenschaft zur Entwicklung von Ver- und Entschlüsselungsverfahren. Sie ist eine nahezu **allgegenwärtige Technik** geworden, die in viele Bereiche des täglichen Lebens eingedrungen ist, ohne dass wir uns dessen immer bewusst sind. Ob beim Bezahlen mit der EC-Karte, bei der Online-Bestellung, beim Bezahl-Fernsehen, bei der Verschlüsselung von E-Mails und Dateien, bei der digitalen Signatur, im WM-Ticket oder Handy – überall gibt es kryptographische Sicherheitsmechanismen. Viele Daten werden nur noch elektronisch gespeichert, übermittelt und verarbeitet. In dieser Form sind sie anfälliger als „klassische" Nachrichten in Papierform gegenüber Fälschungen und gegenüber unbefugten Einblicken von Dritten.

Diese Kryptofibel wendet sich an Endanwender, aber auch an Software-Entwickler, Software-Architekten und verantwortliche Entscheider in den Firmen, die sich neu mit dem Thema beschäftigen. Die Kryptofibel ist aktuell und anwendungsnah. Sie erfahren, wie sich die Kryptologie entwickelte und wo sie praktisch eingesetzt wird und können nach der Lektüre beurteilen, wofür welche Verfahren gut sind und welche Schlüssellängen wo in ihrem Unternehmen oder bei ihnen privat von Nöten sind (siehe Kapitel 3 bis 6).

Die Autoren haben jahrelange Erfahrung mit dem Thema Kryptologie, schulen Studenten, Mitarbeiter und Kunden darüber und verantworten den **adäquaten Einsatz** in Unternehmen (adäquat bedeutet: unter Berücksichtigung der Risiken, der Kosten und der Handhabbarkeit).

INHALT

1 Einleitung

Jahrtausendelang schon haben sich Menschen damit befasst, Geheimschriften zu erfinden und zu knacken. Früher wurden diese vor allem von Experten (Militärs, Diplomaten und Geheimdiensten) genutzt. Heute – im Zeitalter der Computertechnologie – ist auch die Privat- und Geschäftskommunikation von möglichen Lauschangriffen und Manipulationen bedroht.

Das Ziel der **Kryptographen** ist die Konstruktion von sicheren Verschlüsselungsverfahren, die dafür sorgen, dass nur der geplante Empfänger die verschlüsselte Nachricht wieder entschlüsseln und lesen kann. Die **Kryptoanalytiker** dagegen beschäftigen sich mit den Angriffen und dem Knacken dieser Verfahren. Ein guter Kryptograph sollte immer gleichzeitig ein guter Kryptoanalytiker sein, damit er seinen eigenen Konstruktionen kritisch gegenüberstehen kann. In der Wissenschaftswelt trägt das Zusammenspiel von kryptographischen Erfindungen und kryptoanalytischen Angriffen wesentlich zur Qualität der Verfahren bei. Wir halten daher nichts davon, dass Verfahren versteckt werden – aus Angst, sie könnten geknackt werden. Erst Verfahren, die die Analyse der Experten überstanden haben (und ihnen laufend weiter ausgesetzt sind), können als sicher angesehen werden.

In der modernen Internet-Zeit ist jede Form privater und geschäftlicher Kommunikation angreifbar. Im Internet werden deshalb verschiedene kryptographische Systeme eingesetzt, um einen sicheren Datenaustausch zu gewährleisten und vertrauliche Informationen zu schützen. Zu der **Verschlüsselung** kamen weitere Anforderungen wie die **Nachrichtenintegrität** (um zu erkennen, ob Nachrichten unbefugt verändert wurden) oder die **Authentifikation** von Benutzern (verlässliche Anmeldung) oder beispielsweise die Realisierung digitaler Zahlungsmittel wie EC-Karte und Online-Banking hinzu.

In diesem Leitfaden werden wir versuchen, die Grundlagen für jedermann verständlich darzustellen und etwas von der Faszination herüberzubringen, die dieses Gebiet umgibt.

Mit der Lernsoftware **CrypTool** (www.cryptool.de), die Sie kostenlos herunterladen können, können Sie die meisten Verfahren spielerisch nachvollziehen.

Neben den allgemeinen Verfahren und ihrer Geschichte werden in dem von der Uni Koblenz geschriebenen Kapitel 6 gesondert drei Anwendungsbeispiele besonders ausführlich erläutert:

- die SSL-Verschlüsselung und Authentisierung im Browser,
- die WLAN-Verschlüsselung,
- das Öffnen eines Autos mit dem Schlüssel per Funk.

Nach der Lektüre können Sie die Fachbegriffe einordnen und wissen beispielsweise, welche Schlüssellängen bei den aktuellen Verfahren angemessen sind oder warum und wie Sie ein gutes Passwort wählen.[1]

1 Herzlichen Dank an meine Studenten und besonders an Lisa und Lukas für das hilfreiche Gegenlesen. Ebenfalls ein herzliches Dankeschön an Prof. Dr. Rüdiger Grimm und seine Assistenten für die fristgerechte und professionelle Unterstützung, sowie an Klaus Schimmer und Tobias Essig, SAP AG, für die Überarbeitung der schriftlichen Fibel-Version.

2 Kryptologie in der Geschichte – vom alten Ägypten zur Wirtschafts-spionage

Die Kunst der Geheimschrift begann vor rund 4000 Jahren, als ein ägyptischer Schriftgelehrter Hieroglyphen durch veränderte Formen ersetzte. Später kamen **Steganographie** (das Verbergen von Nachrichten in einem harmlos erscheinenden Kontext, z.B. durch unsichtbare Tinten, Mikropunkte oder in Bildern), mit höherer Geschwindigkeit abgespielte Rundfunknachrichten, Buchstaben-Verfahren und Codes, mechanische Apparate und Computer als Verschlüsselungsinstrumente hinzu.[2]

Immer waren Militärs, Diplomaten und Geheimdienste an den Fortschritten interessiert. Heutzutage wird das Abhören und Entschlüsseln in großem Maßstab aber nicht nur bei Kriegshandlungen, sondern vor allem zur **Wirtschaftsspionage** eingesetzt, denn das Knacken einer gegnerischen Chiffre bedeutet immer einen Informationsvorsprung gegenüber der Konkurrenz und damit bares Geld.

In den Berichten unseres Verfassungsschutzes heißt es: „Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Forschungseinrichtungen, Wirtschaftsunternehmen und Betrieben. Die Ausforschungsaktivitäten zielen hierbei auf alle Entwicklungsstufen und hängen sehr vom technischen Stand des auftraggebenden Landes ab".

2 Unter http://www.cryptool.de/menu_zeittafel.de.html finden Sie unter der Überschrift „Zeittafel/Zeitreise durch Kryptographie und Kryptoanalyse" eine ausführliche Übersicht zur Geschichte der Kryptologie und weitere Links.

Am Bekanntesten dürfte das 1948 begonnene und von den USA, Großbritannien, Australien, Neuseeland und Kanada betriebene Echelon-System sein, das den weltweiten Satelliten-Verkehr komplett abhört. Vor allem aufgrund des Einsatzes des britischen Journalisten Duncan Campbell verfasste das EU-Parlament 2001 einen Bericht darüber[3], und rief explizit dazu auf, alle E-Mails mit sensiblen Daten zu verschlüsseln und zu signieren (z. B. mit dem Standard S/MIME).[4]

Im privaten Bereich hat sich diese Maßnahme bisher leider noch nicht durchgesetzt. Auf geschäftlicher Ebene werden dagegen viele Daten inzwischen ganz selbstverständlich verschlüsselt versendet: z. B. aus aktienrechtlichen Gründen die Daten für das Drucken der Bilanz zwischen der Aktiengesellschaft (AG) und der Druckerei oder aus Konkurrenzgründen die Konstruktionszeichnungen zwischen Zulieferern und Automobilhersteller. Dagegen setzen einzelne Branchen wie Anwälte und Steuerberater bei der elektronischen Kommunikation mit ihren (privaten) Mandanten bisher fast nie gesicherte E-Mails ein.

Zur Spionage werden natürlich weiterhin „erprobte" Maßnahmen wie das Filtern des Papiermülls, tote Briefkästen, doppelte Böden oder Bestechung eingesetzt, aber zunehmend auch ausgefeilte Hackermethoden und kryptoanalytische Verfahren. Weitere Informationen dazu finden Sie im Literaturverzeichnis, Teil C, „Links zu Wirtschaftsspionage u. ä. und Stellen, die dagegen behilflich sind".

Viele weitere historische Details finden Sie in den Büchern von David Kahn [Kahn 1996] und Friedrich Bauer [Bauer 2000] (siehe Literaturverzeichnis, Teil B, „Bücher für Erwachsene").

3 vgl. Schulzki-Haddouti, Christiane, „Echelon-Ausschuss verabschiedet Empfehlungen" auf: http://www.heise.de/tp/r4/artikel/9/9014/1.html

4 S/MIME (Secure/Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von E-Mails durch asymmetrische Kryptographie, der von allen modernen E-Mail-Clients (wie Outlook oder Thunderbird) unterstützt wird – aber nicht, wenn Sie Ihre E-Mail im Browser lesen.

3 Ein paar Grundbegriffe aus der Kryptologie

Im Folgenden werden die grundlegenden Begriffe erläutert und die Einbettung der Kryptologie in größere Zusammenhänge veranschaulicht. Dabei wird auch kurz auf den „Sonderfall" Social Engineering eingegangen.

3.1 Begriffserläuterungen – Was ist was?

Meist wird mit **Kryptologie** die Gesamtheit der **Kryptographie** und **Kryptoanalyse** bezeichnet, wobei die Kryptographie sich mit der Verheimlichung von Nachrichten und die Kryptoanalyse mit der Ermittlung von geheimen Nachrichten (Knacken) beschäftigt.[5] Die Kryptoanalyse versucht entweder den **Schlüssel**, der das Verfahren genau festlegt (parametrisiert), oder den ursprünglichen Klartext zu ermitteln.

Ein **Klartext** ist die Information, die der Empfänger erhalten soll. Ein **Geheimtext** oder **Chiffrat** ist ein verschlüsselter Klartext, der für Unbefugte nicht mehr entschlüsselbar sein soll. Als **Schlüssel** wird die wichtige Information bezeichnet, die benötigt wird, um einen Klartext in einen Geheimtext zu verschlüsseln oder um aus einem Geheimtext durch Entschlüsselung den Klartext zu gewinnen.

Den Vorgang der Verschlüsselung bezeichnet man auch als Chiffrierung, den der Entschlüsselung als Dechiffrierung. Die Begriffe **Chiffre** oder Code bezeichnen das Verfahren, das der Chiffrierung bzw. der Dechiffrierung zugrunde liegt.

5 Die Begriffe Kryptologie und Kryptographie sind aus den griechischen Wörtern „kryptos" (geheim), „logos" (das Wort, der Sinn) und „graphein" (schreiben) gebildet.

Folgende **Ziele** sollen durch den Einsatz der Kryptographie erreicht werden:

- **Vertraulichkeit/Geheimhaltung**
  Es ist zu verhindern, dass Unbefugte den Inhalt einer Nachricht erfahren (mitlesen).
- **Integrität**
  Für den Empfänger muss es nachprüfbar sein, dass die erhaltene Nachricht bei der Übermittlung nicht manipuliert wurde (Übertragungssicherheit).
- **Authentizität**
  Die Identität des Absenders einer Nachricht muss für den Empfänger nachprüfbar sein und umgekehrt (Fälschungssicherheit).
- **Nicht-Abstreitbarkeit/Verbindlichkeit**
  Man muss einem Teilnehmer an einer Kommunikation nachweisen können, dass er die entsprechenden Nachrichten versendet hat.

Wichtig sind diese Ziele (Anforderungen) beim Austausch von Informationen über öffentliche Netze, also besonders im Internet. Die ersten drei Anforderungen sind bei jeder Kommunikation interessant, die letzte z. B. bei der Erteilung von Aufträgen/Orders über das Internet.

Die folgende Abbildung soll verdeutlichen, dass man diese Ziele mit Hilfe der Kryptologie erreichen kann, welche Verfahren zur Kryptologie gehören und, dass diese Verfahren aufgrund ihrer Standardisierung Teil unseres Alltags geworden sind.

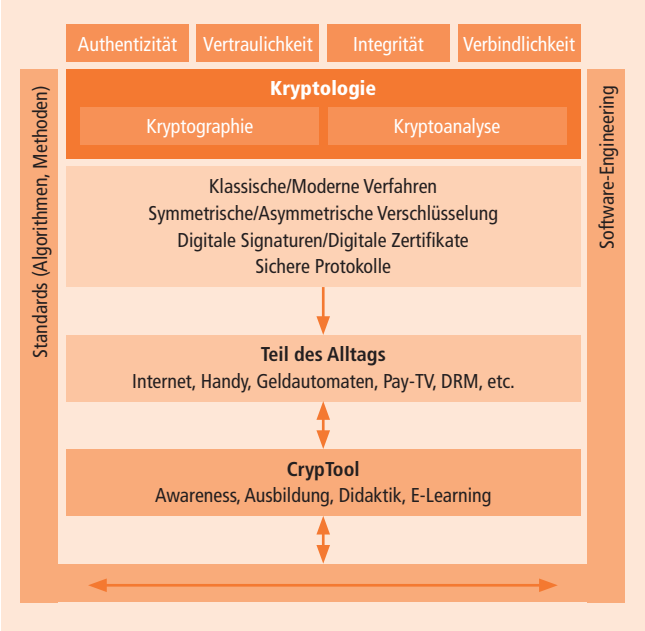


Abbildung 1: Ziele und Komponenten der Kryptologie

3.2 Angriffsszenarien

Unter einem Angreifer versteht man einen „unbefugten Dritten" (den „Bösen", wie Kinder sagen), der sich den **Klartext** und/oder den **Schlüssel** zu einer Information beschaffen will.

In der Kryptologie geht man davon aus, dass Angriffe gezielt erfolgen und Angreifer bewusst Schwächen nutzen. Der Weg, auf dem eine Nachricht vom Sender zum Empfänger gelangt, wird als **Kanal** bezeichnet. Häufig dient er als Angriffsziel.

Die **Angriffe** können dabei auf folgende Weise eingeteilt werden: Ein **aktiver** Angriff erfolgt zum Beispiel, wenn die verschlüsselte Nachricht abgefangen und gegen eine gefälschte Version ausgetauscht und als echt deklariert wird. Ein **passiver** Angriff bezeichnet den Vorgang des Abhörens bzw. das Entschlüsseln der Nachricht.

Ist der Kanal kryptographisch geschützt, erschließt sich einem Gegner der Inhalt der Nachricht nicht. In ähnlicher Weise können auch unbefugte Manipulationen an der Nachricht durch Einsatz kryptographischer Mittel für den Empfänger erkennbar gemacht werden.

