- JAHRESARBEIT -



AUTOR: PETER WEIGEL

Jahresarbeit

Datenverschlüsselung - Kryptographie

Autor: Peter Weigel

Thematik: Diese Arbeit soll einen Überblick über die Datenverschlüsselung, die Grundlage der modernen Sicherheit im Internet, geben. Dabei werde ich auf die Komplexität des Themas im Theoretischen, zum Beispiel die Codierungstheorie, eingehen, und die Verschlüsselung anhand von praktischen Beispielen verdeutlichen.

[Gliederung]

1. Einleitung **Seite 2**

1.1 Allgemeiner Ausgangspunkt **Seite 2**

1.2 Was ist Kryptographie und Verschlüsselung **Seite 3**

1.3 Geschichte **Seite 4**

1.4 Aktuelle Beispiele aus der Welt **Seite 9**

2. Theorie der Verschlüsselung **Seite 14**

2.1 Grundlagen der Verschlüsselung und Zahlentheorie **Seite 14**

2.2 Algorithmen **Seite 24**

2.2.1 Gängige Verschlüsselungsverfahren – Standards – Kryptographie **Seite 24**

2.2.2 Funktionsweise **Seite 30**

2.2.3 Sicherheit **Seite 40**

2.3 Nutzung und Umsetzung **Seite 42**

3. Praxis Teil – Anwendung der Kryptographie **Seite 47**

3.1 Gängige Software und Anwendungen **Seite 47**

3.2 „Knacken“ in der Praxis **Seite 54**

4. Schlusswort – Blick in die Zukunft **Seite 55**

5. Quellenangaben **Seite 58**

1. Einleitung

1.1 Allgemeiner Ausgangspunkt

Das Internet ist der denkbar unsicherste Ort für Rechner. Das Internet ist der Verbund von Millionen von Computern weltweit. Ständig gibt es neue „User“, die dem globalen und virtuellen Netz beitreten. Das Herunterladen von Hausaufgaben, Musikdateien, Dokumenten, Software und der wichtigsten Informationen ist schon längst zur Selbstverständlichkeit in unserer Gesellschaft geworden. 1990 existierte das Internet schon längst, dennoch verbreitete es sich erst ab 1998 immer mehr in die deutschen Haushalte. Doch man kann nun noch mehr mit dem Internet anrichten, als es früher war. In den Pionierzeiten war das Computernetz für das Militär gedacht, um schnell geheime Daten auszutauschen. Heute gibt „e-shopping“ (Einkaufen im virtuellen Netz), Versenden vertraulicher e-Mails, Abschluss von Verträgen usw. Aber wie sieht es mit der Sicherheit aus? Es gibt keinen Zweifel, das egal, was durch die weltweiten Datenleitungen geschickt wird, alles irgendwo einfach abgehört werden kann. Ob es wichtige oder unwichtige Nachrichten sind, spielt dabei keine Rolle. Jede nichtverschlüsselte Kommunikation über das Internet ist völlig unsicher. Im Internet gibt es keine Instanz, wie die Polizei im Staat, die für Ruhe und Ordnung sucht. Das Internet ist der beste Ort für die Anarchie. Jeder kann seine Meinung äußern und dabei seine Identität geheim halten. Dabei kann es immer Schnüffler oder Wirtschaftsspione geben, die die Privatsphäre in Frage stellen können, indem sie e-Mails lesen, das Kaufverhalten im virtuellen Einkaufsmarkt sichern und Verträge analysieren. Die beste mögliche Lösung gegen diese Spionage stellt die Kryptographie dar. Dabei werden die Daten verschlüsselt, das heißt die Klartextzeichen in einem unverständlichen Chiffretext verwandelt, so das, wenn jemand die Daten abhört, diese zwar in verschlüsselter Form besitzt, jedoch nicht verstehen kann.

Die angewandte Kryptographie spielt im Zeitalter der Vernetzung und des E-Commerce eine wichtige Rolle beim Schutz vertraulicher Daten und persönlicher Identität. Sie umfasst die Themen Verschlüsselung, Public-Key-Kryptographie, Authentifikation, digitale Signatur, elektronisches Bargeld und sichere Netze.

Im Zeitalter der Globalisierung des E-Business ist die Welt vernetzt. Immer mehr vertrauliche Daten werden über das Internet ausgetauscht. Dieser Datenaustausch weckt großes Interesse bei Geheimdiensten, um z.B. ihre Konkurrenz auszuspionieren. Allein in Deutschland entstehen in der Industrie pro Jahr geschätzte Verluste in Höhe von mehreren hundert Milliarden Euro durch Lauschangriffe.

Diese Angriffe geschehen meistens im Stillen und werden von den meisten Firmen nicht wahrgenommen. Die Sicherheit von Firmennetzen gegenüber Angriffen von außen wird immer noch vernachlässigt.

Offene Systeme und weltweite Vernetzung führen auch zu Ängsten und zum Wunsch nach Sicherheit, Vertraulichkeit und zum besseren Schutz der Privatsphäre.

Es gibt einen Grund, warum das Internet der letzten Jahre sehr anfällig gegen Angriffe reagierte und es dabei mangelnde Sicherheit besaß und überwiegend heute noch besitzt. In den Anfängen des Internet beabsichtigten die Entwickler ein Netz aufzubauen, was zum schnellen und reibungslosen Austausch von Informationen gedacht war. Mit dem Thema

Sicherheit beschäftigte man sich aus diesem Grund überhaupt nicht, weil man damals mit dem weltweiten Boom nicht gerechnet hatte. Über die Geschichte des Internets wird noch im späteren Kapitel ein kleiner Überblick gegeben.

1.2 Was ist Kryptographie und Verschlüsselung

Kryptographie ist wie wenn ich ein Dokument in einen Safe verstecke. Es muss aber die Möglichkeit geben, das der Angreifer an die Entwicklungspläne des Safes und noch hundert Safes gleicher Bauart mitsamt ihren Kombinationen kommt, damit man den Sperrmechanismus ausgiebig studieren kann. Kryptologie nennt man die Verschlüsselung, die sehr eng mit Mathematik verbunden ist. Wir brauchen Kryptographie aus dem Grund, weil das einfache Abhören der modernen Kommunikationsmittel wie Fax, E-Mail, Telefon, Mobilfunk, Datennetze usw. möglich sind und dies ein Eintritt in die Privatsphäre, das geheime Recht jedes Menschen, ist. Um ein sicheres Kryptosystem entwickeln zu können und um gute Systeme herzustellen, müssen Kryptologen wissen, wie Code-Knacker arbeiten. Die Kenntnis über die Methode der Verfahren ist das Mittel zum Ziel. Allgemein wurde gute Kryptographie als die „Grenze des Machbaren zu Erkennen“ definiert!

Die Theorie sagt uns: "Wir leben in einer Informationsgesellschaft!"

Da stellt sich die Frage, was Information eigentlich ist. Daher wird nun die allgemeine Informationstheorie erläutert.

Information ist an sich nicht greifbar. Man versucht Formeln aufzustellen und Einheiten zu kreieren, wie zum Beispiel die kleinste Informationseinheit des Computers, das Bit ist. Keine brauchbaren Informationen sind die, die bekannt sind oder die zu spät ankommen, die uninteressant sind und falsche. Information ist die Interpretation der Nachricht beim Empfänger. Durch Kommunikation lassen sie sich übermitteln. Technisch gesehen gibt es einen Sender und einen Empfänger, zwischen denen Signale in jeder beliebigen Art, wie zum Beispiel optische, akustische, tastsignalisierte, funksignalisierte, elektrische Impulse oder Lichtleiterimpulse in Lichtleiterkabeln ausgetauscht werden. Die Nachricht besteht dabei aus Zeichen, die aus einem Alphabet entspringen (häufig lateinisch). Zum Beispiel wird der ASCII-Code bei dem PC und das Morsealphabet beim Funkverkehr verwendet. Den Zeichen müssen jedoch Bedeutungen zugeordnet werden. Die Symbole sind die Schnittstellen zwischen Sender und Empfänger und tragen die Bedeutung der Information. Dies funktioniert nur, wenn sich Sender und Empfänger auf ein und denselben Code einigen. Das Problem ist, das digitale Nachrichten in Netzwerken und Telefonleitungen unverschlüsselt eine Chance bieten, dass sie eventuell gelesen, manipuliert oder verändert werden können.

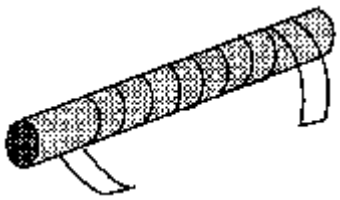
Keiner unser heutigen Systeme, weder die Wegfahrsperre am Auto noch das Instrumenten-Lande-System der Luftfahrt kann als vollkommen sicher betrachtet werden, eine 100%-ge Sicherheit gibt es nie. Das gilt auch in Sicherheitssystemen bei Computern! Die größtmögliche Sicherheit im Umgang mit Datenschutz und Sicherheit im Internet lässt sich am besten mit kryptologischen Verfahren gewährleisten. Diese können aber erst dann sicher sein, wenn mit ihr dementsprechend richtig umgegangen wird. Im Alltag begegnen uns sehr häufig Passwörter und PIN’s, die uns einen authorisierten Zugang gewährleisten. Das ist ein erstes Schutzsystem, was nur befugten Nutzern ein An- und Abmelden in einem System ermöglicht. Die Identität des Mensch wird überprüft. Doch bei falscher Hantierung mit den Passwörtern kann eine Manipulierung nicht ausgeschlossen werden. Der Faktor Mensch ist

eine der größten Schwachstellen. Einfache Passwörter, die aus simplen Reihenfolgen, wie Namen von Freunden, eigene Geburtstage usw., bestehen, bieten keinen großen Schutz. Kennwörter sollten vor gewaltsamen Angriffen, auch Bruteforce-Angriffen genannt, geschützt sein, d.h. sie sollten mindestens aus 7 Zeichen mit Zahlen und Sonderzeichen bestehen. Desto länger und variierter, desto besser.

Wir leben in einer Zeit, wo das Internet schon längst den Status eines Massenmediums erreicht hat. Für Datenschnüffler und Cyberkriminelle sind Internetanschlüsse wertvolle Eingangstore. Informationen können von Datenschnüfflern abgefangen und verändert werden und sogar Firmen in den Ruin treiben. Um solche Probleme zu vermeiden oder zu vermindern, bemüht man sich, Sicherheitssoftware mit der Kombination aus Zugriffskontrollen im Betriebssystem und moderner Verschlüsselungstechnik zu schaffen. Das eingegebene Passwort bei der Anmeldung wird zum Beispiel zusätzlich verschlüsselt. Bei (Zentral-)Banken sieht das etwas komplizierter aus, da es dort um wichtige Finanzen geht. Sobald eine Firma oder Unternehmen im Internet präsent ist, ist die Gefahr groß, Angriffen ausgesetzt zu sein. Einer Gefahr kann am besten durch Sicherheitsexperten vorgebeugt werden.

1.3 Geschichte

Die Anfänge der Kryptologie reichen zurück auf über 25.000 Jahre. Dabei wurde eine Nachricht auf einen schmalen Pergamentstreifen geschrieben und dieser dann in Form einer Winde um die Skytale gewickelt. Nur der Streifen wurde vom Kurier übermittelt. Der Empfänger besaß eine Skytale mit dem gleichen Radius und konnte den Streifen auf seine Skytale aufwickeln und für sich lesbar machen. Der Streifen war für andere Personen nutzlos, denn die Position der Symbole würde sich verändern und als unlesbar erkannt werden.



Berühmte und historische Personen, wie es zum Beispiel auch Leonardo da Vinci (1452-1519) war, hielt seine Notizen in Spiegelschrift geheim, um einen schnellen Zugriff vor Fremden zu vermeiden.

Edgar Allen Poe (1809-1849) lieferte in der Novelle vom Goldkäfer („Golden Bug“) ein instruktives Beispiel einer Geheimschrift und ihrer Entschlüsselung mit informationstheoretischen Überlegungen.

Auch Caesar benutzte ein einfaches, jedoch in damaliger Zeit, nutzvolles Verfahren, was später auch nach seinem Entdecker als das „Caesar-Verfahren“, das Verschiebechiffre, bekannt wurde. Man schreibt sich ein Alphabet auf und darunter eines in verschobener Variante. Das „Caesar-Verfahren“ verwendete den Abstand drei. Aus dem Buchstaben „A“ wurde „D“. Hierzu ein kleines Beispiel bei einem Abstand der Buchstaben von drei:

KLARTEXT: ABCDEFGHJKLMNOPQRSTUVWXYZ

Geheimtext: DEFGHIJKLMNOPQRTUVWXYZABC

Die erste und wirkliche Kunst am Verschlüsseln erfolgte in den beiden Weltkriegen. Die Kommunikation musste durch unterschiedliche Verfahren geheim gehalten werden.

Ein wichtiger Einschnitt in die Geschichte der Kryptographie machte die von der deutschen Wehrmacht im zweiten Weltkrieg eingesetzte Chiffriermaschine – die Enigma. Die Enigma wurde von Arthur Scherbius schon Jahre vor dem Krieg erfunden, aber sie brachte bis zu diesem Zeitpunkt noch keinen wirklichen Nutzen. Ihre Aufgabe war es, deutsche Frontbefehle und Geheiminformationen vor den Abfangeinrichtungen zu schützen, indem sie die zu übermittelten Informationen unkenntlich machte. Die Alliierten konnten zwar alles abfangen, jedoch konnten sie den Sinn des Buchstabensalats nicht verstehen bzw. verarbeiten. Die Chiffriermaschine arbeitete mit einem monoalphabetischem Chiffrierverfahren, ähnlich das von Cäsar, dass aufgrund des symmetrischen Stromlaufs ohne Veränderung der Einstellungen

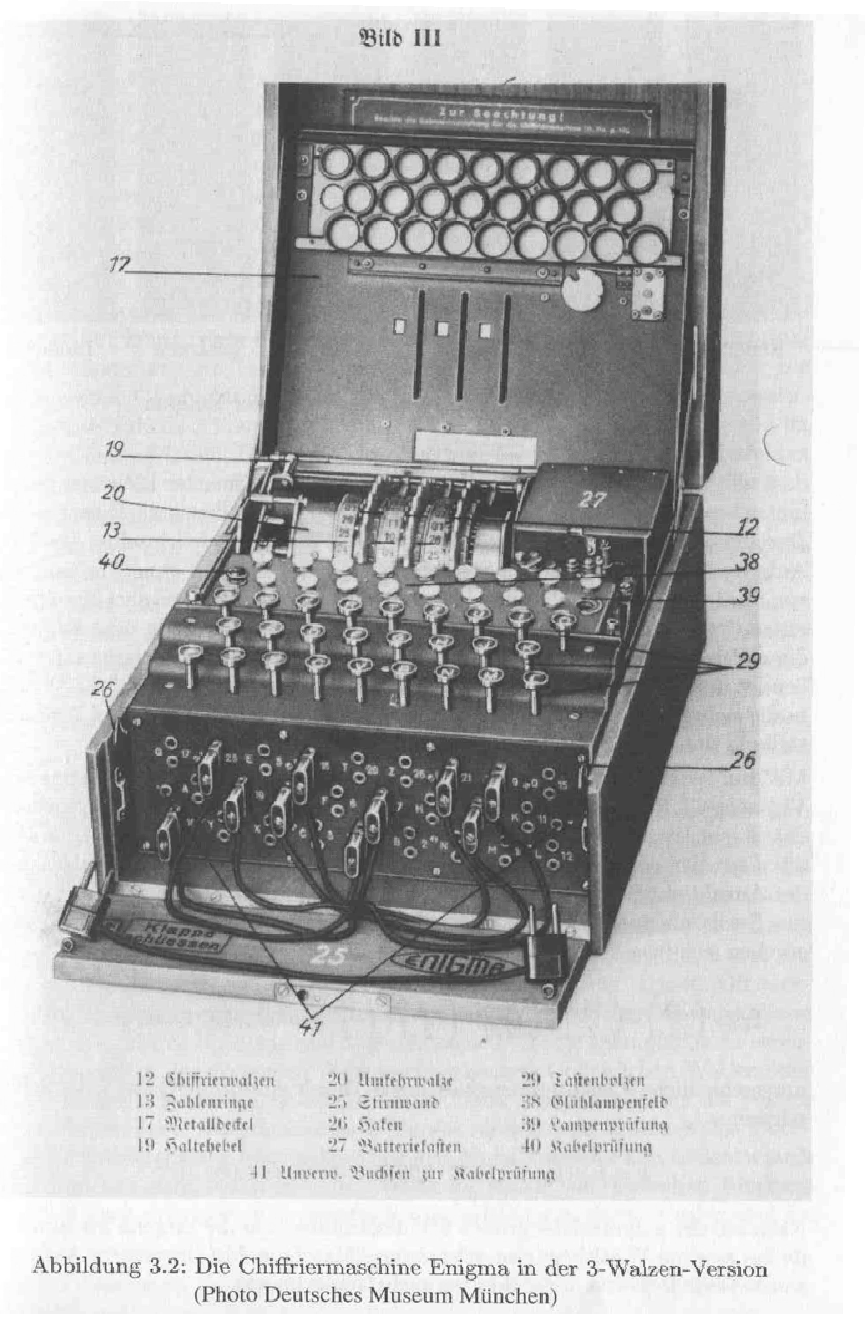


Abbildung 3.2: Die Chiffriermaschine Enigma in der 3-Walzen-Version
(Photo Deutsches Museum München)

Nachrichten sowohl Ver- als auch Entschlüsseln konnte. Die Funktion, die in der Enigma angewendet wird, stellt gleichzeitig die Umkehrfunktion dar.

Sie bestand aus 3 Walzen, 1 Steckverbindung und nutzte das Vigenère Chiffre. Durch die 3 Walzen und der Voraussetzung, dass das Alphabet 26 Buchstaben enthält, besaß es die Schlüssellänge k_a von 26 * 26 * 26 = 17576 ! Bei 5 vertauschten Buchstabenpaaren auf dem Steckbrett ergeben sich

k_s= (26) * (24) * (20) * (18) * (16) = 602350749000 ~ 6.10^{11} unterschiedliche Steckverbdingungen. Der Schlüsselraum k berechnet sich aus $k_s * k_a = 1.06*10^{17}$

Ein Angriff mithilfe der Bruteforce – Technik war damals unmöglich. Durch die fehlenden Digitalrechner war es unmöglich, alle gängigen Schlüssel bei einem Schlüsselraum von ca.$1*10^{17}$ durchzuprobieren. Eine einfache Änderung der Steckverbindung und Walzenstellung hätte diese Arbeit wieder zu Ende gebracht. Trotz der bekannten Funktionsweiße der Enigma, die die Alliierten besaßen, gab es genug Schutz. Trotzdem gelang es den Feinden, die Enigma zu knacken und wichtige Informationen dennoch abzuhören. Ein konstruktionsbedingter Schwachpunkt existierte dennoch. Der Schlüsselraum wird eingeschränkt, indem zum Beispiel ein Chiffrierzeichen an einer anderen aber ähnlichen Stelle im Klartext ausgeschlossenen werden kann. Wenn man weis, dass ein ‚p' in ein ‚f' verschlüsselt wird, dann weis man auch, aus einem ‚f' ein ‚p' wird. Durch die Kryptoanalyse ist dies zum Beispiel möglich.

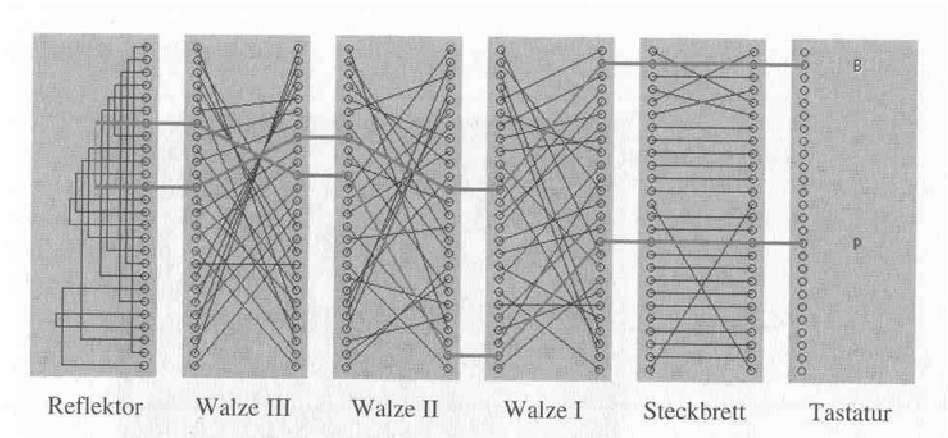


Abbildung 3.3: Verdrahtungsschema der Enigma

1923	Erfindung durch Arthur Scherbius zum Gebrauch für Geschäftsleute.
1925	Deutsche Marine kauft erste Enigmas.
1928	Landstreitkräfte kaufen Enigmas. Polnische Mathematiker beginnen mit der Kryptanalyse. Durch Zufall bekommen die Polen für kurze Zeit Zugang zu einer Enigma (ohne Wissen der Deutschen). Dadurch wird der Algorithmus bekannt, die Enigma ist aber noch nicht geknackt (Prinzip von Kerkhoffs in Abschnitt 2.2).
1930	Verbesserung durch Hinzufügen des Steckbretts.
1933	Einsatz der ersten elektromechanischen Computer, **Bombe** genannt (tickt wie eine Bombe), zum erfolgreichen Knacken der Enigma durch die Polen.
1938	Die Enigma wird durch zwei weitere austauschbare Walzen wieder sicher (drei beliebige der fünf Walzen werden eingesetzt).
1939	Der Großangriff der Briten auf die Enigma in Bletchley Park beginnt und ist auch bald erfolgreich. Alan Turing baut verbesserte Bomben, die schon eingeschränkt programmierbar sind (erste Computer).
1942	Neue Enigma mit vier Walzen ist wieder sicher und wird im U-Boot-Krieg gegen die amerikanischen Versorgungskonvois eingesetzt.
1943	Nach fast einem Jahr wird die 4-Walzen-Enigma geknackt, u. a. helfen Wettermeldungen deutscher U-Boote, sog. Menus für die Bomben bzw. Computer zu erstellen. Hier kam **Colossus**, der erste programmierbare britische Computer zum Einsatz. Er arbeitete mit Röhren und als Programmspeicher diente ein endlos umlaufender Lochstreifen.