Kleiner Exkurs: Social Engineering
Um an vertrauliche Informationen zu kommen, kann man sich auf die Kryptologie konzentrieren und Schwächen in den eigentlichen Verfahren oder in deren Implementierungen in Software ausnutzen. Social Engineering dagegen versucht bewusst, die psychologischen Schwächen von Menschen auszunutzen, um an gewünschte Informationen zu gelangen (siehe den Leitfaden „Faktor Mensch" [Fendl, Baumann, Schimmer 2005]).

3.3 Zusammenspiel von Kryptologie mit IT-Sicherheit und Risikomanagement

Als übergeordneter Begriff über Kryptographie und IT-Sicherheit wird aus **Unternehmenssicht** das Risikomanagement verstanden.[6] Risikomanagement beinhaltet neben der Risikoerkennung auch den transparenten Umgang mit Risiken. Dabei spielen die Kosten der Maßnahmen und der (mögliche) Schaden eine wesentliche Rolle. Da immer mehr geschäftskritische Daten in IT-Systemen verarbeitet werden, sind die Unternehmen dazu angehalten, eine Reihe von rechtlichen, regulatorischen und institutionellen Vorgaben zu berücksichtigen[7] (Basel II, MaRisk, Solvency II, KonTraG sowie Sarbanes Oxley Act (SOX), SAS 70 Typ I und Typ II und der Turnbull Act). Vor allem die Vorgaben zur Reduzierung des operationellen Risikos lassen sich mit kryptographischen Verfahren gut erfüllen.

6 Der Begriff „Risiko" kann aus den italienischen Worten „riscio" bzw. „risicare" abgeleitet werden („etwas wagen", „etwas aufs Spiel setzen").

7 vgl. Bitkom: Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, auf: http://www.bitkom.org/files/documents/Kompass_der_IT_28.06.06.pdf

Analog sollten sich auch **Privatnutzer** über ihr Risiko Klarheit verschaffen und sich fragen, was ihnen ihre Daten (Texte, Bilder) wert sind, welche Nachteile sie haben, wenn Fremde ihre Daten lesen, ins Internet stellen, verändern oder löschen, wenn ihr PC ausfällt oder fremd gesteuert wird und als Teil von verteilten Angriffen missbraucht wird (Bot-Netze[8]).

Während man die Kryptologie also einerseits als Teil von Risikomanagement und IT-Sicherheit sehen kann, kann sie auf der anderen Seite in die wissenschaftlichen Disziplinen der Mathematik und Informatik eingeordnet werden. Deren Erkenntnisse der Zahlen-, Komplexitäts- und Informationstheorie machen sich die Kryptologen ebenso zunutze wie den Einsatz von Computeralgorithmen.

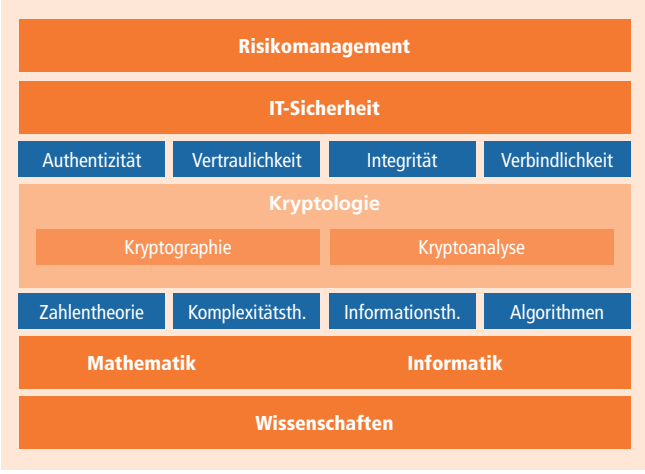


Abbildung 2: Einordnung der Kryptologie in übergeordnete Zusammenhänge wie IT-Sicherheit, Risikomanagement sowie Mathematik und Informatik

8 Ein Botnet oder Bot-Netz ist ein fernsteuerbares Netzwerk im Internet mit PCs, die aus untereinander kommunizierenden Bots bestehen. Die Kontrolle wird durch Würmer bzw. Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisung hin steuern.

Moderne Kryptologie (1):

4 Symmetrische Verschlüsselungsverfahren mit dem Computer

Im Folgenden wird die moderne symmetrische Kryptologie vorgestellt. Wenn Sie dieses Kapitel gelesen haben, werden Sie verstehen, wie **Computer** heute verschlüsseln und wie Daten sicher auf ihrer Festplatte abgespeichert werden können.

Außerdem werden wir versuchen, Ihnen die große Bedeutung von guten Passwörtern nahe zu bringen. Neben Erläuterungen zur Wahl guter Passwörter finden Sie auch Links zu weiteren Infos und zu unterstützenden Tools.

Von konventionellen, **symmetrischen** oder Secret-Key-Verfahren spricht man, wenn vom Sender der Information zum Chiffrieren und vom Empfänger zum Dechiffrieren der gleiche Schlüssel benutzt wird.

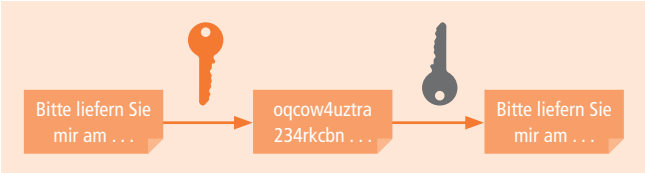


Abbildung 3: Schematische Darstellung der symmetrischen Verschlüsselung

Bemerkung: Schlüssel
Im einfachsten Fall besteht ein **Schlüssel** aus einem leicht zu merkenden Kennwort, wie beispielsweise „BieneMaja". Diese einfache Art eines Schlüssels wird oft auch als **Passwort** bezeichnet. Für moderne Ansprüche an die Sicherheit ist die Wahl eines solch einfachen Schlüssels wie „BieneMaja" allerdings nicht ausreichend, da er relativ leicht zu erraten ist oder durch systematisches Ausprobieren von Wörterbuchbegriffen (Brute-force-Attack) gefunden werden kann, wie wir in Kapitel 4.3 zeigen werden. Sichere Schlüssel können dagegen über eine Hashfunktion (vgl. Kapitel 5.5) aus dem Passwort generiert werden.

4.1 AES – ein modernes symmetrisches Verschlüsselungsverfahren

AES (Advanced Encryption Standard) und das inzwischen veraltete DES (Data Encryption Standard) sind die am häufigsten verwendeten symmetrischen Verschlüsselungsverfahren.

AES ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt sowie in Software bzw. Hardware implementiert werden. Es ist in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen (siehe http://de.wikipedia.org/wiki/Advanced_Encryption_Standard).

Auch wenn der Verschlüsselungsvorgang bei AES sehr kompliziert ist, so lassen sich sowohl in Software wie in Hardware sehr hohe Durchsätze erzielen: Rund 61 MB Daten/Sekunde verschlüsselt die Implementierung der verbreiteten Open-Source-Kryptobibliothek Crypto++ v. 5.2.1[9] auf einem PC. Sie können also den Inhalt einer CD derzeit in rund 11s unknackbar sicher verschlüsseln und kommen auch selbst nicht mehr dran, wenn Sie Ihr Passwort vergessen.

9 vgl. Crypto++, auf: http://www.eskimo.com/~weidai/benchmarks.html.

Das AES-Verfahrens können Sie in CrypTool mit der folgenden Menüfolge durchführen: **Ver-/Entschlüsseln** → Symmetrisch (modern) → Rijndael/AES:

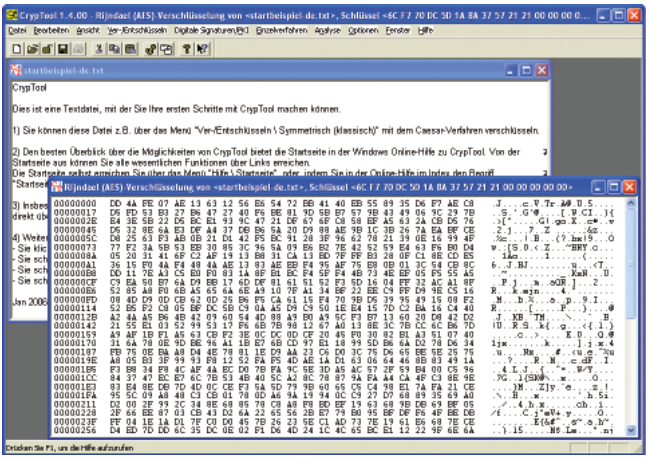


Abbildung 4: Ergebnis einer AES-Verschlüsselung mit CrypTool

AES wird vielfach verwendet: z.B. in den Verschlüsselungsstandards 802.11i und WPA2 für Wireless LAN sowie bei SSH[10] und dem Internetprotokoll IPsec. Außerdem wird der AES-Algorithmus zur Verschlüsselung diverser komprimierter Dateiarchive verwendet. Ebenfalls enthalten ist AES in der Software PGP (und natürlich auch GnuPG) oder TrueCrypt.

10 Secure Shell oder SSH ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf einem entfernten Computer einloggen und dort Programme ausführen kann.

4.2 Zufallszahlen – eine wichtige Komponente in der Kryptologie

Laut den Ausschreibungsanforderungen des NIST[11] soll die Sicherheit von AES für 20-30 Jahre gewährleistet sein. Für AES gibt es also derzeit auch für die Großrechenzentren der Geheimdienste keine Möglichkeit, das Verfahren zu knacken, wenn der Schlüssel geheim und **zufällig** gewählt ist.

Folgen von Zufallszahlen sollten deshalb folgende Eigenschaften aufweisen: Sie sind gleichverteilt[12], nicht vorhersagbar und nicht reproduzierbar.

4.3 Brute-force-Attack und Passwortangriffe

Wenn in Verschlüsselungsverfahren keine Schwächen bekannt sind und die beste bekannte Analysemethode das Durchprobieren aller möglichen Schlüssel ist (Brute-force-Attack), gelten sie unter Kryptologen als „ungebrochen". Eine gute Chiffre sollte einer vollständigen Schlüsselsuche oder Brute-force-Attack demnach widerstehen können.

Da Computer sehr schnell mit Bitmustern umgehen können und man zum Verschlüsseln sehr viel rechnen muss, sind Computer optimal für Verschlüsselungsverfahren geeignet. Dabei werden die vom Benutzer eingegebenen Buchstaben im ASCII- oder Unicode-Alphabet abgespeichert. Beim **ASCII-Code** erfolgt die Darstellung eines Zeichens im Computer als Folge von 8 Bit (= 1 Byte). Da ein Bit nur

11 Das National Institute of Standards and Technology (NIST) ist eine US-Behörde mit Aufgaben, die dem DIN (Deutsches Institut für Normung e. V.) vergleichbar sind. Jedoch sind die Ressourcen, die Ergebnisse und die Bedeutung des NIST um Größenordnungen bedeutender. Das NIST treibt z.B. die weltweite Standardisierung von kryptographischen Verfahren und veröffentlicht diese als U.S. Federal Information Processing Standard (FIPS).

12 Jeder mögliche Zustand tritt mit der gleichen Wahrscheinlichkeit ein, z. B. ist beim Münzwurf die Wahrscheinlichkeit für die Ereignisse Kopf oder Zahl jeweils gleich hoch (50 Prozent Wahrscheinlichkeit).

die zwei Werte 0 und 1 annehmen kann, kann man mit 8 Stellen genau 2^8 = 256 verschiedene Zeichen darstellen (Dualsystem oder Binärsystem). Jedem **Zeichen** ist also eine bestimmte achtstellige Folge von Nullen und Einsen zugeordnet. Man sagt, die Zeichen sind binär codiert. „Zeichen" sind nicht nur Ziffern und Buchstaben sondern auch Satzzeichen und Steuerzeichen.

Um den Zeitaufwand bei heutigen Schlüssellängen zu veranschaulichen enthält die folgende Tabelle eine Abschätzung unter der Annahme, dass man einen 56-Bit-Schlüssel in einer einzigen Sekunde knacken kann:

Schlüssellänge	Anzahl möglicher Schlüssel	Aufwand
56 Bit	7,2*10^16	1 Sekunde
64 Bit	1,8*10^19	4 Minuten
80 Bit	1,2*10^24	194 Tage
112 Bit	5,2*10^33	10^9 Jahre
128 Bit	3,4*10^38	10^{14} Jare
192 Bit	6,2*10^57	10^{33} Jahre
256 Bit	1,1*10^77	10^{52} Jahre
Alter des Universums		10^{10} Jahre

Abbildung 5: Aufwandschätzung zum Knacken per Brute-force-Attack von modernen symmetrischen Verfahren mit unterschiedlichen Schlüssellängen

In modernen symmetrischen Verfahren müssten also ca. 90 Bit Schlüssellänge zurzeit ausreichen, weil sich pro hinzukommendem Bit der Aufwand verdoppelt. Der Entschlüsselungsaufwand beträgt dann mehrere 1000 Jahre (vergleiche Kapitel 5.3 „Sichere Schlüssellängen – Vergleich RSA und AES", mit einer Gegenüberstellung symmetrischer und asymmetrischer Verfahren).

Bemerkung: Keine ausreichende Passwortlänge

Viele Benutzer setzen Tools ein, die moderne Verfahren mit hohen Schlüssellängen verwenden und fühlen sich sicher. Diese Verschlüsselungstools verlangen ein Passwort und leiten daraus z. B. über ein Hashverfahren (vgl. Kapitel 5.5) einen nur formal ausreichend langen Verschlüsselungsschlüssel her. Dabei wird außer Acht gelassen, dass die **Entropie**[13] eines 16 Zeichen langen Passwortes höchstens der von 80 Zufallsbit entspricht anstatt der für AES erwarteten 128 Bit.

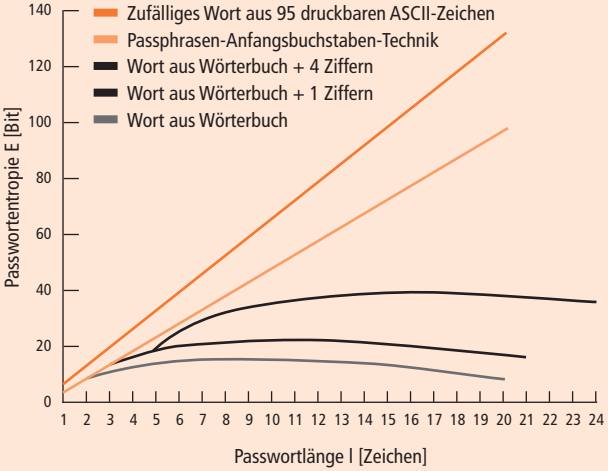


Abbildung 6: Entropie von Passwörtern unterschiedlicher Passwortstrategien [Marchal 2005]

Glauben die Benutzer den Marketingbroschüren, die oft nur die maximale Bitlänge nennen, wiegen sie sich also in einer falschen Sicherheit: Ein Angreifer würde sich das schwächste Glied in der Kette suchen und bei einer gegebenen Länge nur die Hashwerte aller über die Tastatur eingebbaren Passwörter ausprobieren statt aller

13 Maß für die Zufälligkeit möglicher Ergebnisse

möglichen. Starten würde er wahrscheinlich sogar damit, Wörter aus dem **Wörterbuch** auszuprobieren, da immer noch zu viele Benutzer kein **starkes Passwort** verwenden.