Tabelle 3.7: Geschichte der Enigma in Stichworten

Viele Jahre war die Kryptographie dem Militär vorbehalten. Die NSA und andere weltweite Geheimdienste gaben viel Geld aus, um ihre eigene Kommunikation zu sichern und Andere zu knacken. Die Kryptographie wurde seit dem zweiten Weltkrieg ausschließlich vom Militär benutzt. Während der letzten 20 Jahre ist die öffentliche Anwendung der Kryptographie in den öffentlichen Haushalten explosionsartig gestiegen.

Da die Regierung das Recht besitzt, besser gesagt sich nimmt, private Kommunikationen abzuhören, benötigen wir die Sicherheit, um unsere Privatsphäre zu schützen.

Die moderne Datenverschlüsselung findet jedoch im modernen Internet ihren Platz. Die Geschichte des frühen Internets beginnt in den frühen 60er Jahren – 1962, um genau zu sein. Eine kleine Gruppe Forscher der Vereinigten Staaten waren damit beschäftigt, ein Kommunikationsnetzwerk zu schaffen, dass einen nuklearen Angriff überleben könnte und

ausschließlich militärischen Zwecken diente. Dieses sollte jedoch nicht zentral kontrolliert werden. Alle Rechner sollen aber miteinander kommunizieren können und auch bei Ausfall eines Knotenpunktes selbständig weiterlaufen. Früher wurden zentralisierte Daten auf Großrechnern gespeichert, die von jedem Terminal aus erreichbar und abrufbar waren. Diese effektive Vernetzung hatte eine schwerwiegende Auswirkung auf die Sicherheit des Datennetzes. Wäre ein Großrechner ausgefallen, so hätte kein Terminal mehr miteinander kommunizieren können. Man musste daher ein „dezentralisiertes“ Netz aufbauen, wo die Datenpakete selbständig und dynamisch den Weg finden müssen. Die Entwickelung dieses Netzes, was ausschließlich unter Aufsicht von Paul Baran entwickelt wurde, verzögerte sich aufgrund fehlender finanzieller Möglichkeiten bis zum Jahre 1969. Die Entwicklung des ARPANET war beendet. Damals waren nur 4 Universitätsrechner mit dem Telefonnetz miteinander verbunden! In dieser Zeit beschäftigten sich zwei intelligente Männer in ihrer High School Zeit mit dem Vernetzen von Computern. Beide sind heute Milliardäre. Einer davon war Bill Gates! Weiterhin entstand in den folgenden Jahren das bis heute sehr erfolgreiche Betriebsystem UNIX und die Programmiersprache C. Diese beiden Entwicklungen eines Betriebssystem und einer geeigneten Sprache, die den Datenfluss steuern sollte, waren ein großer Sprung zum modernen Internet. Denn 1972 erreichte das ARPANET eine bahnbrechende Entwicklung in Sachen Kommunikation – die elektronische Post – E-Mail – war geboren. Im Jahre 1974 wurde eine andere entscheidende Erfindung gemacht. Vinton Chef und Robert Khan erfanden ein Protokoll, was das heutige Internet ausmacht und seit daher als Internetstandard für den Datenaustausch in jedes Computersystem integriert wurde: Das Transmission Control Protocol – TCP. 1975 war das ARPANET ein weitreichend vollfunktionsfähiges Netzwerk. In den darauffolgenden Jahren klinkten sich immer mehr Universitätsrechner der USA in das ARPANET ein. Bis zum Jahre 1990 wuchs die Anzahl der Hosts bis auf 300.000 an. In dieser Zeit wurde das Internet ausschließlich von militärischen oder akademischen Personal genutzt. Für kommerzielle Zwecke war es verboten, das Internet zu benutzen. 1991 besaßen die ersten kommerziellen Unternehmen die Möglichkeit, über Netzwerkbandbreite zu verfügen. Die ersten Internetserver, auch Backbones genannt, etablierten sich, um einen öffentlichen Zugang zu bekommen.

Weiterhin gestalteten sich Computer und Telefon zu einer festeren Einheit. Neue Technologien drangen in alle Lebensbereiche vor, z.B. in Autos, Kühlschränken, Laptops usw. Ein freier Verkehr auf der Datenautobahn, die ohne Verwaltung auskam, öffnete vielen Menschen neue Dimensionen, denn im Internet ist zu jedem denkbarem Thema, ob rassistisch oder wissenschaftlich, etwas zu finden.

Erst seit 1995 zog die Entwicklung der grafischen Benutzeroberfläche zur Nutzung des Internets an, die Browser wie Netscape und der Internet Explorer eroberten den Markt. Von diesem Augenblick war das Internet für jeden zugänglich, der einen Computer, einen Browser und eine Maus besaß. Großartige Unternehmen hatten sich explosionsartig gebildet, denn durch die Zunahme der Internet Service Provider schlossen sich Tausende dem Netz an.

Laut der Dataquest-Studie nutzten Ende 1997 weltweit 82 Millionen PC’s das Internet. Das die 268 Millionen Grenze heute schon längst überschritten wurde, ist sehr wahrscheinlich.

1.4 Aktuelle Beispiele aus der Welt

Am Rande möchte ich noch kurz die weltpolitische Situation ansprechen. Die NSA (National Security Agency) ist das offizielle Sicherheitsorgan der US-Regierung. 1952 wurde es von Harry Truman gegründet. Die Existenz der NSA blieb sehr lange geheim, da sie sich mit dem Abhören von Kommunikationswegen beschäftigt. Ihre wichtigsten Aufgaben sind das Abhören aller ausländischen Kommunikationswege und die gleichzeitige Dekodierung dieser Daten, das Durchführen von kryptographischen Forschungen und der gleichzeitige Schutz beim Abhören geheimer Informationen der US-Bevölkerung. Die NSA ist der weltweit größte Arbeitgeber von Mathematikern und kann somit zahlreiche Verfahren in der Praxis knacken. Das **ECHELON** ist zum





Beispiel ein Projekt zwischen der NSA und weltweit verbündeten Geheimdiensten. Es entspricht einem weltweitem Abhörsystem, dass routinemäßig Internetleitungen und Sattelitenverbindungen abhört. Doch dies kann man durch zunehmender starker Kryptographie leicht aushebeln. Seit dem 11.September 2001 hat sich die Lage rapide verändert. Das Abhören wurde immer wichtiger, um die Weltbevölkerung vor Terroranschlägen zu verhindern, die nachweislich auch vom Internet aus geplant wurden. Doch die starke Kryptographie, die der allgemeinen Bevölkerung im Laufe der Jahre zugänglicher geworden ist, erschwert der Polizei die Verbrechensbekämpfung. Angeblich wurden die Attentate der Terrorristen in Bilder verschlüsselt und versteckt. Die Steganographie diente ihnen als wichtiges Hilfsmittel.

Erst im Jahre 1997 wurde die Legalisierung zur Verschlüsselung persönlicher Daten mit dem „Signaturgesetz“ in Deutschland besiegelt.

Durch starke Kryptographie wird die Privatsphäre und die Identität bei der digitalen Kommunikation gesichert. Dadurch gelangen mächtige Geheimdienste nicht mehr so leicht an vertrauliche Daten.

Im Laufe der Jahre wurden eine Menge großartiger Datenverschlüsselungsprotokolle entwickelt, die aber alle entweder von Kryptologen, Code-Knackern oder Computern geknackt wurden. Dieser Vorgang, ein wirklich sicheres Verfahren zu entwickeln, ist noch längst nicht abgeschlossen und wird auch viele Kryptologen und Regierungen in Zukunft großes Kopfzerbrechen bereiten.

Auszug aus daily-newsletter@linux05.wekanet-team.de

26.08.02 18:55

+++ Professor: RSA ist weiter sicher +++

Die seit 25 Jahren angewandte Verschlüsselungsmethode RSA läuft nicht Gefahr, dauerhaft entschlüsselt zu werden. Mit dieser Aussage tritt ein Informatik-Professor einem Zeitungsbericht entgegen.

Aufregung bei den Kryptierern und in der Online-Geschäftswelt. In einem Bericht der Frankfurter Allgemeinen Sonntagszeitung hieß es, dass der Verschlüsselungsmechanismus RSA kurz vor der Dechiffrierung stehe. Die Zeitung schrieb, ein amerikanischer Wissenschaftler plane eine Rechenmaschine, die in der Lage sei, RSA zu knacken. Sollte diese Behauptung des US-Mathematikers Daniel J. Bernstein zutreffen, wäre auf einen Schlag der komplette Internet-Handel ungeschützt. Hier wie auch bei der Chiffrierung im herkömmlichen Business verlässt man sich nämlich seit einem Vierteljahrhundert auf RSA. Für den Trierer Informatik-Professur und Leiter des Instituts für Telematik, Christoph Meinel, ist die gegenwärtige Diskussion jedoch eher aus der Luft gegriffen. Selbst wenn es Bernstein schaffe, dreimal so große natürliche Zahlen in ihre Faktoren zu zerlegen, sei das noch nicht das Ende für RSA, heißt es in einer Stellungnahme des Instituts, die auch die F.A.Z. veröffentlichte. Der Wettlauf zwischen Kryptierern und Hackern sei so alt wie das System. Wenn Bernstein eine Methode gefunden habe, den jetzigen RSA-Standard zu knacken, müsse man einfach wieder einen Schritt weitergehen. Beispielsweise sei es möglich, den heute verwendeten 1024-Bit-Schlüssel durch einen 2048-Bit-Schlüssel zu ersetzen. Meinel plädierte dafür, diesen 2048-Bit-Schlüssel spätestens von 2006 an einzusetzen.

http://www.faz.de F.A.Z./Sonntagszeitung http://www.ti.fhg.de - Institut für Telematik

http://www.heise.de/newsticker/data/nl-07.12.99-000/

+++ Handy-Verschlüsselung angeblich geknackt +++

Die beiden israelischen Kryptologen Alex Biryukov und Adi Shamir haben Medienberichten zufolge den Verschlüsselungsalgorithmus geknackt, der GSM-Handy-Telefonate auf der Funkstrecke zur Mobiltelefon-Basisstation schützt. Das Verfahren soll mit einem handelsüblichen PC auskommen, der mit 128 MByte RAM und zwei 73 GByte Festplatten ausgestattet ist. Auf diesem soll das Programm der Forscher durch eine Analyse der ersten zwei Gesprächsminuten in weniger als einer Sekunde den verwendeten Schlüssel errechnen können.

Umstritten ist, ob und mit welchem Aufwand es möglich ist, die Gespräche überhaupt abzufangen, um sie anschließend zu dechiffrieren. Eines zeigen die Vorfälle um die GSM-Verschlüsselungsalgorithmen A5/1 und A5/2 aber schon jetzt deutlich: Der Versuch, Krypto-Verfahren geheim zu halten, dient nicht der Sicherheit. Das hat anscheinend auch die GSM-Association gelernt: Ihr Sicherheitsdirektor James Moran äußerte dem Online-Magazin Wired gegenüber, dass man künftige Algorithmen von vorneherein offenlegen will, um der Fachwelt eine Prüfung zu ermöglichen. (nl/c't)

Freitag, 21. Februar 2003 17:56

+++ SSL geknackt +++

Schweizer Sicherheitsexperten wollen die bislang sichere SSL-Verschlüsselung geknackt haben.

Das Team des "Security and Crypthography Laboratory" des technischen Instituts Lausanne stellt auf seiner (http://lasecwww.epfl.ch/memo_ssl.shtml) Homepage eine detaillierte Beschreibung der möglichen Sicherheitslücke bereit. Nach eigenen Angaben hätten die Experten rund eine Stunde benötigt, um die SSL-Verschlüsselung außer Kraft zu setzen. Danach sei ein Zugriff auf die Datenverbindung zwischen Client und Server möglich gewesen.
Geknackt worden sei im Test das Passwort einer SSL-Verbindung zwischen einem Mailserver und Outlook Express 6. Doch wie bei jeder Sicherheitslücke mussten wieder einige Besonderheiten erfüllt sein, damit die Wissenschaftler die Verbindung "aufbrechen" konnten. Beobachtet wurde die Antwortzeit des SSL-Servers auf gefälschte Anfragen. Danach fingen die Experten eine Anfrage an den Server ab, und schickten eine falsche weiter. Aufgrund der Serverantworten entwickelten und rekonstruierten die Forscher den entsprechenden Inhalt und versuchten so, sich in die Verbindung einzuklinken.
SSL ist die Abkürzung für Secure Sockets Layer und wird vom OpenSSL-Projekt verwaltet. Die Verschlüsselung wird oft bei der Übertragung von Adress- und Bankdaten, aber auch beim Online-Shopping verwendet. Aufgrund der Schweizer Tests haben die SSL-Entwickler bereits aktualisierte Versionen bereitgestellt, um die Sicherheitslücke zu schließen.
(http://lasecwww.epfl.ch/memo_ssl.shtml) Security and Crypthography Laboratory

Meldung vom 30.01.2001 18:22

+++Hardware-Verschlüsselung in Standard-PCs+++

Der von IBM im September 1999 vorgestellte Sicherheitschip soll jetzt Einzug in Rechner erhalten. Die Trusted Computing Platform Alliance (TCPA), eine Gruppe von rund 145 Technologiekonzernen, gibt am heutigen Dienstag genauere Angaben für die Implementierung durch die PC-Hersteller heraus. IBM, ein Gründungsmitglied der TCPA, stellt mit dem Sicherheitschip die Basistechnologie der beschlossenen Spezifikationen. Es handelt sich dabei um ein 256-Bit-Chip, der als fester Bestandteil von Mainboards mittels Public-Key-Kryptographie für Datensicherheit sorgen soll.

Aus der Entwicklung dieses Chips ist dann im Oktober 1999 die TCPA entstanden – Gründungsmitglieder waren neben Big Blue noch Compaq, Hewlett-Packard, Intel und Microsoft. Ziel

der Organisation sei ein Standard für eine sichere Rechnerumgebung sowohl auf Hardware- als auch auf Software-Ebene zu etablieren. "Der Chip ermöglicht Anwendern quasi eine SmartCard auf dem Mainboard ihres Rechners zu verwenden. Ver- und Entschlüsselung finden dann in der gesicherten Umgebung des Chips statt", erläutert Arsen Varjabedian, ein IBM-Sicherheitsexperte.

Außergewöhnliche Kosten sollen auf den Anwender nicht zukommen – nach Schätzungen belaufen sich die Zusatzkosten auf rund zwei US-Dollar pro Rechner. Allerdings können die Kosten je nach Art der Implementierung durch die Hersteller variieren. (pab/c't)

10. November 2002

+++ Es wird munter weitergelauscht +++

Echelon, das mittlerweile bekannte Spionagenetz, ist zum europäischen Thema geworden. Doch unternommen wird nichts.

Das Europäische Parlament hat bereits seit einem Jahr seine Untersuchungen zu dem Spionagenetz abgeschlossen, doch unternommen wird nichts. Das Lauschen geht munter weiter, ohne das jemand etwas dagegen tut. In einer Anfrage des Parlaments soll jetzt geklärt werden, warum weder Rat noch Kommission gehandelt haben. Zwar seien einige Initiativen gestartet worden, um die elektronische Kommunikation sicherer zu machen, aber es seien noch weitere Maßnahmen nötig, um Bürger und Firmen gegen illegale oder missbräuchliche Abhörung zu schützen. Industriespionage und die missbräuchliche Nutzung von nachrichtendienstlichen Informationen müsse verhindert werden. Mit den USA soll deswegen ein Abkommen ausgehandelt werden, durch die EU-Bürger und Firmen vor den Abhörpraktiken geschützt werden sollen. Gleichzeitig soll aber die Kooperation der unterschiedlichen Nachrichtendienste verbessert werden, um den Kampf gegen Terrorismus und organisierte Kriminalität effektiver zu machen. Mit Echelon werden bereits seit einigen Jahren nicht zur Telefongespräche, sondern auch der Datenverkehr wie e-Mails oder Faxe überwacht. In Deutschland haben die USA einen Echelon-Horchposten in Bad Aibling installiert.

(http://www.europarl.eu.int) Europa-Parlament

Meldung vom 18.02.2003 16:16

+++Datenschützerin kritisiert zunehmende Überwachung der Bevölkerung+++

Die nordrhein-westfälische Datenschutzbeauftragte Bettina Sokol hat einen deutlichen Abbau von Persönlichkeits- und Freiheitsrechten kritisiert. Nach den Terroranschlägen vom 11. September 2001 seien die Möglichkeiten zur Überwachung der Bevölkerung ausgebaut worden, sagte Sokol bei der Vorlage des 16. Datenschutz- und 1. Informationsfreiheitsberichtes 2003. Die Nachrichtendienste könnten jetzt personenbezogene Auskünfte bei Banken, Fluggesellschaften sowie Post- und Telekommunikationsunternehmen einholen.

Auch bei der Telefonüberwachung seien die Befugnisse der Strafverfolgungs- und Verfassungsschutzbehörden erweitert worden, kritisierte die Datenschutzbeauftragte...

Im nicht-öffentlichen Bereich wachse eine Kultur des Misstrauens, bemängelte die Datenschützerin. "Im Internet sprießen so genannte Warndateien wie Pilze aus dem Boden", sagte Sokol. (...)

Eine erste Bilanz des Informationsfreiheitsgesetzes, das in Nordrhein-Westfalen vor rund einem Jahr verabschiedet wurde, fällt laut Sokol "überwiegend positiv" aus: "Mit dem Informationsfreiheitsgesetz

sind die Rechte der Bürgerinnen und Bürger gestärkt worden. Transparenz von Verwaltungsentscheidungen ist ein wichtiger Bestandteil einer funktionierenden Demokratie." (jk/c't)

Meldung vom 19.02.2003 13:52

+++Deutschland ist weltweit Spitze beim E-Commerce+++

Das in Genf angesiedelte Weltwirtschaftsforum hat am heutigen Mittwoch in seiner Heimatstadt die zweite Ausgabe des "Global Information Technology Report" vorgestellt. Kern des mehrere hundert Seiten umfassenden Wälzers zur Lage der Informationsgesellschaft in den Jahren 2002/2003 ist die Einordnung von 82 Nationen in eine Rangfolge entlang des so genannten "Network Readiness Index". Für manche Beobachter überraschend nimmt die deutsche Wirtschaft darin die weltweite Spitzenposition ein, wenn es um die kommerzielle Nutzung des Internet geht. Die Autoren der Studie stellen deutschen Unternehmen im Business-to-Business- und im Business-to-Consumer-Bereich generell hervorragende Noten aus. Führend seien sie im Online-Marketing und bei der Entwicklung von Applikationen fürs drahtlose Netz. Auch für die Koordination von Beziehungen zu Kunden und Lieferanten und für ihre Präsenz im Web erhalten deutsche Firmen beste Zensuren.

2. Theorie der Verschlüsselung

2.1 Grundlagen der Verschlüsselung und Zahlentheorie

In diesem Abschnitt werden einige wichtige Begriffe und Theorien zur Datenverschlüsselung erklärt sowie näher beschrieben. In der Verschlüsselungstheorie verwendet man sogenannte Chiffren, die den Klartext unschlüssig machen sollen. Deswegen entwickelte man verschiedene Chiffreverfahren. Die Grundlage der Verschlüsselung verwendet entweder *Stromchiffren*, die ein Zeichen nach dem anderen verschlüsseln, oder *Blockchiffren*, die Nachrichten in Blöcke zerteilt und diese Blöcke dann einzeln verschlüsselt. Das **Kryptosystem** ist dann die Vereinigung von Algorithmus, zugehörigem Schlüssel und der verschlüsselten Nachricht. Der Schlüssel im Algorithmus soll eine natürliche Zahl, dargestellt im Binärsystem bzw. „Bits“, sein. Der Algorithmus sollte allgemein bekannt sein und nur der zugehörige Schlüssel muss geheim gehalten werden. Das garantiert eine Prüfung des Kryptosystems, die das Verfahren verbessern könnte. Ein anderer wichtiger Begriff der Kryptographie nennt sich die **Kryptoanalyse.** Dies ist die Kunst des vollständigen Aufbrechens des Algorithmus, des jeweils verwendeten Kryptosystems. Wenn man den Schlüssel *K* zum Algorithmus gefunden hat, dann kann man damit die verschlüsselte Nachricht entschlüsseln, bei der Voraussetzung, dass der Algorithmus bekannt ist. Eine andere Möglichkeit nennt sich die lokale und globale Deduktion. Bei der Lokalen besitzt man einen abgefangenen Chiffretext und schließt aus diesen den Klartext heraus. Und bei der Globalen findet man zum Entschlüsselungsverfahren des Schlüssels *K* einen äquivalenten und alternativen Algorithmus ohne Kenntnis des Schlüssels. Bei der zusätzlichen Informationsdeduktion können nur eingeschränkte Informationen über den Schlüssel oder den Klartext ermittelt werden.

Um die Information, Nachricht, Klartext oder wie auch immer undeutlich zu machen, gibt es zwei hauptsächliche Arten der Geheimhaltung: Die **Steganographie** und die **Kryptographie!**

Bei der Steganographie ist es die Absicht, geheime Nachrichten zu verbergen. Unsichtbare Tinte und versteckte Texte in Bildern, durch Veränderung von Pixeln durch Bits, sind hierfür typische Beispiele. Bei der Kryptographie soll es nicht die Absicht sein, die Nachricht zu verstecken, sondern das diese von dem Gegner nicht entziffern werden kann.