Ein Passwort wird erst dann stark, wenn man ein breites Spektrum an Möglichkeiten (Groß-, Kleinschreibung, Sonderzeichen, Zahlen) ausnutzt und die möglichst maximal vorgegebene Passwortlänge verwendet. Ein Passwort „ast" wird mit 100%-iger Wahrscheinlichkeit gefunden, wenn ein Angreifer bei 26 Kleinbuchstaben 26 x 26 x 26 = 17.576 Möglichkeiten durchprobiert. Nimmt der Anwender aber das Kennwort „der1.Ast", nutzt er ein wesentlich größeres Alphabet. Er erhöht also schneller die Anzahl möglicher Kombinationen, als wenn er nur ein längeres Passwort, das nur aus Buchstaben besteht, wählen würde.

Starke Passwörter kann man sich zum Beispiel aus den Anfangsbuchstaben eines gut zu merkenden Satzes zusammenbauen: Der Satz „Dieser Leitfaden ‚Kryptographie für Jedermann' lässt sich in rund 3 Stunden lesen." ergibt z. B. das Passwort: „DL,KfJ'lsir3Sl". Sensible Informationen sollten Passwörter von 12-20 Zeichen Länge haben.

Einige Betriebssysteme und Anwendungen akzeptieren dabei auch sehr lange Passwörter bzw. Passphrases mit bis zu 256 Zeichen im Gegensatz zu den oft üblichen maximal acht Zeichen bei der Passwortgenerierung. Testen Sie aus, wie viele Zeichen ihre Softwarelösung akzeptiert.[14] Denn eine hohe Komplexität ihres Passwortes durch den Einsatz von Sonderzeichen und durch eine gute Passwortlänge bietet einen starken Schutz vor Angriffen auf ihre Daten. Riskant ist auch, wenn Sie identische oder sehr ähnliche Passwörter für all ihre Konten wählen. Am sichersten sind Passwörter, die vollständig nach Zufallsprinzipien erstellt werden. Das geht mit Hilfe von

14 Leider gibt es Anwendungen [Sun Solaris bis Version 9, AOL in den USA in 2006, PHP bei crypt(), ...], die das Passwort intern abschneiden, während die Eingabemaske ein längeres Passwort zulässt. Hilfreich ist hier, die Sonderzeichen möglichst schon in der ersten Hälfte und nicht nur am Ende des Passwortes zu verwenden.

Passwort-Tools wie z.B. der Open-Source-Software Keepass. Voraussetzung ist, dass Sie die Passwörter auch in einem solchen Programm verschlüsselt speichern. Denn ohne Hilfe können Sie sich diese Kombinationen nicht merken.[15]

Falls man Teile eines Schlüssels kennt und nur einen kleineren Schlüsselraum vollständig durchsuchen muss, kann man jedes beliebige symmetrische Verfahren brechen. Mit CrypTool kann man dies leicht ausprobieren: Es wird z.B. angenommen, man kennt den Schlüssel bis auf beliebige 24 Bit. Das Programm entschlüsselt dann auf einem Pentium 4 alle 2^24 = 16 Millionen Möglichkeiten, berechnet die Entropie und findet – unter der Annahme, dass der Klartext ein normal-sprachlicher Text ist – mit erstaunlich hoher Erfolgsquote den richtigen Schlüssel und den richtigen Klartext in weniger als 3 Minuten. Die meisten Laien finden es sehr erstaunlich, dass ein Computer, der Textinhalte nicht versteht, den richtigen Text allein anhand einer statistischen Kennzahl (Entropie) erkennt.

4.4 Festplatten-Verschlüsselung in der Praxis

Wenn Privatanwendern daran liegt, dass ihre Daten nicht für jedermann einsehbar sind, können sie zur Verschlüsselung von Festplatten, Teilen davon oder Wechseldatenträgern die kostenlose Open-Source-Software TrueCrypt nutzen. **TrueCrypt** läuft unter Microsoft Windows und Linux und bietet eine Verschlüsselung mit den Algorithmen AES, Blowfish, Twofish, CAST5, Serpent und Triple-DES. Homepage: http://www.truecrypt.org.

Firmen dagegen verwenden kommerzielle Systeme mit umfangreichem Support, mit denen man auch auf einem Datei-Server die Daten unterschiedlicher Benutzer sichern kann. Dabei ist sowohl die Übertragung als auch die Abspeicherung verschlüsselt. Nutzer oder Nutzergruppen können dabei jeweils verschiedene Schlüssel verwenden.

15 Vergleiche http://keepass.info/ und den PC-Welt-Artikel "Know-How: Das perfekte Passwort" (http://www.pcwelt.de/know-how/sicherheit/81780).

4.5 Nachteile symmetrischer Verfahren

Der große Nachteil symmetrischer Verschlüsselungsverfahren liegt im Schlüsselaustausch: Der Benutzerschlüssel beim Ver- und Entschlüsseln muss derselbe sein. Sender und Empfänger müssen also über denselben Schlüssel verfügen. Dies wiederum setzt voraus, dass beide den Schlüssel **vorher** ausgetauscht haben, was aber nur im unverschlüsselten Klartext erfolgen kann. Besonders problematisch ist das, wenn der Schlüssel mit sehr vielen und nicht gut bekannten Kommunikationspartnern über öffentliche und daher ungesicherte Netze ausgetauscht werden muss.

Rein symmetrische Verfahren werden in der Praxis hauptsächlich genutzt, um lokale Festplatten zu verschlüsseln oder Datenträger, bei denen alle Datenzugriffe über ein zentrales System laufen zu schützen, da dieses System den Schlüssel selbst generiert und mit keinem anderen System austauscht. **Zur Datenübertragung benutzt man asymmetrische Verfahren** (siehe Kapitel 5) **oder eine Kombination aus symmetrischen und asymmetrischen Verfahren (Hybridverschlüsselung**).

4.6 Zusammenfassung

Moderne Verschlüsselungsverfahren nutzen leistungsfähige Computer. **Die geheime Information, die zur Verschlüsselung und Entschlüsselung dient, nennt man Schlüssel**. Bei symmetrischen Verfahren wird zum Chiffrieren und Dechiffrieren der gleiche Schlüssel benutzt – ihn über offene Netze auszutauschen birgt Gefahren.

Das aktuell sichere symmetrische Verschlüsselungsverfahren heißt AES und wird mit einer Schlüssellänge von mindestens 128 Bit eingesetzt: Damit ist man nach heutigem Kenntnissstand auf mindestens 20-30 Jahre sicher vor Brute-force-Angriffen.

Hashverfahren sind ebenso wie Zufallszahlengeneratoren eine wichtige Komponente für die Anwendung kryptographischer Verfahren.

Moderne Kryptologie (2):

5 Asymmetrische Verfahren – nicht nur zur Verschlüsselung

Im Folgenden werden Elemente der modernen asymmetrischen oder Public-Key-Kryptologie vorgestellt und weitere Einsatzmöglichkeiten der Kryptologie für die Computer- und Netzwerksicherheit besprochen.

Wenn Sie dieses Kapitel gelesen haben, werden Sie verstehen, welche Schlüssellängen sicher sind, wie Daten [per E-Mail oder mit dem Browser (siehe auch Kapitel 6.1)] sicher übertragen werden, warum asymmetrische Verschlüsselung eine Lösung für die Schlüsselverteilung in offenen Netzen bietet und wie man mit Hilfe von elektronischen Zertifikaten sicher prüfen kann, mit wem man gerade kommuniziert.

Bei symmetrischen Chiffren ist der Verschlüsselungsschlüssel direkt oder indirekt identisch zum Entschlüsselungsschlüssel. **In einem asymmetrischen Verfahren hat jeder Benutzer zwei Schlüssel** (ein Schlüsselpaar): Diese zwei Schlüssel ergänzen sich, aber bei genügend großer Schlüssellänge kann ein Dritter nicht einen aus dem anderen herleiten. Den ersten Schlüssel kann der Empfänger als den Verschlüsselungsschlüssel (öffentlicher Schlüssel) veröffentlichen. Wenn ich eine Nachricht verschlüsselt erhalten will, gebe ich dem Absender meinen öffentlichen Schlüssel. Mit meinem privaten Schlüssel (Entschlüsselungsschlüssel), den ich gegenüber jedem geheim halte und nicht weitergebe, kann nur ich die Nachricht entschlüsseln.

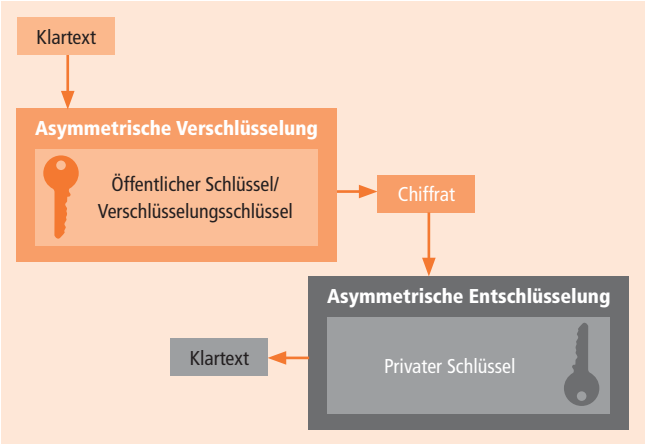


Abbildung 7: Asymmetrische Verschlüsselung (nur der Empfänger kann entschlüsseln)

5.1 RSA – ein asymmetrisches Kryptoverfahren

RSA ist ein asymmetrisches Kryptosystem, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. 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 nicht oder nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

Anwendungsgebiete:

- Internet- und Telefonie-Infrastruktur: X.509-Zertifikate[16]
- Übertragungs-Protokolle: IPSec, TLS, SSH, WASTE
- E-Mail-Verschlüsselung: PGP, S/MIME
- Kartenzahlung: EMV.

16 X.509 ist ein Telekommunikationsstandard für eine Public-Key-Infrastruktur und derzeit der wichtigste Standard für digitale Zertifikate.

5.2 Vorteil der asymmetrischen Verschlüsselung

Der Vorteil asymmetrischer Verfahren gegenüber symmetrischen Verfahren besteht in der Vereinfachung der Schlüsselverteilung. Es ist möglich, dass auch bei einer großen Anzahl von Kommunikationspartnern, wie beispielsweise im Internet, jeder mit jedem sicher kommunizieren kann. Die Ursache liegt in der viel kleineren Anzahl benötigter Schlüssel.[17] Durch Public-Key-Systeme entfällt auch die Notwendigkeit, den Schlüsselaustausch gegen Abhörversuche zu härten, da nur der öffentliche Schlüssel ausgetauscht werden muss.

Falls kein Zweifel über die Identität des Partners besteht und die Nachricht nicht von einem Dritten verändert werden kann, ist der Schlüsselaustausch beim Public-Key-Verfahren problemlos. Ansonsten werden öffentliche Schlüssel mit Hilfe von sogenannten Zertifikaten verteilt. Dass man den Zertifikaten vertrauen kann, liegt an sogenanten Public-Key-Infrastrukturen (siehe Kapitel 5.7).

5.3 Sichere Schlüssellängen – Vergleich RSA und AES

RSA-Schlüssellängen von 1620 Bit gelten heute als sehr sicher – als adäquat sicher gilt das symmetrische Verfahren AES mit einer Schlüssellänge von 128 Bit.[18] Da man bei RSA nicht alle möglichen Schlüssel durchprobiert, sondern aufgrund der mathematischen Problemstellung dahinter eher das mathematische Problem angeht, müssen asymmetrische Schlüssel länger sein als die der modernen symmetrischen Verfahren, wo man keine besseren Ansätze als Brute-force-Angriffe kennt (vgl. Kapitel 4.3 „Brute-force-Attack und Passwortangriffe“).

17 Die Anzahl der benötigten Schlüssel wächst nun linear statt quadratisch mit der Anzahl der Kommunikationsteilnehmer.

18 Verschlüsselungstechnologien ändern sich kontinuierlich. Die angegebenen Werte spiegeln deshalb nur den Status Quo wider. Die aktuellen Empfehlungen finden sich auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI) unter www.bsi.de.

Symmetrischer Schlüssel	RSA	Angriffsdauer
56 Bit	430 Bit	5 Minuten
80 Bit	760 Bit	600 Monate = 50 Jahre
98 Bit	1020 Bit	3 Mill. = 3 x 10^6 Jahre
128 Bit	1620 Bit	10^{16} Jahre

Abbildung 8: Gegenüberstellung adäquat sicherer Schlüssellängen für symmetrische und asymmetrische Verfahren (AES bzw. RSA)[19]

Die Werte in der obigen Abbildung sind Schätzwerte unter der Annahme, dass man einen 56 Bit DES-Schlüssel in 5 Minuten knacken kann. Sie antizipieren den Fortschritt und die nötigen Aufwände: In grober Näherung und in Relation zueinander treffen sie zu.

5.4 Das beste aus beiden Welten – Hybride Verschlüsselung

Hybridverfahren verbinden die Vorteile der symmetrischen und asymmetrischen Verfahren: schnelle symmetrische Verschlüsselung der Nachricht, sichere asymmetrische Schlüsselverteilung und gegenseitige Authentisierung. Dabei wird ein symmetrischer Schlüssel (Session-Key) zufällig erzeugt. Die (relativ lange) Nachricht wird dann damit symmetrisch verschlüsselt. Der (relativ kurze) Session-Key wird mit dem asymmetrischen Verfahren verschlüsselt und beides wird übertragen. Diese „digitalen Umschläge" sind weit verbreitet in der Praxis. Deshalb wurden dafür Standardformate wie PKCS#7 definiert, die z. B. in sicheren E-Mails (nach dem S/MIME-Standard) zum Einsatz kommen. PGP verwendet ebenfalls hybride Verfahren.

19 RSA Bulletin, auf: ftp://ftp.rsasecurity.com/pub/pdfs/bulletn13.pdf

5.5 Hashverfahren – digitale Fingerabdrücke

Hashverfahren sind ebenso wie Zufallszahlen (vgl. Kapitel 4.2) unbedingt notwendige Komponenten von kryptographischen Verfahren. Eine Hashfunktion ist eine (mathematische) Funktion, die eine Eingabe beliebiger Länge erhält und einen Funktionswert (Hashwert) einer festen Länge (meist 128 oder 160 Bit) zurückliefert. Sie liefert zu einer (langen) Eingabe, zum Beispiel zu einem Text, eine kurze Ausgabe (den Hashwert des Textes). Dieser Hashwert ist eine Art Fingerabdruck der Eingabe. Das ist z.B. dann sinnvoll, wenn man zwei große ähnliche Dateien vergleichen will: Anstatt alle Seiten eines Textes durchzusehen, ob auch wirklich jeder Buchstabe gleich ist, berechnen und vergleichen wir nur die kurzen Hashwerte der beiden Dokumente, und sehen sofort, ob diese beiden gleich oder verschieden sind.