Die Steganographie ist der Begriff für die Wissenschaft mit dem Ziel, Nachrichten zu verstecken. Es handelt sich hierbei um das Prinzip, dass es keine Eigenschaft gibt, an der man erkennen könnte, dass eine geheime Nachricht vorliegt. Die eigentliche Information ist nicht die Nachricht, sondern deren Bedeutung. Dabei werden zum Beispiel geheime Nachrichten in Texten, in Computergrafiken und im Strom, der digitale Signale wie bei ISDN überträgt, versteckt. Auch wenn die Gegner über die Methode der Verschlüsselung Bescheid wissen, muss die Steganographie die Information vor der Entdeckung schützen. Im Zeitalter des Computers werden einzelne Bits der geheimen Information in den Bytes der unwichtigen Nachricht versteckt. Bei Computergrafiken verändert man das Bit mit dem niedrigsten Wert, um die Farben einiger Pixel zu verändern. Die Veränderung des Bildes fällt bei der Intensität und Schattierung, durch abgestufte Farben der Farbpaletten, nicht auf. Oder auch das „Rauschen“ der Sprachübertragung kann man sich zu nutze machen, indem man das analoge Rauschen in der Leitung oder die akustische Hintergrundkulisse verwendet. Durch die

Erzeugung künstlichen Rauschens und das darin Einschleusen von Information, macht es möglich, geheime Nachrichten zu übertragen. Die Entropie, eine eindeutige und unverwechselbare Grundeigenschaft eines Zustandes oder Sache, des Grundrauschens wird durch Entropie der geheimen Information ersetzt. Gleichzeitig muss auch auf die Charakteristik des Phasenspektrums geachtet werden, so dass sich das Modell des künstlichen Rauschens vom originalen Modell des Echtzeitrauschens wenig unterscheidet.

Für die ***Kryptographie*** gibt es verschiedene Verfahren, die man anwenden kann. Leicht nachzuvollziehen sind die zwei ältesten Verschlüsselungsverfahren *Substitution* und *Transposition*. Bei der Substitution werden die Zeichen des Klartextes systematisch durch Zeichen aus einem Geheimtextalphabet ersetzt. Durch Transposition werden dagegen die Zeichen des Klartextes systematisch an eine andere Position gesetzt.

Zum einen unterteilt man einfache Chiffren der **klassischen Kryptographie** in homophone, polyphone und Produkt-Chiffren. Bei den homophonen Chiffren werden verschiedene Geheimzeichen zu einem Klartext dechiffriert (aus A wird 111,1,2,21) und bei der polyphonen Chiffrierung bedeutet ein Geheimtextzeichen mehrere Klartextzeichen. Die Produktchiffrierung ist das Produkt aus der Kombinierung vieler schwacher Verfahren und daraus wird dann ein viel stärkeres Verfahren gebildet. Schwache Verfahren sind zum Beispiel Substitution, Transposition, Permutation, Addition und Multiplikation. Produktchiffren wie DES und FEAL vereinen diese schwachen Verfahren miteinander und bilden daraus ein sehr gutes Verfahren.

Die Kanalkapazität bestimmt immer die Datenmenge pro Zeiteinheit und wird durch folgende Formel errechnet:

$C = 2 * v_G * H$ [bit/s]

v_G = Bandbreite in Hz

H = Entropie in Bit

Die Telefonleitung besitzt zum Beispiel eine Bandbreite von $3*10^3$ Hz. Jetzt stellt sich nur noch die Frage, was Entropie eigentlich bedeutet. Die Entropie besitzt die Eigenschaft der Information, welchen Informationsgehalt die einzelnen Zeichen theoretisch besitzen. Mit ihr kann man die enthaltene Information „ergreifen“. Sie ist der Schlüssel zur Information und stellt den zentralen Punkt bei Texten dar. Die Entropie aus der Thermodynamik besagt, dass ein System unter gegebenen Bedingungen von selbst in einen wesentlich unwahrscheinlichen Zustand übergeht. Auch den Informationsgehalt von Zeichen kann man messen. Die Entropie berechnet sich aus den Wahrscheinlichkeiten des Auftretens einzelner Zeichen. Je unwahrscheinlicher ein Zeichen, desto höher die Entropie, also der Informationsgehalt.

In der KLASSISCHEN VERSCHLÜSSELUNGSTHEORIE unterteilt man einfache Substitutionsverfahren in monoalphabetische, homophone und polyalphabetische Chiffrierungen.

Die **monoalphabetische Chiffrierung** benutzt ein Chiffrieralphabet, wo jedes Zeichen des benutzten Klartextalphabetes zu demselben Geheimtextzeichen chiffriert wird (Beispiel: Caesar-Verschlüsselung). Es ist ein schwaches Verfahren, denn wenn ein einziges Zeichen

identifiziert wird, dann wird die restliche Reihenfolge des Geheimalphabetes offengelegt. Nur der Anfangspunkt des Alphabetes ändert sich dabei. Indem man sich die Eigenschaften der Wahrscheinlichkeiten und die Entropie des Textes zu Hilfe nimmt, ist dies kein großes Problem. Man sucht nach Häufigkeiten der einzelnen Buchstaben im Geheimtext und danach benutzt man eine Tabelle mit den bekannten Häufigkeiten. Unterteilt man die Buchstaben nach der größten und kleinsten Häufigkeit, so erkennt man den Verschiebungsfaktor (Offset) an dem Buchstaben der größten Auftrittswahrscheinlichkeit. Diese Unterteilung der Häufigkeit unterstützt das Finden der wichtigsten Buchstaben. In der deutschen Sprache decken die Buchstaben „e“ und „n“ fast ein Drittel aller Vorkommen ab. Der Beweis der Wirkungslosigkeit wird im folgenden Beispiel anschaulich verdeutlicht :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

VWXYZABCDEFGHIJKLMNOPQRSTU

Klartext: SEIN ODER NICHT SEIN DAS IST HIER DIE FRAGE

Geheimtext: NZDI JYZM IDXCO NZDI YVN DNO CDZM YDZ AMVBZ

Häufigkeit der Buchstaben im Geheimtext:

N : 4 Z : 5 D : 4 I : 3 J : 1 Y : 3 M : 3

X: 1 C: 2 O: 2 N: 4 V: 2 A: 1 B: 1

Der Buchstabe Z kommt mit der Anzahl 5 am häufigsten vor. Der Offset beträgt also 5 Abstände. Die Buchstaben wurden im Alphabet um 5-stellen verrückt. Das Chiffrierverfahren „Rot13“ benutzt den Offset 13. Das Verfahren ist sehr einfach aufgebaut und zu knacken. Man denkt sich einen Schlüssel aus, den man vor die restlichen Buchstaben des Alphabets setzt, damit jeder Buchstabe nur einmal vorkommt.

SCHLÜSSEL: CAESAR

ABCDEFGHIJKLMNOPQRSTUVWXYZ

CESARZYXWVUTQPONMLKJIHGFDB

Natürlich kann man das Alphabet auch ohne einen Schlüssel durcheinander bzw. verwürfeln wie man möchte, doch am Ende wird immer jedem Chiffrebuchstabe ein Klartextbuchstabe zugeordnet. Daraus ergeben sich 27! (Fakultät) Möglichkeiten zur Durchwürfelung des Alphabets. Obwohl es soviel Möglichkeiten gibt, ist eine Lösung in wenigen Minuten offengelegt.

Um die Entropie eines Klartextes weiter zu verschleiern, ordnete man zu jedem Klartextzeichen mehrere Geheimzeichen zu. Diese Art der Verschleierung nennt man die Homophonen Chiffren. Beim Verschlüsseln wird zufällig für jedes Klartextzeichen immer ein anderes Geheimzeichen gewählt. Alle Geheimzeichen kommen gleichhäufig vor. Dadurch wird die Analyse des Textes erschwert. Dennoch ist das Verfahren knackbar. Durch die

charakteristische Verteilung von Paaren der Geheimzeichen kann man Teile der Klartextzeichen herausfinden.

Bei **den polyalphabetischen Chiffreverfahren** wird jedes Klartextzeichen auf unterschiedliche Chiffretextzeichen abgebildet. Die Homophonen Chiffren sind eine spezielle Untergruppe, die die Häufigkeit der Klartextzeichen verschleiert, indem jedes Zeichen im Geheimtext gleich häufig vorkommt. Die Sicherheitslücke besteht nur darin, dass man mit statistischen Angriffsmethoden die Häufigkeit von Paaren testen kann. Eine anderes Chiffre, das Vigenère-Chiffre oder das Verschiebchiffre, nutzt das Vigenère - Quadrat zur Verschleierung der Buchstaben. Wir wählen uns ein Schlüsselwort *K* : *geheim* und einen Klartext P : *dieloesunglautetx* und stellen danach folgendes Schema auf:

Schlüsselwort K: GEHEIMGEHEIMGEHEI --- Suche Buchstabe in Zeile
Klartext P: DIELOESUNGLAUTETX ---Suche Buchstabe in Spalte

Chiffretext C: JMLPWQYYUKTMAXLXF

Die Buchstaben vom Schlüsselwort suchen wir in der Zeile und die Buchstaben des Klartextes suchen wir in der Spalte des Vigenère – Quadrat und folgen dann den waagerechten und senkrechten Linien, die auf einen neuen Buchstaben treffen.

Nehmen wir an das Schlüsselwort wäre "FAUST". Wenn man den Klartext verschlüsseln möchte, sucht man in den Zeilen den Anfangsbuchstaben des jeweiligen Klartextbuchstaben und in den obigen Spalte den Buchstabe des jeweiligen Schlüsselwortes Geheimwortes. Die Zeile und Spalte kreuzen sich in einem neuen Buchstaben, der gesuchte Geheimbuchstabe. Dies wird solange wiederholt, wie lang auch der Klartext ist. Die Analyse des Geheimtextes fällt nun wesentlich schwieriger aus.

<u>Beispiel:</u>

SCHLÜSSEL : FAUSTFAUSTFAUST

KLARTEXT : HEXENEINMALEINS

GEHEIMTEXT : MERWGJIHEAQECFL

Vigenère – Quadrat:

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Chiffretext 0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Abbildung 3.1: Das Vigenère-Quadrat

Beispiel einer verbundenen XOR-Verknüpfung:

KLARTEXT: 01000001

SCHLÜSSEL: 10101010

GEHEIMTEXT: 11101011

SCHLÜSSEL : 10101010

KLARTEXT: 01000001

Bei der XOR-VERBINDUNG entsteht immer eine 1 wenn beide beteiligten Bits ungleich sind und eine 0 resultiert bei 2 gleichen Bits.

Die Kryptoanalyse des Vigenère – Quadrat funktioniert ganz einfach. Man untersucht den Geheimtext nach Wiederholungen von Zeichenfolgen von mindestens 3 Zeichen und misst deren Abstand. Je länger die gefundene Zeichenfolge ist, desto größer ist die Wahrscheinlichkeit, dass der Abstand ein Vielfaches der Schlüssellänge ist. Eine andere Idee zur Analyse des Verfahrens besteht darin, dass man zuerst sagt, dass alle Buchstaben innerhalb der Teiltexte nicht zufällig verteilt sind. Gedacht sei dabei, die Schlüssellänge näherungsweise zu bestimmen. Man untersucht die Häufigkeiten der Buchstaben, indem man die Wahrscheinlichkeit dafür errechnet, das 2 zufällige gewählte Buchstaben mit beliebigen Abstand gleich sind.

Ein ideales und perfektes Chiffriersystem wäre das Vigenère – Quadrat mit unendlichen langem Schlüsselwort. Dieses Schemata nennt man ein **One-Time-Pad**, wo die Sicherheit mathematisch garantiert ist. Ein beliebiger Klartext M und ein beliebiger Chiffretext C müssten statistisch unabhängig voneinander sein. Das theoretisch und praktisch unknackbare Verfahren, ONE TIME PAD, wurde nach Gilbert S. Vernam (1890 bis 1960) von einem Ingenieur bei AT&T entwickelt. Ein bestimmter Schlüssel wird mit dem Text verknüpft. Der Schlüssel muss genauso lang wie der Klartext sein, streng zufällig gewählt werden und nur ein einziges mal verwendet werden und dann nie wieder. Und genau das ist das Problem, denn bei symmetrischen Verfahren muss der Empfänger den Schlüssel auf einem sicheren Kanal erhalten. Da der Schlüssel immer mehr als einmal verwendet wird, ist das Verfahren nicht praktikabel. Weiterhin verdanken es Angreifer der menschlichen Trägheit und Schusseligkeit, dass der Schlüssel öfters benutzt wird.

Die perfekte Sicherheit entsteht bei einer echten Zufallsbitfolge (zum Beispiel durch XOR Verbindungen). Diese Zufallsbitfolge enthält die Werte von 0 und 1, wo die Wahrscheinlichkeiten von ½ vorkommen. Die Bedingung soll natürlich sein, dass keine Ableitung vom Anfang der Bitfolge bis zum Ende möglich ist. Echte Zufallszahlen sind im PC nicht realisierbar, nur die Folgen von Pseudozufallszahlen. Das folgende Funktionsschema stellt eine einfache Stromchiffrierung dar.

Folge von Zufallsbites:(Stromchiffrierung)

001011011010111

2 Klartexte: → XOR-VERBINDG.--> 111001100110010

110010111100101 (Chiffretext)

Effiziente Zufallszahlen spielen in der Kryptographie und in der Informatik (randomisierte Algorithmen oder stochastischer Simulation) eine große Rolle. Die Definition für „zufällig“ lautet: „Die Bits einer Folge, die paarweiße statistisch unabhängig sind, das Wissen der ersten n Bits einer Folge liefert keine Informationen über das n+1 te Bit“.

Die perfekte zufällige Zahle sollte am besten keine Möglichkeit geben, aus der Kenntnis eines Anfangsstückes den Rest der Folge oder Teile davon vorherzusagen. Aus dem Grund, dass das Thema „zufällig“ in der Philosophie schon unterschiedlich stark debattiert wurde und nie wirklich geklärt wurde, ob es „echte“ zufällige Zahlen in unserem Universum überhaupt gibt, da man für jedes Ereignis eine Statistik führen kann, führte man sogenannte Pseudozufallsgeneratoren (PRNG) ein. Diese enthalten einen Algorithmus, der nach Eingabe einer oder mehrer Initialisierungszahlen deterministisch eine Zahlenfolge erzeugt. Er wird aber nie echte Zufallszahlen erzeugen können, er versucht dem nur sehr nahe zu kommen. Denn wenn der Angreifer den Algorithmus kennt, dann weiß er auch über Teile der Folge bescheid. Gute Zufallsgeneratoren für kryptographische Anwendungen dürfen Pseudozufallsgeneratoren nur als Alternative sehen. Eine meist bessere Alternative ist die Verwendung physikalischer Zufallsereignisse aus der Natur. Das thermische Rauschen eines Widerstandes im Prozessor oder der radioaktive Zerfall von Uran beruhen heute noch auf den Mythos des Zufalls. Man kann auch jeglichen anderen physikalischen Prozess verwenden, aber nur wenn dieser zufällig passiert und keine Symmetrie aufweist.

Bis heute wurde es nicht bewiesen, dass der Mensch zukünftige physikalische Prozesse vorhersagen könne. Wäre dies möglich, dann müsste man den Begriff „zufällig“ wieder neu definieren.

Fragt man sich zum Beispiel, ob die Dezimalstellen von der Zahl PI zufällig sind, dann muss man diese Frage mit NEIN beantworten. Ein Computerprogramm kann beliebig viele dieser Dezimalstellen berechnen.

Um trotzdem noch ein Beispiel für ein Pseudozufallsgenerator zu zeigen, den man auch in der Kryptographie ohne große Besorgnis anwenden kann, erläutern die nächsten Zeilen die Funktionsweise eines BBS-Generators. Er ist ein kryptographisch sicherer Kombinationsgenerator. Das Ziel ist es, die aufwendigen Zufallstests zu bestehen, das bedeutet die Zahlen sollten so berechnet werden, dass man daraus keine Statistik erschließen kann. Das Funktionsprinzip des BBS-Generators besteht aus den Kombinationen der Kongruenzgeneratoren. Lineare Kongruenzgeneratoren berechnet man zum Beispiel mit

$$X_n = (aX_{n-1} + b) \bmod m$$

Trotzdem ist diese Formel nichts weiter als eine Simulation, die genauso eine Statistik besitzt.

PROGRAMM, DAS PSEUDOZUFALLSZAHLEN BERECHNET!

```
static long s1 = 1;

static long s2 = 1;

#define MODMULT(a,b,c,m,s) q = s/a; s= b*(s-a*q) - c*q; if (s<0) s+=m;

/*liefert eine reelle Pseudozufallszahl im Intervall (0,1). Die Funkt kombiniert lineare Kongruenzgeneratore mit
Perioden 2^31  - 85 und 2^31  -249 Ihre Periode entspricht dem Produkt dieser beiden Primzahlen */

double combinedLCG(Void) {

  long q;

  long z;

   MODMULT(53668,40014,12211,2147483563L,s1)

   MODMULT(52774,40692,3791,2147483399L,s2)

   z = s1 - s2;

   if ( z < 1)

       z+= 2147483562;

    return z * 4.656613e-10;

}

void initLCG(long InitS1, long InitS2)

{

 s1=InitS1

 s2=InitS2;

         }
```

Würde man den Algorithmus eines Pseudozufallsgenerators erklären, so könnte man dies so beschreiben. Man wählt sich 2 große Primzahlen p und q, die beide bei der Division durch 4 den Rest 3 ergeben (p = q = 3 mod 4). Danach berechnet man das Produkt aus beiden Primzahlen mit n = p*q und wählt sich eine Zufallszahl s, die relativ prim (ggT = 1) zu n ist.

Der Generator berechnet, beginnend mit i = 1 wiederholend:

$x_i = (x_{i-1}^2 \bmod n)$

$b_i = x_i \bmod 2$

Zusätzlich ist noch anzumerken, das die XOR Operation für ein exklusives ODER steht, die auf Bits arbeitet:

0 XOR 0 = 0

1 XOR 0 = 1

0 XOR 1 = 1

1 XOR 1 = 0

Die polyalphabetischen und homophonen Chiffrierungen wurden am Anfang in einfache und **symmetrische Verschlüsselungen** integriert. Man bezeichnet sie auch als die einfache Art und Weise, zu verschlüsseln. Symmetrisch bedeutet es aus dem Grund, da zum Ver- und Entschlüsseln immer dieselbe Funktion bzw. derselbe Schlüssel benutzt wird. Es gibt immer einen Klartext M (message), einen Geheimtext C (ciphertext), eine Verschlüsselungsfunktion E (encrypt) und eine Entschlüsselungsfunktion D (decrypt). Der Vorteil an der Symmetrie E = D ist, dass große Menge an Daten in kurzer Zeit ver- und entschlüsselt werden können. Beide Partner müssen sich jedoch vorher auf dasselbe Verfahren und denselben Schlüssel einigen.

Außer den klassischen Chiffreverfahren existiert noch ein sehr populäres und neueres Verfahren. Ein Spezialfall des asymmetrischen Verfahren - das sogenannte Public-Key-Verfahren. Es stellt eine sehr sichere Kommunikation im Internet dar, die Mitte der 70er Jahre erfunden wurde.

Aufgrund der schnell aufkommenden und gewaltigen Mengen von Daten, die ständig über große Distanzen und weltweitverzweigte Datennetze ausgetauscht werden müssen, kristallisiert sich ein neuer Bedarf heraus: Mit seinen Partnern schnelle, sichere und vertrauliche Informationen auszutauschen, die man vorher nicht kannte und wo es gleichzeitig unmöglich war, mit ihnen auf gesichertem Wege geheime Schlüssel auszutauschen. Ein gutes Beispiel gibt es in der Wirtschaft. Wenn man viel mit nationalen Kunden in Berührung kommt und Verträge abschließt, gilt immer das Problem der Anerkennung der Unterschrift.

Ein öffentlicher Schlüssel sowie ein geheimer Schlüssel werden mit Hilfe eines asymmetrischen Algorithmus erzeugt. Wenn der Empfänger Bob eine Nachricht empfangen möchte, dann erzeugt er einen öffentlichen Schlüssel und schickt diesen zu dem entsprechenden Partner – Alice. Bob generiert weiterhin, aus der Basis des öffentlichen Schlüssels, einen geheimen Schlüssel für sich und bewahrt ihn für sich auf. Der öffentliche Schlüssel wird verwendet ausschließlich zum Verschlüsseln und der geheime ausschließlich zum Entschlüsseln. Somit kann außer Alice jeder, der den öffentlichen Schlüssel von Bob besitzt, dem Empfänger (Bob) verschlüsselte Nachrichten zu kommen lassen. Doch nur Bob kann diese geheimen Nachrichten entschlüsseln, weil nur er den geheimen Schlüssel besitzt.

Dieses Schemata kann man auch mit dem Prinzip der Wohnungstür vergleichen: Jeder kann die Tür schließen, doch das Öffnen von Außen ist dagegen nur für Besitzer des Schlüssels möglich.

Eine noch ganz frische, neue und noch nicht ganz ausgereifte Art der Kryptographie ist die **Quantenkryptographie**! Das hat auch damit zu tun, da sie die Ungewissheit der Quantenwelt ausnutzt. Der Quantenkanal ist durch die Gesetze der Physik abgesichert. Die Quantenmechanik besagt in groben Zügen: Teilchen existieren an mehreren Orten. Es besteht immer eine gewisse Wahrscheinlichkeit, wo sich ein Teilchen gerade befindet. Der Ort und die Geschwindigkeit sind durch die Formel p = m * v nicht gleichzeitig messbar.

Dadurch existiert eine Unschärfe, nach der Heisenberg' schen Unschärferelation $x * p_x = h$, zur Generierung geheimer Schlüssel.