Hashfunktionen werden in der Kryptologie somit verwendet, um die Integrität einer Nachricht sicherzustellen. Außerdem werden von Passwörtern nur Hashwerte abgelegt,[20] damit ein Administrator durch Auslesen der Passwortdatei nicht direkt Kenntnis von den Passwörtern erlangt. Die wichtigste Anwendung von Hashverfahren sind die elektronischen Signaturen.

5.6 Elektronische Signaturen – die Unterschriften im Internetzeitalter

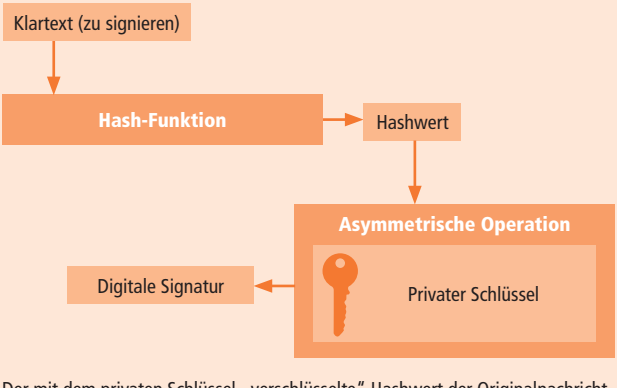
Die elektronische **Authentizität** einer Nachricht / eines Dokuments ist also erfüllt, wenn die empfangene Nachricht wirklich vom angegebenen Absender ist und nicht verändert wurde. Die Authentizität wird normalerweise durch eine Unterschrift bestätigt (zudem kommt im juristischen Sinne der damit bekundeten Willenserklärung eine besondere Bedeutung zu).

20 Die optimale Vorgehensweise unter Berücksichtigung von so genannten Salzwerten und Iterationen (zum Beispiel, um Wörterbuchangriffe drastisch zu erschweren) wird in dem Standard PKCS#5 von RSA Labs beschrieben (siehe http://www.ietf.org/rfc/rfc2898.txt, Version 2.0, 2000).

Wesentliche Anforderungen an eine digitale Unterschrift sind:

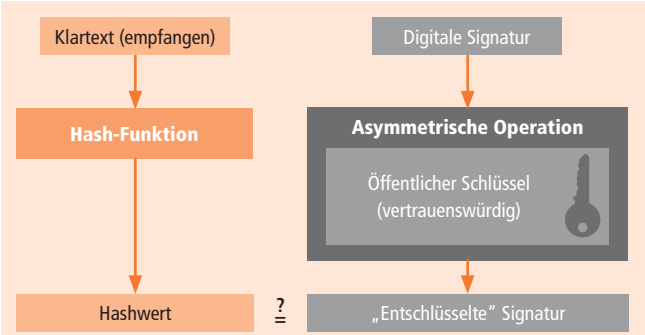
- Nur der rechtmäßige Absender eines Dokuments kann die Unterschrift erzeugen.
- Der Empfänger kann die Unterschrift zweifelsfrei prüfen.
- Die Unterschrift gilt nur im Zusammenhang mit dem gegebenen Dokument.

Realisiert wird dies damit, dass die Software des Absenders einen Hashwert des Dokuments berechnet und dann den Hashwert mit seinem privaten Schlüssel unterschreibt. Mit Hilfe des öffentlichen Schlüssels kann jeder dann die Integrität und die Urheberschaft des empfangenen Dokuments überprüfen.



Der mit dem privaten Schlüssel „verschlüsselte" Hashwert der Originalnachricht ist die Signatur.

Abbildung 9: Signieren – Erzeugen einer elektronischen Signatur



Die Verifikation ist ein Vergleich zwischen dem erneut berechneten Hashwert und der „entschlüsselten" Signatur (beim RSA-Schema).

Abbildung 10: Validieren – Prüfen einer elektronischen Signatur

Rechtlich wird innerhalb der EU zwischen einfachen, fortgeschrittenen und qualifizierten Signaturen unterschieden. Kryptographisch gleichwertig von den eingesetzten Verfahren her sind fortgeschrittene und qualifizierte Signaturen. Qualifizierte Signaturen sind rechtlich einer händischen Unterschrift gleichgestellt. Aufgrund des für viele Zwecke überdimensionierten formalen Aufwandes für qualifizierte Signaturen sind die **fortgeschrittenen Signaturen** (selbst in den Behörden) heute viel verbreiteter.

Aufgrund der rechtlichen Folgen bei der qualifizierten Signatur geben das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur eine Übersicht „über die Algorithmen und zugehörigen Parameter, die (…) als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt" heraus.[21] Ähnliche Zusammenstellungen zu den einzuhaltenden kryptographischen Sicherheitsstandards erstellen auch die Finanzinstitute für ihre Anwendungen.

21 vgl. Verordnung zur elektronischen Signatur, auf: http://www.bundesnetzagentur.de/media/archive/5264.pdf oder verständlicher aufbereitet auf den Rechtsseiten zur Digitalen Signatur: http://www.signaturrecht.de/sigv/anlage1.html

5.7 Infrastrukturen für die öffentlichen Schlüssel

Da es wichtig ist, dass der öffentliche Schlüssel wirklich dem Autor zugeordnet werden kann, braucht man so genannte **Zertifikate**, die in einer Public-Key-Infrastruktur (PKI) erstellt werden und die dem Nachweis dienen, dass ein öffentlicher Schlüssel zu einer angegebenen Person, Institution oder Maschine gehört. Weiterhin wichtig für die Gesamtsicherheit einer Signatur ist das Hashverfahren, da man ja nicht das Gesamtdokument unterschreibt, sondern nur den Hashwert (Fingerabdruck). Zertifikate werden z. B. von öffentlichen Trustcentern und von Internet-Providern herausgegeben. Die mengenmäßig größten PKIs (Trustcenter) geben ihre Zertifikate aber an geschlossene Benutzergruppen heraus (Militär, Firmen wie Siemens, Microsoft, Boeing, Deutsche Bank oder Behörden). Diese PKIs vernetzen sich untereinander z. B. in Form gegenseitigen Vertrauens wie der **European Bridge-CA** (http://www.bridge-ca.de). Dadurch kann z. B. ein Siemens-Mitarbeiter innerhalb von 5 Minuten erreichen, dass er eine sichere E-Mail an einen Mitarbeiter der Deutschen Bank versendet, mit dem er bisher nie kommuniziert hat. Der Empfänger kann sowohl die Validierung der fortgeschrittenen Signatur als auch die Entschlüsselung vornehmen (natürlich geht das in beide Richtungen so unkompliziert).

5.8 Ein Blick in die Quantenzukunft

Quantencomputer und **Quantenkryptographie** sind moderne Entwicklungen aus der Forschung.

Die **Quantenphysik** beschäftigt sich mit den Eigenschaften von Mikroobjekten: Ihr typisches Untersuchungsobjekt sind Atome, Elektronen, Protonen und Neutronen. Oft bezieht sich der Begriff Quanten auf kleinste Energieeinheiten, die von einem System auf ein anderes übertragen werden.

Diese Elementarteilchen können Träger von Quanteninformationen sein, die unter Beobachtung genau einen von zwei wohl unterscheidbaren Basiszuständen annehmen (vereinfacht 0 und 1). Ein solches Zweizustandssystem wird Quantenbit oder Qubit genannt. Qubits können – außerhalb der Messung – auch jeden Wert zwischen 0 und 1 annehmen (Superposition) und miteinander verschränkt sein. Die Qubits und dazu gehörende Quantengatter werden benutzt, um Computer zu modellieren, die bei bestimmten Problemen theoretisch fast beliebig schnell rechnen können. Der bislang schnellste reale „**Quantencomputer**" kann mit 7 Qubits gerade mal die Zahl 15 in seine Faktoren 3 und 5 zerlegen. Würden sich deutlich größere Qubit-Systeme stabil bauen lassen, wäre das Kryptoverfahren RSA, das heute die meisten Kommunikationsformate und -protokolle sichert, auch mit hohen Schlüssellängen nicht mehr sicher (z. B. schätzte Nguyen von der TU München, dass ein fiktiver Quantencomputer mit 2047 Qubits und einer Leistung von 10^7 Operationen/sec in 80 Tagen eine 1024 Bit RSA-Zahl faktorisieren könnte)!

Die Fortschritte der Quantenphysik führen aber nicht nur dazu, dass die vorhandenen Verfahren unsicherer werden. Gleichzeitig werden sie auf dem Gebiet der **Quantenkryptographie** dazu genutzt, den Schlüsselaustausch unüberwindlich zu machen: Die Sicherheit der Quantenkryptografieverfahren entsteht dadurch, dass ein Angreifer, der die Schlüsselübertragung abhört, fast immer bemerkt wird. Stellt man fest, dass die Übertragung belauscht wurde, verwirft man den übertragenen Schlüssel und beginnt die Schlüsselerzeugung und -übertragung neu. Mit Quanteneffekten kann man dabei Zufallszahlen erzeugen, die man in herkömmlichen symmetrischen Verfahren als Session-Key verwenden kann. Es ist also ein sehr sicheres Übertragungsverfahren, aber auch ein sehr störanfälliges und in der Reichweit beschränktes Verfahren (der Rekord von Weinfurter/Zeilinger liegt bei 144 km)[22] .

Für alle, die sich mit dem RSA-Verfahren auf die sichere Übertragung der Daten verlassen müssen, trifft es sich gut, dass die Realisierung der Quantenkryptographie bisher sehr viel schneller vorankommt als die von Quantencomputern.[23]

22 Siehe die Heise-Meldung vom 4.6.2007 „Quantenkryptographie mittels Teleskop" (http://www.heise.de/newsticker/meldung/90586).

23 Auf der Webseite des Instituts für Theoretische Physik der Universität Wien illustrieren die so genannten „Quanten-Gickse" anschaulich, was es mit Quantenzuständen und dem Messprozess in der Quantentheorie auf sich hat: http://homepage.univie.ac.at/Franz.Embacher/Quantentheorie/gicks/.

6 Ausgewählte Anwendungen detailliert betrachtet

In den folgenden drei Beispielen wird gezeigt, wie elektronische Anwendungen mithilfe kryptographischer Verfahren abgesichert werden. In jedem Beispiel erklären wir das Ziel der Verschlüsselung, erläutern den technischen Hintergrund, besprechen im Detail den Ablauf der Anwendung mit ihrer Verschlüsselung und diskutieren Stärken und Schwächen des Verfahrens.

Die Beschreibung der kryptografischen Anwendungen dieses Kapitels und einiger weiterer Beispiele (Protokolle, GSM, Geldauszahlungsautomaten, kontaktlose RFID-Tickets) wird in einem Arbeitspapier des Instituts für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau weitergepflegt und dort stets aktuell zum Download bereitgehalten [Grimm, Hundacker, Meletiadou 2006].

6.1 SSL (Secure Sockets Layer), das Sicherheitsprotokoll des World Wide Web

6.1.1 Anwendung

Anwendungen im Internet wie E-Mailing, Datenübertragung und das World Wide Web nutzen das standardisierte Verfahren TCP/IP („Transmission Control Protocol", „Internet Protocol") zum Transport ihrer Anwendungsdaten. TCP-Transportdaten sind unverschlüsselt. Also kann sie jeder, der an irgendeiner Stelle Zugang zu dem Transportweg hat, unbemerkt mitlesen und sogar konsistent verändern. Zugang zum Transportnetz hat zum Beispiel jeder Router[24]-Administrator. Da zwischen Sender- und Empfangsrouter durchschnittlich 20-30 Zwischenrouter liegen, gibt es sehr viele Nutzer, die unberechtigt auf ihren Datenverkehr zugreifen könnten. Die Lösung liegt darin, dass

24 Ein Router ist ein Vermittlungsrechner, der mehrere Rechnernetze koppelt. Bei ihm eintreffende Netzwerk-Pakete eines Protokolls werden analysiert und zum vorgesehenen Zielnetz weitergeleitet oder „geroutet".

ein Anwender seine Daten nur verschlüsselt auf den Transportweg gibt. Allerdings braucht der vorgesehene Empfänger dann die richtigen Entschlüsselungsschlüssel („Ende-zu-Ende-Verschlüsselung").

Das SSL ist eine Funktionsschicht zum verschlüsselten Austausch von Anwendungsdaten über das TCP-Transportsystem. Um die Anwendungen bei der Verschlüsselung zu entlasten, bietet es eine einheitliche Schnittstelle zwischen dem Anwendungssystem und dem Transportsystem. Statt also den Anschluss an das Transportsystem direkt zu programmieren, programmiert der Anwendungsentwickler den Anschluss an das SSL. Die Programmanschlüsse von SSL enthalten dabei eine ganze Reihe starker Verschlüsselungsfunktionen.

Typische Nutzer von SSL sind Webbrowser und Web-Server. Das Protokoll https des World Wide Web ist das um den SSL-Service erweiterte Protokoll http. Die Nutzung von SSL im World Wide Web wird durch ein Schlosssymbol im Browserfenster angezeigt, zum Beispiel beim Homebanking oder in Online-Shops.

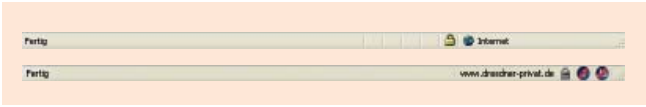


Abbildung 11: SSL-gesicherte Seite im Internet (mit den Browsern Microsoft Internet Explorer und Mozilla Firefox)

6.1.2 Ziel von SSL

Das Ziel von SSL ist die Herstellung eines sicheren Transportkanals zwischen Internetanwendern. „Sicher" bedeutet, dass die Vertraulichkeit der Daten, deren Unverletztheit und die Authentizität der Kommunikationspartner gewährleistet werden. Insbesondere signalisiert der SSL-Anschluss eines Browsers, dass ein Web-Server, der SSL unterstützt, der richtige ist, und dass alle Daten zwischen Browser und Server verschlüsselt sind und auf dem Transportweg nicht verändert wurden.

6.1.3 Eingesetzte Algorithmen

Im SSL-Protokoll verabreden die Anwendungspartner, welche Verschlüsselungsverfahren sie einsetzen wollen. Dabei tauschen sie über ein asymmetrisches Verschlüsselungsverfahren symmetrische Schlüssel aus und verschlüsseln anschließend ihre Daten mit diesen symmetrischen Schlüsseln. In der Regel kommen die Verschlüsselungstechniken RSA oder Diffie-Hellman für den Schlüsselaustausch, und Triple DES, AES oder IDEA (128 Bit) für die symmetrische Phase zum Einsatz.