Im nächsten Abschnitt werden die verschiedenen Arten von Angriffen erklärt, die auf alle Verschlüsselungsverfahren anwendbar sind. Beim *Ciphertext-Only-Angriff* verfügt der Kryptoanalytiker nur über eine bestimmte Menge an Chiffretext. Der *Known-Plaintext-Angriff* benutzt Chiffretext mit Klartext, um eine gewisse Struktur zu erklären und somit den Schlüssel zu „erraten". Bei der Verwendung des *Chosen-Plaintext-Angriffs* kann dem Kryptoanalytiker ein beliebiger Klartext vorgegeben sein und hat dabei die Möglichkeit zu diesem Klartext den zugehörigen Chiffretext zu bekommen. Ein gutes Beispiel wäre das Public-Key-System. Der Angreifer kann mit dem öffentlichen Schlüssel jeden beliebigen Klartext verschlüsseln. Bei dem *Chosen-Ciphertext-Angriff* kann dem Kryptoanalytiker beliebiger Chiffretext vorgeben sein und er hat dabei nur eine Möglichkeit, an den zugehörigen Klartext zu gelangen. Nutzt man jedoch das Mittel der Gewalt, um an den Schlüssel zu gelangen, dann bedroht man diejenige Person. Doch dies wäre der unmathematischste und uneleganteste Versuch des Knackens von kryptographischen Verfahren.
Eli Biham und Adi Shamir führten 1990 die *differentielle Kryptanalyse* ein. Dabei handelt es sich um eine neue Methode der Kryptanalyse, die bis dahin nicht öffentlich bekannt war.
Bei der differentiellen Kryptanalyse betrachtet man gezielt gewisse Paare von Chiffretexten, nämlich solche, deren zugehörige Klartexte bestimmte Differenzen aufweisen. Dann untersucht man die Entwicklung dieser Differenzen, während die beiden Klartexte die Verschlüsselungsrunden durchlaufen und mit dem gleichen Schlüssel chiffriert werden.
Man kann einfach Klartextpaare mit fester Differenz wählen. Die Auswahl der Paare kann zufällig erfolgen, solange die Differenz nur bestimmte Bedingungen erfüllt. Der Kryptanalytiker muss nicht einmal die Werte kennen. Mit Hilfe der Differenzen der entstandenen Chiffretexte weist man verschiedenen Schlüsseln unterschiedliche Wahrscheinlichkeiten zu. Analysiert man eine genügend hohe Zahl von Chiffretextpaaren, so kristallisiert sich schließlich ein Schlüssel als der wahrscheinlichste heraus. Dies ist der korrekte Schlüssel.
Allgemein kann man beweisen, daß ein Algorithmus resistent gegen differentielle Kryptanalyse ist, wenn man zeigen kann, daß zur Durchführung eines solchen Angriffs mehr Klartextblöcke nötig sind als insgesamt überhaupt möglich. Außerdem ist dieser Angriff zum größten Teil theoretischer Natur. Die Anforderungen bezüglich Zeit und Speicherplatz sind so enorm, daß sie fast nie erfüllt werden können.

Der am einfachsten und am logischsten verwendete Angriff ist der weitverbreitete *BruteForce-Angriff*. Bei ihm werden alle möglichen Schlüssel ausprobiert, meist mit Hilfe

eines Computers, der solange probiert bis der Klartext Sinn ergibt. Ein sehr großer Aufwand ist damit verbunden. Bei sehr langen Schlüsseln müssen alle Schlüssel versucht werden den Chiffretext zu entschlüsseln. Ergibt der Klartext keinen Sinn, so muss der nächste Schlüssel generiert und ausprobiert werden. Desto länger also der Schlüssel, desto sicherer und komplizierter ist auch das Kryptosystem. Der Angriff benötigt keine große Gedankenarbeit, sondern gute Rechenleistung. Es ist zwar eine unelegante, aber eine gefährliche Lösung, da die Rechenleistung billig und leistungsfähiger geworden ist. Höhere analytische Kenntnisse sind nicht nötig.

Heute bezeichnet man eine Schlüssellänge von 1024 Bit als sicher. Durch die in der Welt ständig zunehmende Rechenleistung, muss sich auch dieser Schlüsselwert ändern. Ein sicherer Algorithmus muss sich dadurch kennzeichnen, dass der nötige Geldaufwand zum Knacken größer sein sollte, als der Wert der verschlüsselten Daten. Weiterhin muss die erforderliche Zeit des Knackens größer sein, als wie die Daten geheim bleiben müssen und das chiffrierte Datenvolumen muss wesentlich kleiner sein als die zum Knacken erforderliche Datenmenge. Uneingeschränkte Sicherheit liegt erst dann vor, wenn auch dann der Klartext nicht ermittelt werden kann, wenn der Chiffretext in beliebigen Umfang vorhanden ist.

2.2 Algorithmen

2.2.1 Gängige Verschlüsselungsverfahren – Standards – Kryptographie

Der derzeit am Verbreitesten und wichtigsten Vertreter der symmetrischen Blockchiffren ist *DES*, der Nachfolger von LUCIFER. Vom US-amerikanischen Handelsministerium ausgerufen, entwickelte IBM 1977 ein entsprechendes Verschlüsselungsverfahren, den *Data Encryption Standard*. Zu dieser Zeit gab es zwei Gründe für den Erfolg von DES: 1. Die differentielle Kryptoanalyse war noch nicht allgemein bekannt und 2. war die Rechenleistung damaliger Rechner vergleichsweise gering. DES ist seit 1977 als Standard für nicht geheime Nachrichten entworfen worden, und es wurde und wird heute noch von Banken eingesetzt.

Geschichte:

vor 1970: wurde Kryptographie im Wesentlichen zur militärischen Kommunikation genutzt. Durch das Aufkommen der elektronischen Datenverarbeitung entsteht Bedarf zum Verschlüsseln von Daten und zur Authentifikation.

Mai 1973: das NIST (National Institute of Standards and Technology, USA) startet eine öffentliche Ausschreibung für einen standardisierten kryptographischen Algorithmus.

August 1974: Mangels qualifizierter Einreichungen veröffentlicht das NIST eine zweite Ausschreibung. Schließlich wird ein Algorithmus eingereicht.

17.3.1975: Im amerikanischen Bundesanzeiger werden Einzelheiten eines von IBM entwickelten und von der NSA (National Security Agency) geprüften Algorithmus veröffentlicht.

1.8.1975: Im amerikanischen Bundesanzeiger wird die Öffentlichkeit zu Stellungnahmen aufgefordert, die dann im Folgenden die undurchschaubare Rolle der NSA kritisierten.

15.6.1977: Der Data-Encryption-Standard wird veröffentlicht. Unter anderem schreibt der Standard eine Zertifizierung von DES-Implementierungen durch das NIST vor. Außerdem muss DES alle fünf Jahre überprüft werden.

1981: ANSI (American National Standards Institute) erkennt DES als Standard an.

1982-1986: Basierend auf DES werden Standards für die Verschlüsselung von PINs, für die verschiedensten Finanztransaktionen, zur Schlüsselverteilung sowie für Telekommunikation und FAX definiert.

1983: DES wird geprüft und ohne Probleme neu zertifiziert.

1987: Nach langen Debatten wird DES neu zertifiziert.

1993: DES wird erneut zertifiziert (mit der Bemerkung, dass es Ende der 90er Jahre überholt sein würde).

1994: Mit einem Rechenaufwand von 50 Tagen auf 12 HP-9735-Workstations wurde DES erstmals geknackt.

1997: NIST kündigt die Entwicklung des Advanced-Encryption-Standard (AES) an.

17.7.1998: Die Electronic Frontier Foundation (EFF) knackt DES mit einem Spezialchip in weniger als drei Tagen.

19.4.1999: 100 000 PCs von Distributed.net und der EFF Spezialrechner knacken DES in 22 Stunden, 15 Minuten.

Der Algorithmus benutzt 64 Bit Blöcke mit einer 128 Bit Schlüssellänge. Die Gesamtzahl aller Chiffren beträgt bei 64 Bit Blöcken 2^{64} ! Auf den Blöcken wird abwechselnd Substitution und Permutation ausgeführt. Der Prozess wird mit unterschiedlichen Teilen des Schlüssels mehrmals wiederholt. Dieses Verfahren war für eine sehr lange Zeit sehr sicher und bietet heute noch einen guten Schutz. Trotzdem wurde DES in den letzten Jahren mehrfach geknackt. Aus dem heutigen Standard kann man DES beim Austausch von sehr geheimen Informationen als unsicher bezeichnen. Eine sicherer, effizienterer und verbesserter Algorithmus wurde basierend aus DES entwickelt: TRIPLE-DES. Es wendet DES dreimal hintereinander mit 2 verschiedenen Schlüsseln an. Die Schlüsselraumgröße beträgt 2^{112}. Für das Verschicken von e-Mails reicht die Sicherheit von TRIPLE-DES vollkommen aus.

Crypt(3) ist eine DES – Variante, die auf UNIX-Systemen ihren Einsatz findet. Die eingegebenen Passwörter werden mit Hilfe einer Einwegfunktion in einer Passwortdatei gespeichert.

Ein weiterer Standard in der Kryptographie und der offizielle Nachfolger von DES ist der AES - Advanced-Encryption-Standard - Algorithmus. Er wurde von Rijndael von Joan Daemen und Vincent Rijmen (Belgien) entwickelt. Die Blockchiffre wurde von Rijndael folgendermaßen erklärt. Die iterierten Blockchiffre, die aus der Blocklänge b und Schlüssellänge k bestehen, können unabhängig voneinander auf den Wert 128, 192 oder 256 gesetzt werden. Die Rundenzahl r variiert dabei. Das Zwischenergebnis wird als S_i bezeichnet. Der Ablauf der Verschlüsselung funktioniert so: Die Schlüsselexpansion erzeugt r+1 Rundenschlüssel K_0...,K_r der Länge b aus den Schlüsseln der Länge k. Die Rundenschlüssel haben dabei die gleiche Länge wie der jeweilige Zustand bzw. Zwischenergebnis. Vor der ersten und letzten Runde werden die Schlüssel und das Zwischenergebnis XOR verknüpft. Das Ergebnis dient als Eingabe für die nächste Runde (als Chiffre). Als nächstes werden noch 3 mathematisch-komplexe Funktion (ByteSub, ShiftRow, MixColumn) der zyklischen Verschiebung abgearbeitet. Jede einzelne Runde in AES ist invertierbar. Man kann den ganzen Algorithmus umkehren, indem alle Transformationen durch ihre Inverse ersetzt und in ihrer Reihenfolge umgekehrt werden.

2.1.1997: Ankündigung der AES Entwicklungsanstrengungen durch das NIST.

12.9.1997: Formaler "call for algorithms" für AES. AES sollte öffentlich, lizenzfrei und weltweit verfügbar sein. Technisch sollte AES Blöcke mit mindestens 128 Bit und Schlüssellängen von 128, 192 und 256 Bit unterstützen.

20.8.1998: Das NIST gibt auf der ersten AES Candidate Conference (AES1) die 15 AES-Kandidaten bekannt. NIST bittet um Kommentare zu den Algorithmen.

15.4.1999: Die Kandidaten für das Finale werden bekannt gegeben. Es sind MARS, RC6, Rijndael, Serpent und Twofish. Wieder bittet NIST öffentlich um Kommentare zu den Algorithmen.

13.-14.4.2000: Dritte AES Candidate Conference (AES3) mit öffentlichen Diskussionen der fünf Kandidaten-Algorithmen.

15.5.2000: Abgabeschluss für öffentliche Kommentare.

2.10.2000: Bekanntgabe des Gewinners. Der Algorithmus heißt Rijndael und wurde von den beiden belgischen Kryptologen J. Daemen und V. Rijmen [DR99] entwickelt.

bis Feb. 2001: Öffentliche Kommentare zu AES sind erwünscht.

April-Juni 2001: AES wird offiziell zum "federal information processing standard" (FIPS).