6.1.4 Ablauf

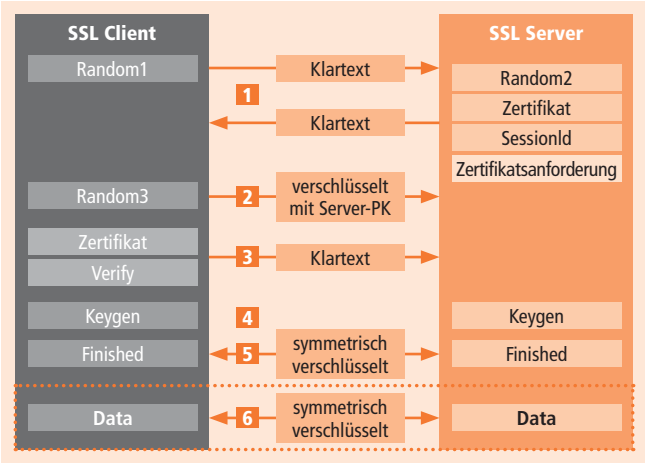


Abbildung 12: SSL-„Handshake"-Protokoll

Schritt 1: Das SSL-Verfahren kann von jedem der beiden Anwendungspartner, im Falle des WWW also sowohl vom Browser als auch vom Server, angestoßen werden. Die „Hello"-Phase, in Abb. 11 als Schritt 1 dargestellt, eröffnet das so genannte „SSL-Handshake--Protokoll", in dessen Verlauf der Server sich gegenüber dem Browser (SSL-Client) authentifiziert und beide Partner die Verschlüsselungsverfahren und die symmetrischen Schlüssel für die spätere Datenphase (Schritt 6) austauschen.

Der Browser sendet hierzu dem Server in seiner „Client-Hello"-Nachricht eine Liste kryptographischer Algorithmen und Schlüssellängen, die er selbst beherrscht. Der Server wählt die Verfahren aus, die er ausführen kann und sendet diese Auswahl zurück oder, falls er kein angebotenes Verfahren kennt, antwortet er mit einer „Handshake Failure"-Nachricht, die die Kommunikation zwischen Browser und Server beenden würde. Typischerweise wird in dieser Phase das symmetrische Verfahren AES mit einer als sicher geltenden Schlüssellänge von 256 Bit ausgewählt, das heutzutage alle Server und Browser beherrschen.

Das SSL-Programm ist entweder in den Browser integriert, oder es ist in einen externen Prozess in der lokalen Umgebung des Browsers ausgelagert, über den der Browser alle Kommunikation ins Web leitet. Ein extern ausgelagerter SSL-Prozess wird „SSL-Proxy" genannt.

Im unmittelbaren Anschluss an sein „Server-Hello" sendet der Server ein Zertifikat seines öffentlichen Schlüssels, der für die nun folgende asymmetrische Phase gebraucht wird. Abschließend werden in der „Hello"-Phase zwei Zufallszahlen ausgetauscht, von denen jeder der beiden Partner eine erzeugt und dem anderen mitteilt.

Schritt 2: Während die beiden ersten Zufallszahlen im Klartext ausgetauscht werden, übermittelt der Browser dem Server eine dritte Zufallszahl, die mit dem öffentlichen Schlüssel, den er dem Zertifikat des Servers entnommen hat, verschlüsselt ist. Der Browser kann also sicher sein, dass nur der berechtigte Inhaber des zugehörigen privaten Schlüssels und damit der im Zertifikat bestätigte Server die dritte Zufallszahl bekommt.

Schritt 3 wird nicht immer ausgeführt. Er dient der Authentifizierung des Browsers gegenüber dem Server. In höherwertigen Anwendungen, zum Beispiel in einer Homebanking-Anwendung nach dem Standard HBCI, sind Browser mit einem Bankenzertifikat ausgestattet, das an dieser Stelle zum Einsatz kommt.

In Schritt 4 erzeugen nun Browser und Server, jeder auf seiner Seite, nach einem von SSL für alle Teilnehmer festgelegten Verfahren einen gemeinsamen Satz von sechs symmetrischen Schlüsseln. Sie kommen zum selben Ergebnis, weil sie dieselben Zufallszahlen als Parameter einsetzen. In die Schlüsselerzeugung gehen alle drei Zufallszahlen ein, so dass erstens beide Partner an der Entwicklung der Schlüssel beteiligt sind, und zweitens kein Dritter den Schlüsselsatz erzeugen kann (die dritte Zufallszahl wurde ja vom Browser erzeugt und dem Server asymmetrisch verschlüsselt zugestellt).

In den Schritten 1-4 des „SSL-Handshake" tauschen Client und Server auch gegenseitig Nachrichten darüber aus, dass der Schlüsselaustausch und die Authentifizierung erfolgreich waren.

Schritt 5 ist gewissermaßen der Probelauf für die Datenphase. Die nun ausgetauschten „Finished"-Nachrichten sind die ersten Nachrichten, die mit Hilfe der ausgehandelten Parameter verschlüsselt werden. Die Empfänger prüfen jeweils, ob der Inhalt korrekt ist.

Schritt 6: Die „Handshake"-Phase ist nun abgeschlossen und die verabredeten Verfahren und Schlüssel können sicher in der folgenden Datenphase eingesetzt werden.[25]

25 Eine gut lesbare Darstellung des SSL-Protokolls findet sich auch bei (Esslinger, Müller 1997).

6.1.5 Stärken

Der große Vorzug des SSL-Protokolls liegt darin, dass Anwendungsdaten ohne weiteres Zutun der Nutzer von den Anwendungsinstanzen automatisch verschlüsselt werden und mit einem Unverletztheitskennzeichen versehen sind. Das erkennt der Nutzer daran, dass eine Web-Verbindung am Anfang ihrer URL-Adresse den Protokollnamen „https" statt „http" erhält. Alle Browser zeigen außerdem bei der Adresse und im Rahmen des Browserfensters ein deutlich sichtbares Symbol eines Bügelschlosses (Abbildung 11). Das zeigt dem Nutzer an, dass die ausgetauschten Daten nicht von dritter Seite mitgelesen, verändert, gelöscht oder in der Reihenfolge verändert werden können. Moderne Browser hinterlegen zusätzlich die Adresszeile mit einer Farbe.

Optional können sich beide Partner noch sicher authentifizieren. Dazu braucht der betreffende Partner (also der Server und gelegentlich zusätzlich auch der Browser) nur anfänglich sein Zertifikat einzustellen, und dann läuft die Authentifizierung jedes Mal automatisch ab. Der Nutzer eines Browsers, bzw. der Administrator eines Servers kann hierzu über die Sicherheitseinstellungen eigene Zertifikate, die er zuvor von einer Zertifizierungsstelle erworben hat, importieren.

Um das Server-Zertifikat zu prüfen, klickt der Nutzer im Browserfenster das Schloss an und erhält die in der Abbildung 13 dargestellte Seiteninformation. Bei einem weiteren Klick auf den Reiter „Sicherheit" wird das Zertifikat gezeigt. Es ist wichtig, dass der Nutzer die Organisation, die als Zertifikataussteller bezeichnet ist, kennt und ihr vertraut.

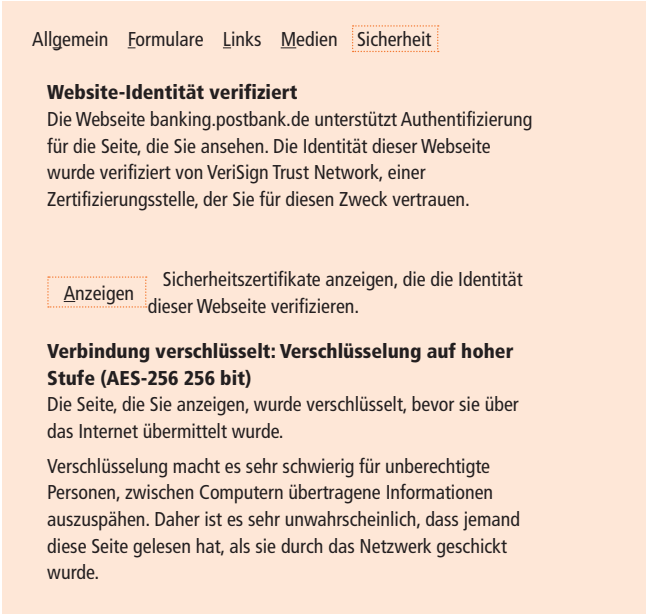


Abbildung 13: SSL-Sicherheitsinformation für den Browser

Allerdings kann auch eine unzertifizierte SSL-Verbindung nützlich sein. Jedenfalls ist auch in diesem Fall die Kommunikation verschlüsselt und mit dem Integritätsschutz versehen. Und auch bei anonymem Schlüsselaustausch werden die übermittelten Zufallszahlen in den erzeugten Schlüssel integriert und so eine Attacke vermieden.

6.1.6 Schwächen und Lösungshilfen

Das SSL-Verfahren hat zwei Schwächen und eine Einschränkung, über die sich ihre Nutzer klar sein müssen. Die erste Schwäche ist die Unsicherheit darüber, wer der Partner auf der anderen Seite wirklich ist, wenn die Authentifizierung entweder nicht stattfindet (was das SSL-Protokoll zulässt) oder nicht richtig ausgeführt wird. Ein Web-Server, der sich mit einem gefälschten, ungültigen oder abgelaufenen Zertifikat bei einem Browser zurückmeldet, erzeugt beim Browser eine Warnmeldung. Viele Nutzer von Web-Browsern können mit einer solchen Meldung nichts anfangen und ignorieren sie. Sie wiegen sich

dann in der falschen Sicherheit einer mit einem hübschen Bügelschloss markierten SSL-Verbindung, kommunizieren auch tatsächlich verschlüsselt, allerdings mit einem falschen Partner, der ihnen nun alle möglichen vertraulichen Informationen, wie zum Beispiel PINs und TANs für Homebanking, entwenden kann.

Eine zweite Schwäche liegt darin, dass die automatisierte Sicherheit von SSL nur dann gewährleistet ist, wenn die Client- und Server-Komponenten unmanipuliert funktionieren. Ein so genannter SSL-Trojaner könnte alle Sicherheitsfunktionen ausschalten, indem er alle Warnungen des Browsers unterdrückt und dem Nutzer dadurch suggeriert, dass alles in Ordnung ist.

Achten Sie deshalb auf einen aktiven und aktuellen Antivirenschutz und besonders genau auf die Zertifikate des Partners. Dazu klickt ein Nutzer auf das Bügelschloss und liest das angezeigte Server-Zertifikat. Er sollte den Namen des Zertifikatausstellers kennen und ihm vertrauen. Wenn das nicht der Fall ist, ist es ratsam, die Web-Verbindung nicht weiter zu verfolgen und gegebenenfalls direkten Kontakt zu seiner Zieladresse (Bank, Online-Shop, etc.) zu suchen.

Überprüfen Sie außerdem die SSL-Einstellungen ihres Browsers.
Internet Explorer: *Extras* → *Internetoptionen* → *Reiter „Erweitert"* → *Sicherheit*.
Mozilla Firefox: *Extras* → *Einstellungen* → *Reiter „Sicherheit"*.

Ein dritter Punkt ist nicht eigentlich eine Schwäche von SSL, sondern nur eine Einschränkung seiner Wirkung: Der Integritätsschutz von SSL wirkt nur für die Dauer der SSL-Verbindung. Es werden nämlich nicht die Anwendungsdaten im Ganzen geschützt, sondern nur ihre Fragmente im Transport-System. Ein elektronischer Vertrag also, der über eine SSL-Verbindung ausgehandelt wird, ist erst dann gegen spätere Abstreitung gesichert, wenn er insgesamt mit einer digitalen Signatur versehen ist, die auf Anwendungsebene ausgestellt, verifi-

ziert und aufbewahrt wird. Denn die SSL-Signaturen sind nach Ende einer SSL-Verbindung alle verschwunden („flüchtiges Sicherungsverfahren").

6.2 WLAN (Wireless Local Area Network) – kabellos (un-)sicher

Eine adäquat geschützte WLAN-Verbindung lässt sich schwer ohne fortgeschrittene technische Kenntnisse einrichten. Im folgenden Anwendungsbeispiel werden gängige Verfahren genannt, deren Stärken und Schwächen aufgezeigt und konkrete Vorschläge für verschiedene Einsatzszenarien (Heim-WLAN, Kleinbetrieb, mittelständisches Unternehmen) geschildert.

Vertiefende technische Details bietet beispielsweise [Rech 2006].

6.2.1 Anwendung

Die LAN-Technologie (Local Area Network) verbindet einzelne Arbeitsrechner zu einem Netzwerk. Die einfachste Form eines kabellosen lokalen Netzes (WLAN= Wireless Local Area Network) ist unverschlüsselt und erlaubt Zugang für jeden ohne Überprüfung der Identität. Die Verbindung der teilnehmenden Computer untereinander und ins Internet übernehmen Geräte, die nach ihrer Funktionalität „Access-Point" oder „Router" genannt werden.

Sind drahtlose Netze unverschlüsselt, so ist jeder im Umkreis von 30 bis 100 Metern (je nach Umgebung) in der Lage auf dieses Netzwerk zuzugreifen. Ein Angreifer könnte nicht nur den Netzdienst frei in Anspruch nehmen, sondern auch jegliche Kommunikation innerhalb des Netzwerkes belauschen und persönliche Daten und Passwörter, die bei Anwendungen im Internet eingesetzt werden, abgreifen. Das unberechtigte Nutzen des Internetzugangs birgt auch die Gefahr, dass illegale Handlungen im Internet dem Eigentümer des Internetanschlusses zur Last gelegt werden können, und dieser kaum Möglichkeiten haben wird, seine Unschuld zu beweisen.

6.2.2 Ziel der Verschlüsselung des WLAN

Zur Überprüfung der Authentizität der berechtigten Nutzer bietet die WLAN-Technologie verschiedene Varianten wie

- die Möglichkeit die Adresse der Netzkarte (MAC – Media Access Control) zu überprüfen,
- ein vorher definiertes Kennwort zu verwenden (PSK – Pre Shared Key)
- oder die Authentizität implizit über die Verschlüsselung zu überprüfen.

Weitere Authentifikationsmöglichkeiten sind in dem Protokoll EAP[26] (Extensible Authentication Protocol) zusammengefasst.

Über die Authentifizierung hinaus wird der Datenverkehr in der Luft verschlüsselt. Zusätzlich können die Verschlüsselungsverfahren die Integrität der Daten schützen, so dass Angreifer Daten auf dem Übertragungsweg nicht verfälschen oder gar falsche Daten einspielen können. Aktuelle Verfahren dafür sind WEP (Wired Equivalent Privacy), WPA (Wireless Fidelity Protected Access) und WPA2.

6.2.3 Ablauf

Im Folgenden werden die üblichen Authentifikations- und Verschlüsselungsverfahren für die Absicherung von WLANs vorgestellt. Eine aktuelle Beschreibung der verschiedenen Verfahren findet sich auch bei [Detken 2006].

26 EAP ist kein einzelnes Protokoll, sondern ein Rahmen für verschiedene Authentifikationsverfahren wie zum Beispiel die Authentifikation per User-ID und Passwort oder per Signatur und Zertifikat.

Offener Zugang:
Die meisten WLAN-Router werden im offenen Zugangsmodus ausgeliefert. Das bedeutet, dass der Zugang zum WLAN weder verschlüsselt ist, noch eine Zugangsberechtigung erfordert.

Überprüfung der MAC-Adresse (Media Access Control):
Die MAC-Adresse ist eine weltweit eindeutige Kennung von jedem netzwerkfähigen Gerät wie z.B. ein Laptop. Zur Authentifikation trägt der WLAN-Betreiber erlaubte MAC-Adressen in einer Zugriffskontrollliste entweder direkt im Zugangsgerät (Access-Point) oder auf einem zentralen Server im Netzwerk ein, die der Access-Point zur Authentifikation heranzieht. Angreifer sind in der Lage, die MAC-Adresse zu fälschen. In Kombination mit anderen Authentifikationsverfahren bietet es allerdings eine zusätzliche Hürde für Angreifer.

Einsatz eines geheimen Schlüssels (PSK – Pre Shared Key):
Die einfachste Variante sieht ein gemeinsames Kennwort für alle autorisierten Nutzer des Netzwerkes vor. Da alle Teilnehmer dieses Kennwort kennen müssen und die Netzwerkkomponenten dementsprechend konfiguriert werden müssen, ist diese Variante nur für kleine Netzwerke oder Heimnetzwerke sinnvoll.

WEP (Wired Equivalent Privacy):
WEP ist das ehemalige Standard-Verschlüsselungsverfahren für WLAN. Es soll die Vertraulichkeit und Integrität der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren heute als unsicher angesehen und kann nach dem Mitschneiden ausreichender Datenmengen (was innerhalb weniger Minuten geschieht) innerhalb weniger Sekunden entschlüsselt werden.[27] Daher sollten aktuelle WLAN-Installationen die sicherere WPA2-Verschlüsselung verwenden.

27 vgl. WEP-Verschlüsselung von WLANs in unter einer Minute geknackt, auf: http://www.heise.de/security/result.xhtml?url=/security/news/meldung/87874

Implizite und explizite WEP-Authentifikation

Bei der impliziten Authentifikation wird auf ein Authentifikationsverfahren selbst verzichtet, allerdings ist die Verschlüsselung nur mit einem zuvor ausgetauschten Schlüssel (Pre Shared Key) möglich. Das wirkt wie eine implizite Authentifizierung, denn nur die Kenner des Schlüssels können die geforderte Ver- und Entschlüsselung durchführen. Darüber hinaus bietet WEP einen expliziten Authentifizierungsmechanismus. Es wird aber empfohlen, auf diesen lieber zu verzichten, da er einem potentiellen Angreifer zusätzliche Angriffspunkte liefert, den verwendeten Schlüssel herauszufinden (vgl. Kap. 6.2.5). Beim reinen WEP wird deshalb die implizite Authentifikation empfohlen.

EAP (Extensible Authentication Protocol):

EAP ist kein einzelnes Authentifikationsverfahren, sondern ein Rahmen für verschiedene Verfahren wie zum Beispiel die Authentifikation mit User-ID und Passwort oder mit Signatur und Zertifikat. Das Grundprinzip besteht in einer Ende-zu-Ende-Authentifikation zwischen dem Client und einem Authentifikationsserver über den vermittelnden Access-Point hinweg. Da in drahtlosen Netzen in der Regel keine direkte Ende-zu-Ende-Kommunikation möglich ist, muss diese von einem anderen Protokoll wie IEEE 802.1x, einem Standard zur Authentifizierung in Rechnernetzen, realisiert werden.

WPA und WPA2 (Wireless Fidelity Protected Access):

Bei WPA und seinem Nachfolger WPA2 unterscheidet man zwei Authentifikationsmodi. Neben dem Pre-Shared-Key-Verfahren, welches für Heimanwendungen beibehalten wird, werden nun die EAP-Verfahren bevorzugt, welche über das IEEE 802.1x Protokoll eine direkte Server-Client-Authentifikation durch den Access-Point hindurch ermöglichen.

WPA verwendet zur Verschlüsselung ein so genanntes Temporal Key Integrity Protocol (TKIP), welches aus Kompatibilitätsgründen auf die WEP-Verschlüsselung aufsetzt. Verbesserungen gegenüber WEP

wurden zum Beispiel durch die Verwendung eines besseren Integritätschecks, durch längere Initialisierungsvektoren und ein besseres Schlüsselmanagement erreicht.

WPA2 basiert demgegenüber auf dem Advanced Encryption Standard (AES) und implementiert die grundlegenden Funktionen des neuen Sicherheitsstandards IEEE 802.11i. Die Verwendung von TKIP ist dadurch nicht mehr notwendig.

Handlungsempfehlung:

- Entnehmen Sie dem Handbuch ihres WLAN-Routers, wie Sie WPA2 direkt an ihrem Router einstellen.
- Wählen Sie WPA2 als Verschlüsselung. Für ein Heimnetzwerk wählen Sie PSK (Pre Shared Key), und legen einen starken Schlüssel fest.
- Suchen Sie mit ihrem mobilen Endgerät (z. B. Laptop) nach dem entsprechenden WLAN. Wenn Sie sich mit dem WLAN verbinden, geben Sie den vorher festgelegten Schlüssel wieder ein.

6.2.4 Stärken

WLAN-Betreiber können mit angemessenen Authentifikations- und Verschlüsselungsverfahren Angriffe auf ihre Netzwerke deutlich erschweren oder verhindern. Damit schützen sie sich nicht nur vor Lauschen und Ressourcendiebstahl, sondern kommen auch ihren Haftungspflichten gegenüber illegalen Handlungen in ihren Netzen nach. Selbst geringe Schutzmaßnahmen (z. B. MAC-Adressen-Überprüfung) sind besser als gar keine, da sie das unbeabsichtigte Einwählen und das Einwählen durch unerfahrene Angreifer abhalten.

Standardtechniken bieten heutzutage die Möglichkeit, sich mit stärkeren Mitteln zu schützen. Das WPA2-Verfahren erreicht dabei schon ein recht hohes Sicherheitsniveau durch die Verwendung des starken AES-Algorithmus. EAP bietet eine allgemein verfügbare Schnittstelle für verschiedene Authentifikationsverfahren.

6.2.5 Schwächen vermeiden

Die höchste Sicherheitsstufe (WPA2) bei WLAN ist leider sehr selten im Einsatz, da vor allem ältere WLAN-Hardware-Komponenten AES nicht beherrschen. Andere Komponenten unterstützen das Verfahren nur durch softwareseitige Berechnungen, so dass erhebliche Einbußen bei der Übertragungsgeschwindigkeit die Folge sind. Das macht WPA2 für viele Nutzer unattraktiv.

Um Ihr WLAN sicher zu machen, folgen hier einige allgemeine Hilfestellungen: An erster Stelle sollte beim Pre-Shared-Key die Wahl eines sicheren WPA-Netzwerkschlüssels stehen. Dieser sollte die maximale Schlüssellänge von 63 Zeichen nutzen. Wichtig ist hierbei die lose Kombination von Buchstaben, Ziffern und Sonderzeichen, um Brute-Force- oder Wörterbuchangriffe zu erschweren.

Weitere Sicherheitsmaßnahmen sind:

- das Standard-Passwort des Access-Points ändern beziehungsweise überhaupt erst mal ein Passwort setzen.
- der vergebene Name des Access Point (SSID) sollte keine Rückschlüsse auf verwendete Hardware, Einsatzzweck oder Einsatzort zulassen.
- WLAN-Geräte (z. B. der Access Point) sollten nicht per WLAN konfiguriert werden (können), sondern ausschließlich über eine kabelgebundene Verbindung.
- im Access-Point sollte, sofern vorhanden, die Fernkonfiguration aus dem Internet abgestellt werden.
- WLAN-Geräte ausschalten, wenn sie nicht genutzt werden.
- Reichweite des WLANs durch Reduzierung der Sendeleistung bzw. Standortwahl des WLAN-Gerätes beeinflussen.

- regelmäßige Firmware-Updates vom Access Point durchführen, um sicherheitsrelevante Aktualisierungen zu erhalten.
- Auch viele ältere Router unterstützen WPA2 nach einem Firmware-Upgrade. Es lohnt sich also hin wieder nachzusehen, ob der Hersteller dies nachträglich implementiert hat. Falls dies das WLAN zu sehr ausbremst, weil das nur softwaremäßig, aber nicht durch die Hardware unterstützt wird, ist bei älteren Routern WPA immern noch besser als nichts.

6.3 Elektronische Türschlösser

6.3.1 Anwendung

Zutritt zu geschützten Objekten wie Gebäuden oder in ein Fahrzeug wird traditionell mit physischen Schlüsseln gewährt. Wer den passenden Schlüssel hat, kommt hinein, andere nicht. Bei Diebstahl oder Verlust des Schlüssels muss das ganze Schloss ersetzt werden, was bei größeren Schließanlagen mit Gruppenschlüsseln sehr teuer werden kann. Bei elektronischen Schließanlagen dagegen braucht nur das Schloss umprogrammiert werden, und der verlorene oder gestohlene Schlüssel wäre wertlos. Auch bei einem Wechsel der Zutrittsberechtigung müssten bereits verteilte elektronische Schlüssel nicht umverteilt werden, da sich die betroffenen Schlösser umprogrammieren lassen. Elektronische Schließanlagen können also die Schlüsselverwaltung erleichtern und sicherer machen.

6.3.2 Technische Grundlagen bei elektronischen Türschlössern

Bei elektronischen Schließsystemen sind zwei Phasen zu unterscheiden: Zum einen die Schlüsselverwaltung, in der physische Schlüssel hergestellt, unter den berechtigten Personen verteilt und bei Bedarf umverteilt werden. Und zweitens die Schließvorgänge, bei denen ein Schlüsselträger über einen elektronischen Kontakt oder durch die Luft per Funk oder Infrarot Schließ- und Entriegelungsbefehle an ein Schloss überträgt. Wir erläutern hier nur die zweite Phase.

Für die Schlüsselverwaltung setzen wir dabei voraus, dass die Schlüsselträger, seien es elektronische Kontaktschlüssel oder kontaktlose Transponder, vom Betreiber der Schließanlage vor der Ausgabe richtig programmiert wurden, wobei Algorithmen, Identifikationsnummern und geheime kryptographische Schlüssel eingebracht werden können.

Für die Schließvorgänge selbst ist wiederum zu unterscheiden, wer die Entscheidung trifft, ob ein Schließ- oder Entriegelungsbefehl ausgeführt wird. Elektronische Schlösser können eigenständig und ohne Anschluss an einen zentralen Server entscheiden, wenn ihnen die Berechtigungen dezentral vorab einprogrammiert wurden. Das ist zum Beispiel bei Funkschlössern für Fahrzeuge der Fall.

Alternativ können elektronische Schlösser mit einem zentralen Server verbunden sein, dem sie die Schlüsselbefehle vom Schlüsselträger weiterleiten und von dem sie die Entscheidung zum Schließen oder Entriegeln mitgeteilt bekommen. Dies ist in der Regel bei Schließanlagen in Gebäuden oder Gebäudekomplexen der Fall. Im Fall der mit einem Server vernetzten Schlösser ist die Kommunikation zwischen Schlössern und Schlüssel-Server ebenfalls abzusichern. Wir gehen hier davon aus, dass dieses Netz gegen Lauschangriffe und Manipulation geschützt ist, zum Beispiel dadurch, dass es im physisch geschützten Gebäudebereich fest verdrahtet ist und unter zentraler Aufsicht steht.

Für die Schließ- und Entriegelungsvorgänge zwischen elektronischem Schlüsselträger und Schloss gibt es verschiedene technische Ausführungen von Identitätsnachweisen. Es gibt biometrische Sensoren, sowie kontaktbehaftete und kontaktlose elektronische Schlüsselträger.

Die biometrische Variante löst die Authentifizierung anhand eines biometrischen Merkmals aus. Ein Sensor für Fingerabdrücke (oder für Augenhintergrundmuster oder Gesichtsformen) ist direkt neben dem Schloss angebracht und mit einem Prozessor verbunden, der sowohl neue Berechtigungen aufnehmen als auch bestehende Berechtigungen prüfen kann. Die Datensätze, welche die biometrischen Informationen beinhalten (so genannte „Templates"), können als Schlüssel interpretiert werden, welche direkt im Schloss gespeichert sind. Separat von der Schlosseinheit ist lediglich noch eine Schaltung notwendig, welche das Relais zur Öffnung der entsprechenden Tür mit Spannung versorgt. Von zahlreichen Unternehmen werden heute Varianten von einer einzelnen Tür für die Heimanwendung bis zur komplexen Vernetzung in Unternehmensgebäuden angeboten.

Kontaktbehaftete Schlüsselträger wie Zugangskarten kommunizieren mit ihrem Schloss vor Ort über einen elektrischen Schleifkontakt.

Kontaktlose Schlüsselträger können die Datenübertragung zum Schloss über Funk, RFID oder Infrarot realisieren. Eine allgemein etablierte Anwendung kontaktloser Schlüsselträger sind Autoschlüssel. Die frühen Formen von Autoschlüsseln übertrugen die Daten per Infrarot. Das hat den Nachteil, dass eine Sichtlinie zwischen Schlüsselträger und Empfänger erforderlich war. Heute wird hauptsächlich die Funktechnologie verwendet. Die meisten Autoschlüssel senden im lizenzfreien ISM-Band (Industrial, Scientific, and Medical Band) bei 433 MHz. Zusätzlich beinhalten moderne Autoschlüssel einen RFID-Transponder, der die elektronische Wegfahrsperre schaltet. Während RFID-Chips eine Reichweite von ca. 10 cm besitzen, hat die Funkübertragung eine Reichweite von etwa 10 m.

6.3.3 Eingesetzte Algorithmen

In elektronischen Schließsystemen kommen in der Regel symmetrische Verfahren zum Einsatz. Bei vielen Anwendungen wie zum Beispiel bei einem Kfz-Schlüssel werden die kryptographischen symmetrischen Schlüssel während der Produktion in den Schlüsselträger eingebettet, so dass auf eine Aushandlung der Schlüssel mit asymmetrischen Verfahren verzichtet werden kann. Dabei kommen alle symmetrischen Algorithmen, wie Triple-DES, AES, IDEA oder RC4 zum Einsatz.

Viele Hersteller neigen dazu, verwendete Algorithmen geheim zu halten, da sie davon ausgehen, dass ihre Systeme dadurch sicherer sind. Allerdings gibt es genügend viele öffentlich bekannte Verschlüsselungsverfahren, die als sicher gelten. Deshalb kann das Publizieren des Algorithmus ein Qualitätsmerkmal sein, während die Geheimhaltung den Verdacht nährt, dass aus Kosten- und Effizienzgründen unsichere Verfahren eingesetzt werden.

6.3.4 Ziel der Verschlüsselung

Werden Schließ- und Entriegelungsbefehle in einem Netzwerk zu einem entfernten Schloss übertragen, so müssen sich die Schlösser ihrerseits identifizieren. Wenn dann noch ein Schlüssel-Server im Netz die Verteilung der Schlüssel organisiert, muss sich der Schlüssel-Server ebenfalls authentifizieren, um zu verhindern, dass ein Angreifer dem Schloss eigene Schlüssel zusendet. Zusätzlich muss die Kommunikation verschlüsselt stattfinden.

Die elektronischen Übertragungswege müssen dagegen vor Fehlbedienung, Lauschangriffen und Manipulation geschützt werden. Das gilt insbesondere für kontaktlose Schlüssel, die ein Schloss durch die Luft bedienen und Angreifern die Gelegenheit bieten, eine mitgelauschte Identifikation wieder in das System einzuspielen (Replay-Attacke).

6.3.5 Ablauf

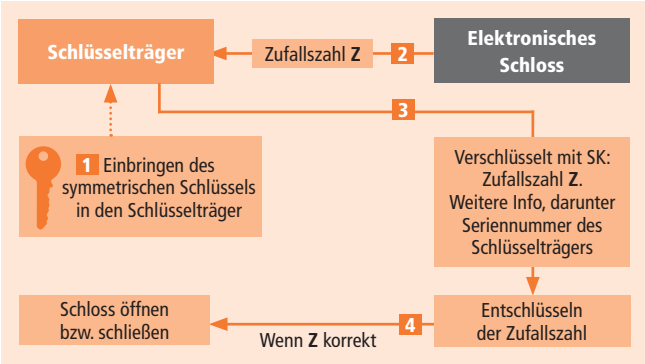


Abbildung 14: Einseitige Authentifizierung eines Schlüsselträgers gegenüber seinem elektronischen Schloss

Schritt 1: Ein Schlüsselträger und sein elektronisches Schloss verwenden einen gemeinsamen, geheimen symmetrischen Schlüssel. Diesen kryptographischen Schlüssel, anhand dessen das Schloss den berechtigten Schlüsselträger erkennt, berechnet das elektronische Schloss aus einem Hauptschlüssel, den er für alle Schlüsselträger verwendet und aus der Seriennummer des Schlüsselträgers.

Schritt 2: Bei Annäherung des Schlüsselträgers an das elektronische Schloss löst sein jeweiliger Besitzer ein Signal aus, mit dem er anzeigt, ob er das Schloss öffnen oder schließen will. Daraufhin sendet das elektronische Schloss eine Zufallszahl **Z** aus, die der Schlüsselträger empfängt.

Schritt 3: Der Schlüsselträger verwendet den ihm eingepflanzten symmetrischen Schlüssel, um die Zufallszahl **Z** zu verschlüsseln. Das Kryptogramm sendet er dann gemeinsam mit weiteren Informationen, darunter seiner Seriennummer, an das elektronische Schloss zurück.

Schritt 4: Das elektronische Schloss prüft, ob die Seriennummer bei ihm eingespeichert ist. Wenn das der Fall ist, dann berechnet es aus der Seriennummer und seinem Hauptschlüssel den geheimen Schlüssel des Schlüsselträgers und verwendet diesen zur Entschlüsselung des zugesandten Kryptogramms. Wenn das Ergebnis mit der von ihm in Schritt 2 ausgesendeten Zahl **Z** übereinstimmt, dann ist der Schlüsselträger authentisch und das Schloss kann den Befehl ausführen, das Schloss zu schließen bzw. zu öffnen.

Aufwändigere elektronische Schließanlagen wie in Firmengebäuden arbeiten mit zusätzlichen Entscheidungsregeln (so genannten „Policies"). Regeln können sich auf Zeiten, Personen, Personengruppen und der Anzahl Schließvorgänge beziehen. So kann es zum Beispiel Regeln geben, die den Zutritt nur zu bestimmten Zeiten oder verschiedenen Gruppen zu verschiedenen Zeiten erlaubt. Weitere Regeln können ein Schloss dazu veranlassen, einen Schlüssel nach einer bestimmten Anzahl von Fehlversuchen zu sperren. Soweit Regeln programmierbar sind, können sie von Schließanlagen mit Hilfe digitaler Prozessoren realisiert werden.

6.3.6 Stärken

Ein Vorteil elektronisch gesteuerter gegenüber physischen Schließanlagen liegt darin, dass sie leichter und billiger zu verwalten sind. Die Nutzung kontaktloser Schlüsselträger ist für die Anwender zudem bequemer. Geht bei den beschriebenen Verfahren ein Schlüsselträger verloren, so reicht es aus, den entsprechenden Schlüssel zu sperren und einen neuen Schlüsselträger mit neuem Schlüssel auszuhändigen, während bei physischen Schlüsseln ein Austausch aller betroffenen Schlösser erforderlich ist.

Schließregeln („Policies") bringen zusätzlichen Nutzen wie zum Beispiel die Ermittlung des Status einer Tür, das Festlegen von Zeiten und die flexible Vergabe von Gruppenschlüsseln.

Schließanlagen werden zentral verwaltet und kommen daher mit den effizient arbeitenden symmetrischen Verschlüsselungsprotokollen aus. Sofern sie auf starken Verschlüsselungsverfahren wie AES mit entsprechend großen Schlüssellängen beruhen, sind sie sicher.

6.3.7 Schwächen

Bei elektronischen Schließsystemen muss bei einem Stromausfall oder bei technischen Problemen eine alternative Lösung verfügbar sein, Zugänge öffnen oder verschließen zu können und Fluchtwege zu erreichen. Da in den meisten Fällen also zwei Schließsysteme parallel bestehen, reduziert sich die Gesamtsicherheit, da ein Angreifer nun die Auswahl hat, welches System er angreift. Optimal wäre, das mechanische Schließsystem mit einem Alarmsystem zu kombinieren, so dass die Türen mittels verplombter Nothebel entriegelt werden können.

Die Festlegung von Policies kann bei großen Systemen sehr komplex werden. Hinzu kommt, dass sowohl die Policies als auch die Schlüssel in die Schlösser verteilt werden müssen. Je nach Lösung kann dies einen hohen Aufwand bedeuten.

Wenn die eingesetzten Verschlüsselungsverfahren schwach sind, dann sind elektronische Schlüssel leichter angreifbar als physische Schlüssel. Insbesondere Transponder reagieren auf ein Funksignal, auch wenn es nicht von einem autorisierten Schloss stammt, sofern die Authentifizierung nur einseitig erfolgt, was die Regel ist. Wenn sie aber schlecht verschlüsselt sind, dann können die zugehörigen kryptographischen Schlüssel geknackt und mit ihnen perfekt gefälschte Funkschlüssel nachgebaut werden. Ein physischer Diebstahl wäre dann nicht mehr erforderlich. Eine gute Verschlüsselung und Frischemerkmale wie Zufallszahlen und Zeitinformationen beseitigen die Schwachstelle.

7 Was soll und kann ein Endanwender/ein Unternehmen konkret tun?

Hier soll in Kürze und nicht vollständig aufgelistet werden, was Endanwender und Mitarbeiter tun können/sollen, um die Sicherheit in ihrem Wirkungsumfeld zu erhöhen.

7.1 Wissen, Awareness und Organisatorisches

- Ein Bewusstsein dafür entwickeln, dass das Ausforschen von Firmengeheimnissen, die Manipulation von Identitäten und das Unterschieben bzw. Fälschen von Dokumenten auch über das Internet verbreitet sind
- Sich ein Grundverständnis von Verschlüsselung und Kryptologie aktiv erarbeiten. Tipp: CrypTool (www.cryptool.de)
- Gesetzliche Vorschriften kennen: z. B. KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
- Umsetzung der Maßnahmen zu den Themen Risikomanagement und IT-Sicherheit: siehe Grundschutz-Kataloge des BSI GSHB
- Kostenlosen Newsletter vom Bundesamt für Sicherheit in der Informationstechnik (BSI) abonnieren (www.bsi.de → *Presse* → *Newsletter*)
- Bundes- und Landesverfassungsschutzbericht zum Thema Wirtschaftsspionage
- Social Engineering kennen: der „Faktor Mensch" als schwächstes Glied (s. Literaturverzeichnis)
- Gesundes Misstrauen und Aufmerksamkeit gegenüber Spam- und Phishing-Attacken
- Sich trauen, Fragen zu stellen und offene Quellen wie www.wikipedia.de nutzen
- Weitere Verweise: siehe Literaturverzeichnis, Teil C, „Links zu Wirtschaftsspionage u. ä. und Stellen, die dagegen behilflich sind"

7.2 Technisches

- Regelmäßiges Einspielen von Updates und Patches für Betriebssysteme und Anwendungen
- Wichtigste aktuelle Bedrohungen kennen: Viren, Spybots, Spam und Phishing. Nutzung aktueller Antiviren-Software, von Spamfiltern und Firewalls
- Ändern aller Default-Passwörter, Nutzung starker Passwörter
- Auf SSL-Verschlüsselung (SSL-Schloss im Browserfenster, vgl. Abb. 11) achten, Zertifikate beachten und prüfen
- Aktivieren und verwenden Sie die jeweils stärkste WLAN-Verschlüsselung und WLAN-Authentisierungsverfahren (vgl. Kapitel 6.2). Aktivieren Sie die MAC-Adressen-Überprüfung als zusätzliche Hürde gegen Angreifer.
- Verwendung von zusätzlicher Kanalverschlüsselung mittels VPN bei der Verbindung von Rechnern über das Internet
- Nutzung von Tools bzw. sicheren Varianten wie beispielsweise:
  - Sichere E-Mail mit S/MIME (eingebaut in fast alle Standard E-Mail-Clients wie Outlook oder Thunderbird), PGP (Pretty Good Privacy) oder Gpg4win (Open-Source-Variante von PGP)
  - Festplattenverschlüsselung mit TrueCrypt (vgl. Kapitel 4.4)
  - Dateiverschlüsselung mit dem AES-Tool im CrypTool-Paket
  - Einsatz langer kryptographischer Schlüssel bei Anwendungen wie WLAN, E-Mailing oder Festplattenverschlüsselung. Das RSA-Verfahren wird in den meisten dieser Anwendungen eingesetzt. Das populärste Beispiel ist das Programm PGP bzw. seine Open-Source-Varianten. Mit einem solchen kostenlosen Programm ist jeder PC-Besitzer in der Lage, Texte oder Dateien sicher zu ver- und entschlüsseln oder zu signieren.
- Weitere Verweise: siehe Literaturverzeichnis, Teil C, „Internet-Links (URLs)“

8 Schlusswort

Wir haben zahlreiche Beispiele aus dem Alltagsleben vorgestellt, die kryptologische Techniken bereits nutzen. Oft haben die Verfahren Schwächen, aber sie sind erstens durch den Anwender verbesserungsfähig und zweitens erreichen sie im Verbund mit anderen Maßnahmen ihr Ziel.

Es ist wichtig, dass Verschlüsselung an vielen Stellen von selbst arbeitet, ohne dass sich die Anwender darum kümmern müssen – wie zum Beispiel am Geldautomaten oder beim Funkschloss an der Autotür. Sogar die geschützten Web-Verbindungen beim Homebanking und bei elektronischen Bestellungen funktionieren zunächst von selbst. Da Computer viele Funktionen erfüllen und unter anderem auch unser Schaufenster in die elektronische Welt des Internet darstellen, können Schadfunktionen auf vielen Wegen eindringen. Daher müssen alle Anwender lernen, ihren Computer zu verstehen und richtig zu bedienen. Die geschützten Verbindungen bei SSL nützen nichts, wenn es auf der anderen Seite einem Betrüger gelingt, sich als jemand anderes auszugeben. Daher muss der Anwender lernen, Warnungsmeldungen über unsichere Identitäten zu beachten statt sie zu ignorieren.

Ein Grundverständnis der Verschlüsselung und ihrer Anwendungen ist daher für jeden, ob als Nutzer zu Hause oder als verantwortlichem Planer, Softwarearchitekt oder Entwickler im Unternehmen, eine wesentliche Voraussetzung zur sicheren Nutzung des Internet und anderer Computer-gesteuerter Anwendungen im Alltagsleben. Denn bei aller Unterstützung aus dem Netz ist und bleibt **Selbstschutz** ein wesentlicher Sicherheitsbaustein. Die hier vorgelegte Kryptofibel hat den Anspruch, auf dem Weg zu diesem Ziel ein erster Schritt zu sein. Weitere Schritte können die Leser anhand der aufgeführten Literaturhinweise leicht gehen. Als besonders lehrreich empfehlen wir, mit dem Lernprogramm **CrypTool** Verschlüsselungsverfahren selbst spielerisch auszuprobieren.

Abbildungsverzeichnis

Literaturverzeichnis

A Bücher für Kinder

Dahl, Kristin / Nordqvist, Sven (1996): Zahlen, Spiralen und magische Quadrate – Mathe für jeden, Qetinger Verlag
Für Kinder geeignet, um den Spaß an Mathematik zu entdecken.

Flessner, Bernd (2004): Die drei ???. Handbuch Geheimbotschaften, Kosmos
Auf 127 Seiten wird erklärt, welche Geheimsprachen (z. B. die der Navajo-Indianer oder Dialekte) und welche Geheimschriften (z. B. echte Verschlüsselung, aber auch technische und linguistische Steganographie) es gab und wie man einfache Verfahren entschlüsseln kann.

Kippenhahn, Rudolf (2002): Streng geheim!, Rowohlt Tb.
Entlang einer Kindergeschichte werden die klassischen Kryptographie-Verfahren erläutert. Der „kleine Kippenhahn" ist empfohlen ab 11 Jahren allerdings auch von pfiffigen 8/9-jährigen zu verstehen

Singh, Simon (2004): Codes. Die Kunst der Verschlüsselung, Dtv
Spannend erzählte Geschichte der Kryptologie. Der „kleine Singh" jedoch ist m.E. nur eine (schlechte) Kürzung der „Geheimen Botschaften" und wohl eher für Jugendliche als für Kinder geeignet.

Weitere Kinderbücher werden z.B. auch auf der Website von Tobias Schrödel in der Rubrik „Literatur – Aktuell" besprochen: http://www.sichere.it/aktuelle_literatur.php

B Bücher für Erwachsene

Beutelspacher, Albrecht (2005): Geheimsprachen. Geschichte und Techniken, Beck'sche Verlagsanstalt
Gute Übersicht, die fast ohne Mathematik auskommt.

Beyrer, Klaus (1999), Streng geheim! Die Welt der verschlüsselten Kommunikation., Kataloge der Museumsstiftung Post und Telekommunikation, Band 5, Umschau Braus
Sehr anschauliche, unabhängige Einzelkapitel rund um Verschlüsselung und Spionage.

Ertel, Wolfgang (2003): Angewandte Kryptographie. 30 Aufgaben, Hanser Fachbuchverlag
Aktuell, allgemein verständlich trotz Mathematik.

Paul Garrett, Making, Breaking Codes (2001): Introduction to Cryptology, 1st edition, Prentice Hall
Hervorragende Darstellung, nur für mathematisch Interessierte (englischsprachig).

Kippenhahn, Rudolf (1999): Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte., Rowohlt Tb.
Allgemeinverständliche Einführung in die Kryptologie.

Meissinger, Jan (2005): Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland, Verlag Dr. Kova

Oppliger, Rolf (2005): Contemporary Cryptography, Artech House
Aktuelles Standardwerk zu den Kryptoverfahren (englischsprachig, mathematisch orientiert und gut verständlich)

Schmeh, Klaus (2007): Kryptografie – Verfahren, Protokolle, Infrastrukturen, dpunkt Verlag
Gute, aktuelle, sehr umfassende und allgemein verständliche Übersicht der Verfahren und Anwendungen.

Schmeh, Klaus (2004): Die Welt der geheimen Zeichen. Die faszinierende Geschichte der Verschlüsselung., w3L
Fundierte Darstellung der historischen Bedeutung und technischer Hintergründe ohne Mathematik und inkl. aktueller Erkenntnisse zu Erfolgen deutscher Codebrecher.

Singh, Simon (2001): Geheime Botschaften, Dtv
Spannend erzählte Geschichte der Kryptologie. Bestseller.

Laudon, Laudon, Schoder (2006): Wirtschaftsinformatik – Eine Einführung, Pearson
In Kapitel 14 (S. 649-705), „Sicherheit und Kontrolle von Informationssystemen" wird die Kryptologie ebenfalls in einem größeren Rahmen dargestellt.

Ulfkotte, Udo (2001): Wirtschaftsspionage, Goldmann
Liefert dem Leser eine Vielzahl von Fakten und Einblicke in die Welt der heutigen Wirtschaftsspionage.

Wobst, Reinhard (1998): Abenteuer Kryptologie, Addison-Wesley Verlag

C Internet-Links (URLs)

European Bridge-CA http://www.bridge-ca.de/eb-ca2/index.php
Die European Bridge-CA (EB-CA) ermöglicht eine sichere und authentische Kommunikation zwischen Unternehmen und öffentlicher Verwaltung. Dabei werden die Public-Key-Infrastrukturen der einzelnen Organisationen miteinander verknüpft, und bereits ausgegebene Zertifikate können über die lokalen „Identitätsinseln" hinaus verwendet werden. Dies erlaubt, unterschiedliche Geschäftsprozesse (Secure Email, Secure Logon, etc.) über die Grenzen der einzelnen Organisationen hinweg nutzbar zu machen.

C.a Links zu Lernsoftware und Tools

CrypTool www.cryptool.de
Umfangreiche freie Open-Source-Lernsoftware für Kryptographie und Kryptoanalyse, die es komplett in Deutsch und Englisch gibt und sowohl in Unternehmen, Behörden als auch in Schulen und Hochschulen eingesetzt wird. Weitere Mitentwickler (C, C++, C#, Java, HTML, Perl) sind jederzeit willkommen.

http://www.truecrypt.org, http://de.wikipedia.org/wiki/TrueCrypt
TrueCrypt ist eine kostenlose Open-Source-Software zur hochmodernen Verschlüsselung von Festplatten und Wechseldatenträgern für Windows und Linux.

http://passwordsafe.sourceforge.net/,
https://sourceforge.net/projects/passwordsafe/
„Password Safe" ist wie „KeePass Password Safe" ein freies Open-Source-Programm für Windows, mit dem man seine unterschiedlichen Passwörter sicher verschlüsselt auf dem Computer ablegen kann. Es wurde ursprünglich von Bruce Schneier's Counterpane Labs geschrieben. Auf der erstgenannten Seite befinden sich immer sehr aktuelle deutsche Versionen (Dieses Programm ist nicht zu verwechseln mit dem namensähnlichen kommerziellen Programm „Password Safe and Repository").

Open-Source-Varianten von PGP

http://www.gpg4win.org/, http://www.gnupg.org/

Gpg4win ist ein Installationspaket für Windows mit Programmen und Handbuch für Dateiverschlüsselung, Schlüsselmanagement und Sichere-E-Mail-Plugins, das auf die betriebssystemunabhängige Basis GnuPG aufsetzt. Ein alternativer Installer für Windows ist das Paket „GnuPG-Pack Basics" (http://people.freenet.de/rose-indorf/).

C.b Links mit Informationen für Kinder zur Kryptologie

http://www.blinde-kuh.de/geheim

Auf dieser hervorragenden Suchmaschine für Kinder befindet sich Catrins Kryptologie-Seite (wird seit 2003 leider nicht mehr aktualisiert).

http://www.geo.de/GEOlino/kreativ/basteln/278.html

Hier finden sich sehr anschauliche Informationen für kleinere Kinder – mit Bastelanleitungen zu jeder erläuterten Geheimschrift.

http://www.cipher.maths.soton.ac.uk

Die Universität von Southampton führt jedes Jahr die „National Cipher Challenge" durch, ein sehr ansprechend gemachter und anspruchsvoller Wettbewerb, bei dem tausende englischer Schüler anspruchsvolle Aufgaben zum Code-Knacken lösen.

http://www.nsa.gov/kids

Eine aufwändig gemacht Seite, die leider in letzter Zeit häufig nicht mehr von Deutschland aus aufrufbar ist: „CryptoKids – America's Future Codemakers & Codebreakers". Auf der Kinderseite des NSA zeigen die „CryptoKids" (bunte Tier-Cartoons) die verschiedenen Aspekte der elektronischen Informationsbeschaffung.

Leider gibt es bisher in Deutschland keine derartig nachhaltigen Bildungsanstrengungen zu diesem Thema, wie es diese beiden Vorbilder aus dem angelsächsischen Raum zeigen.

C.c Links mit kryptologischen Aufgaben für Bewerber

http://www.bnd.bund.de/cln_027/nn_354724/SharedDocs/Publikationen/DE/Downloads/Dateien/kryptoaufgabe,templateId=raw,property=publicationFile.pdf/kryptoaufgabe.pdf

Ein kleiner, feiner, aber leider einmaliger Versuch für moderne Bewerbersuche stammt von der Abteilung 2 des Bundesnachrichtendienstes (BND): Sie hat vier anspruchsvolle Aufgaben für zukünftige Bewerber zusammengestellt, deren Lösung sowohl Kreativität als auch mathematische Begabung erfordert.

http://www.gchq.gov.uk/codebreaking/index.html

Der britische Geheimdienst GCHQ führt regelmäßig Wettbewerbe (engl. challenges) durch und weist bei seiner Bewerbersuche (engl. recruitment) auch explizit darauf hin. Hier werden der Spieltrieb und die Neugier von talentierten und interessierten Jugendlichen explizit gefördert.

C.d Links mit allgemeinen Informationen zur Kryptologie

http://www.wikipedia.de

Sucheingabebegriffe: Kryptologie, Kryptografie, CrypTool; WikiProjekt Kryptologie.

http://www.schneier.com/essay-037.html

Bruce Schneier: „Why Cryptography is Harder than it Looks", 1997

Der Artikel beschreibt, warum es nicht einfach ist, starke Kryptosysteme zu entwerfen.

http://www.garykessler.net/library/crypto.html
Englischsprachige Webseite mit vielen Verfahren.

http://www.apprendre-en-ligne.net/crypto/activites/index.html
Französischsprachige Seite des Schweizers Dr. Didier Müller, die viele – auch alte – Verschlüsselungsverfahren liebevoll und umfassend erklärt.

http://shoup.net/ntb/
Elektronische Version des Buches „A Computational Introduction to Number Theory and Algebra" von Victor Shoup, 2005, Cambridge University Press
Aktuelles Standardwerk zur Zahlentheorie (in Englisch, sehr mathematisch orientiert).

http://www.cacr.math.uwaterloo.ca/hac/index.html
Elektronische Version des Buches „Handbook of Applied Cryptography" von Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 1997, CRC Press
Standardwerk zu kryptographischen Verfahren (in Englisch, sehr mathematisch orientiert).

C.e Links zu Wirtschaftsspionage u. ä. und Stellen, die dagegen behilflich sind

http://www.verfassungsschutz.de
Das Bundesamt für Verfassungsschutz und insbesondere die Landesämter informieren unter dem Kapitel „Spionageabwehr, Geheim- und Sabotageschutz" auch über Wirtschaftsspionage. Näheres dazu finden Sie z. B. in dem Faltblatt „Verfassungsschutz: Spionageabwehr – Geheimschutz" oder in den jährlichen Verfassungsschutzberichten – leider werden aus politischen Gründen die umfangreichen Aktivitäten der westlichen Geheimdienste nicht aufgeführt.

http://www.verfassungsschutz.nrw.de,
http://www.im.nrw.de/sch/742.htm
Beispielhaft führt das Land Nordrhein-Westfalen aktiv Informationsveranstaltungen durch, um nicht nur Behörden sondern auch Unternehmen ganz konkret vor Gefahren wie Wirtschaftsspionage und Sabotage aufzuklären.

http://www.sicherheitsforum-bw.de/berichte/berichte_start.html,
http://www.verfassungsschutz-bw.de/spio/files/spio_sonst_2004-11.htm
Der Verfassungsschutz in Baden-Württemberg bietet ebenfalls einige sehr gute Informationen rund um das Thema Wirtschafts- bzw. Konkurrenzspionage.

http://www.asw-online.de/Anmerkungen-zur-Sicherheitslage-der-deutschen-Wirtschaft20043.pdf
Bericht der ASW (Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.) aus dem Jahr 2005, der auch Aussagen zur Wirtschaftsspionage enthält.

http://www.geocities.com/dulfkotte/spionage1.html
Webseite zur Vorlesung von Udo Ulfkotte an der Uni Lüneburg mit vielen Links zum Thema Wirtschaftsspionage.

http://www.heise.de/tp/r4/artikel/6/6928/1.html
„Inside Echelon – Zur Geschichte, Technik und Funktion des unter dem Namen Echelon bekannten globalen Abhör- und Filtersystems" von Duncan Campbell, 2000.

http://www.bsi.bund.de
Startseite des Bundesamtes für Sicherheit in der Informationstechnik BSI

http://www.bsi.bund.de/gshb/index.htm
Die IT-Grundschutzkataloge mit konkreten Maßnahmen zur IT-Sicherheit generell.

http://www.sicherheit-im-internet.de,
http://www.bsi-fuer-buerger.de, http://www.buerger-cert.de
Webseiten unter dem Titel „Internet-Sicherheit" sowohl für die Zielgruppe der mittelständischen Unternehmen als auch der Privatanwender.

http://www.klicksafe.de
Das von der EU geförderte Projekt ist eine „nationale Sensibilisierungskampagne zur Förderung der Medienkompetenz im Internet". Hauptzielgruppe sind Kinder und Jugendliche.

https://www.sicher-im-netz.de
Startseite der Initiative „Deutschland sicher im Netz", die sich durch konkrete Handlungsversprechen von Unternehmen wie Microsoft und SAP auszeichnet und viele praktische Hilfen zur IT-Sicherheit generell bereithält.

D Explizit aufgeführte Literaturquellen

[Bauer 2000] Friedrich L. Bauer: „Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie", Springer, dritte, überarbeitete Auflage, 2000
Überwältigend viele spannende Details, vor allem zu den klassischen Verfahren.

[Bitkom] Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, 2006
http://www.bitkom.org/files/documents/Kompass_der_IT_28.06.06.pdf

[CT-Skript 2007] Skript zu CrypTool, Version 1.4.10, 2007
http://www.cryptool.de/downloads/CrypToolScript_1_4_10_de.pdf.
Ein sehr guter Einstieg zu einem tieferen Verständnis.

[Detken 2006] Detken, Kai-Oliver: „WLAN-Sicherheit von WEP bis CCMP". In DACH Security 2006, Syssec, 2006, 187-201.

[Rech 2006] Jörg Rech; „Wireless LANs", 2006, heise Verlag, Hannover

[Esslinger, Müller 1997] Esslinger, Bernhard; Müller, Maik: „Secure Sockets Layer (SSL) Protokoll – Sichere Internet-kommunikation mittels SSL und Sicherheits-Proxy", DuD 12/1997, 691-697.

[Fendl, Baumann, Schimmer 2005] Andreas Fendl, Uwe Baumann, Klaus Schimmer: SAP Pocket-Seminar „Faktor Mensch – Die Kunst des Hackens oder warum Firewalls nichts nützen", 2005. Im Rahmen der Initiative „Deutschland sicher im Netz"
Eine der besten Darstellungen zum Social Engineering überhaupt.

[Grimm, Hundacker, Meletiadou 2006] Rüdiger Grimm, Helge Hundacker, Nancy Meletiadou: „Kryptofibel-Anwendungen". Arbeitspapier des Instituts für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau, Oktober 2006.
http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGGrimm/Downloads/Kryptofibel-Anwendungen.pdf.

[Kahn 1996] David Kahn, "The Codebreakers", Macmillan Co., New York, 1967, revised and updated 1996
Geschichtlich orientiert, über 1100 Seiten, in Englisch, veraltet.

[Marchal 2005] Florian Marchal: „Analyse und Weiterentwicklung von Werkzeugen zur Qualitätsmessung von Passwörtern", 2005, Bachelorarbeit FH Darmstadt.
Eine Kopie der Arbeit ist über den Autor dieser Kryptofibel erhältlich.

Index

Anhang

Grobe Einteilung und ausgewählte Beispiele kryptographischer Verfahren

Symmetrische Verfahren

- **ein** Schlüssel zum Codieren und Decodieren, für Sender und Empfänger
- **Private Key** oder Single-Key oder Secret-Key oder Session-Key
- Problem: Schlüsselverteilung
- schnell

Beispiele

DES (Data Encryption Standard)
- 64 Bit Blöcke
- 56 Bit Schlüssellänge
- 56 Bit sind bei symmetrischen Verfahren heute nicht mehr sicher

AES (Advanced Encryption Standard)
- 128 Bit Blöcke
- 128, 192 und 256 Bit Schlüssellänge

Asymmetrische Verfahren

- **zwei** Schlüssel pro Teilnehmer:
  - **Private Key** zum Decodieren, für Empfänger
  - **Public Key** zum Codieren, für Sender
- sicherer
- Schlüssel ca. 10 mal so lang wie bei vergleichbaren symmetrischen Schlüsseln

Beispiele

RSA (Rivest, Shamir, Adleman)
- Primfaktorzerlegung großer Zahlen
- weit verbreitet
- 768 Bit bis 2048 Bit Schlüssellänge

DSA (Digital Signature Algorithm)
- diskretes Logarithmus Problem
- 1024 Bit Schlüssellänge
- oft kritisiert

Hash-Verfahren

- Einwegfunktion
- verarbeitet beliebig lange Nachricht zu einem eindeutigen Wert fester Länge
- Hash-Wert = Digitaler Fingerabdruck

Beispiele

MD5 (Message Digest)
- 128 Bit Hash-Wert
- 128 Bit gelten bei Hashverfahren heute nicht mehr als ausreichend sicher

SHA-1 (Secure Hash Algorithm)
- 160 Bit Hash-Wert

Abbildung 15: Überblick über ausgewählte Beispiele kryptographischer Verfahren