Tabelle 4.4: Geschichte von AES in Stichworten

Zusammenfassend kann man sagen, dass AES sehr viel schneller als DES ist. Die Geschwindigkeit liegt weit über ein Gigabit pro Sekunde. Der Algorithmus lässt sich sogar in 8 Bit Prozessoren Chipkarten implementieren.

AES weißt eine große Sicherheit von Resistenz gegen differentielle Kryptoanalyse und lineare Kryptoanalyse auf. Ihre Funktion ist den Bereichen der Telekommunikation und Sattelitenübertragungen von digitalen Daten brauchbar. Als Einweg-Hash-Funktion kann man es bei Stromchiffren, Pseudozufallsgeneratoren und Erzeugungen von MAC - Adressen verwenden.

Die meisten symmetrischen Verfahren benutzen das Blockchiffreverfahren und nicht die Stromchiffreverfahren. Der Betriebsmodi von Blockchiffren funktioniert folgendermaßen. Die Blöcke werden einzeln nacheinander und mit den gleichen Schlüsseln verschlüsselt. Die Blockstruktur die man im Chiffretext finden kann, ist auch im Klartext vorzufinden. Für einen festen Schlüssel ließe sich eine Tabelle aller Klartext-Chiffre-Paare anlegen. Dies bezeichnet man als den ECB (electronik codebook) – Modus. Die Lösung für dieses Problem stellt der CBC (cipher block chaining) Modus dar. Vor der Verschlüsselung werden die Chiffretexte des Vorgängerblocks, ab dem zweiten Block, mit den aktuellen Klartextblock XOR verknüpft.

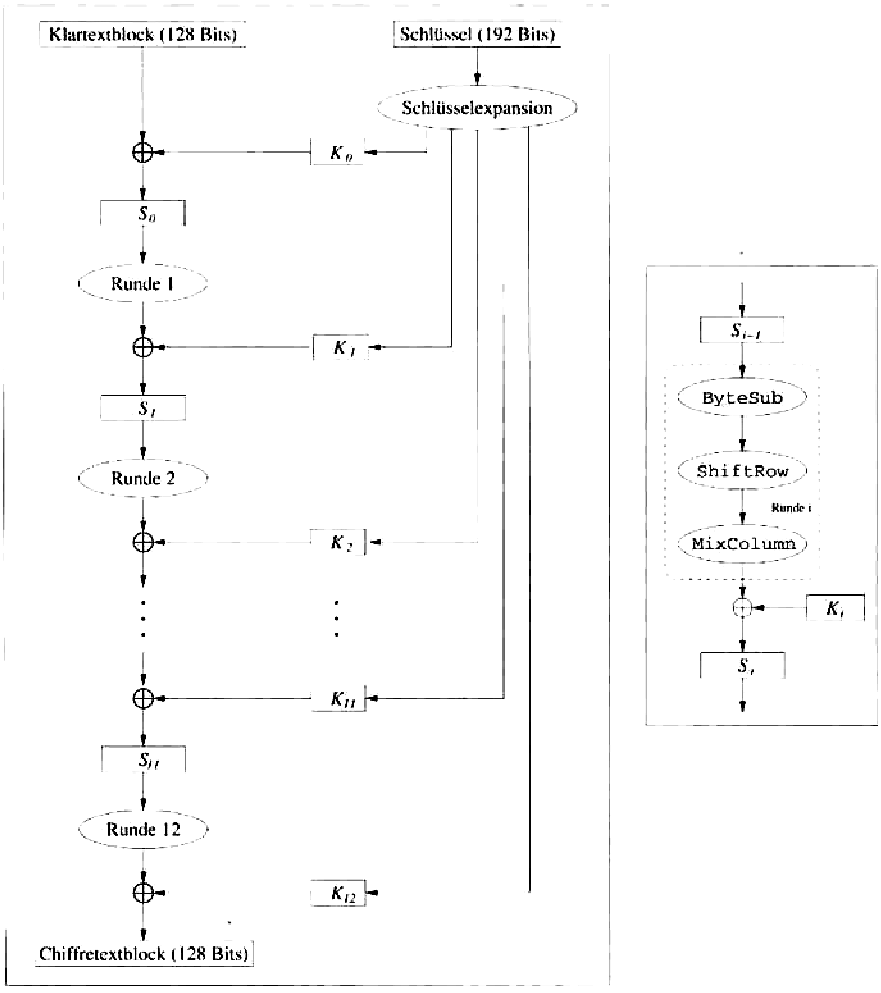


Abbildung 4.5: Schematischer Ablauf der Verschlüsselung aller Runden von Rijndael (links) und einer einzelnen Runde (rechts) bei Blockgröße 128 Bit und Schlüssellänge 192 Bit

Ein anderer sehr sicherer Algorithmus ist IDEA (international data encryption algorithm), der in der Technischen Hochschule in Zürich von James Massey und Xuejia im Jahr 1990 entwickelt wurde. IDEA ist die Form der modernen Art der symmetrischen Verschlüsselung. Sein wichtigstes Einsatzgebiet war es, dass es in den erfolgreichen E-Mail-Verschlüsselungsstandard integriert wurde, nämlich PGP. Das Verfahren beruht auf den Prinzipien der Konfusion und Diffusion, dass von einem der Pioniere der Informationstheorie, Shannon, beschrieben wurde. Es werden 3 unterschiedliche, nicht „kompatible“ Abbildungen aus drei verschiedenen Gruppen, die auf algebraische Strukturen beruhen, miteinander verknüpft. Der Schlüsselraum ist wesentlich größer als bei DES und deswegen ist IDEA sehr sicher. Bis heute wurde noch keine Angriffsart entdeckt, die Erfolg verspricht.

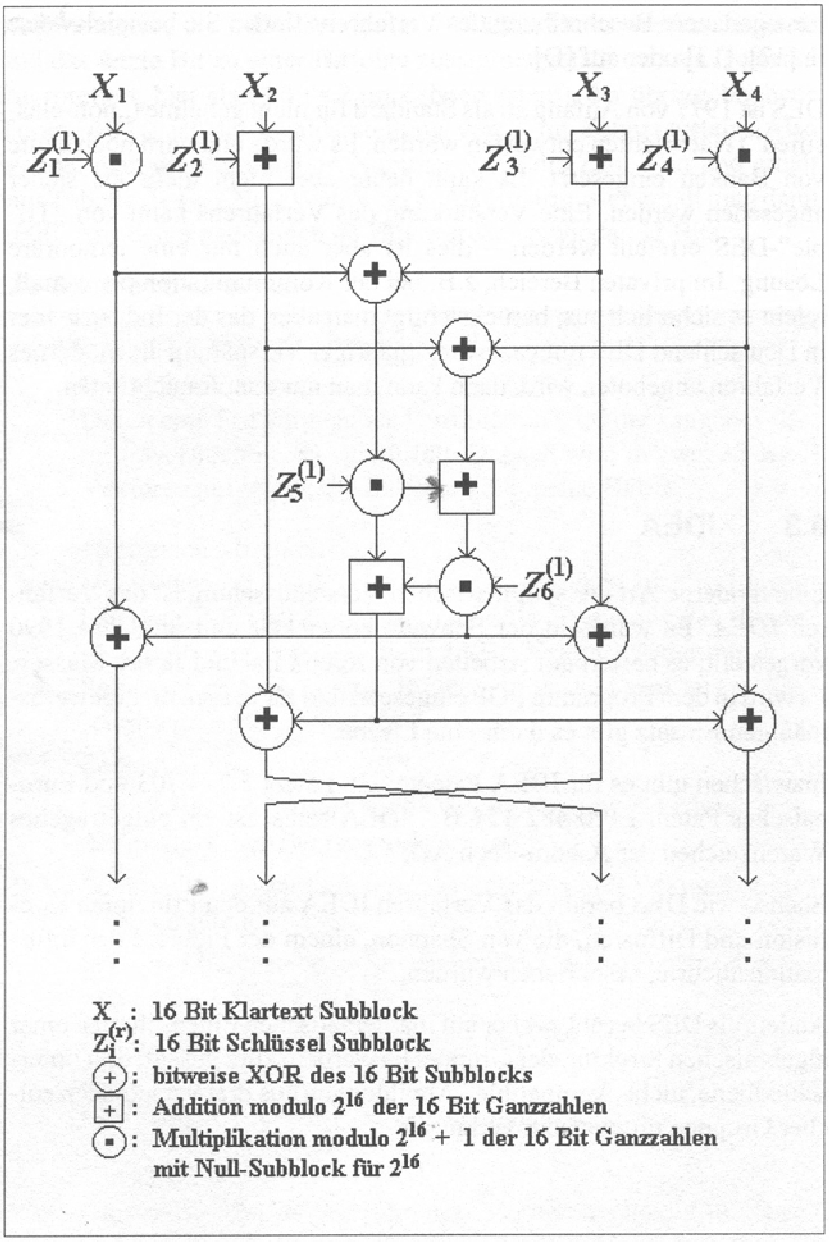


Abb. 6.3: IDEA, 1 Runde.

Zwei weitere Blockchiffren sind Blowfish und TwoFish. BlowFish basiert auf der 64-Bit Blockchiffrierung mit variabler Schlüssellänge. Die Schlüsselexpansion, die alle Schlüssel bis zu 448 Bit in verschiedene Teilschlüssel umwandelt, und die Datenverschlüsselung, bei der dieFunktion 16mal abgearbeitet wird, sind die 2 Verläufe bei Blowfish.

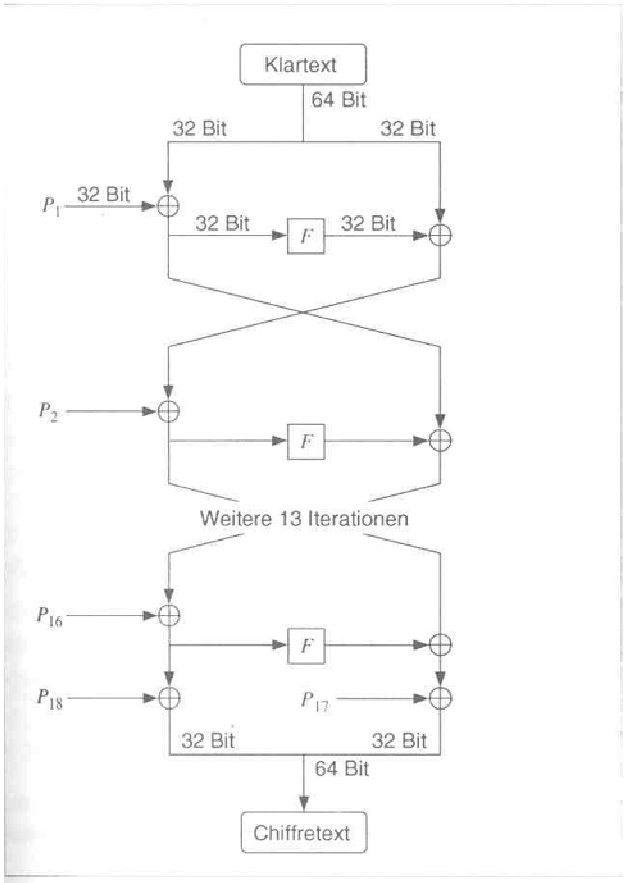


Abb. 14.2: Blowfish

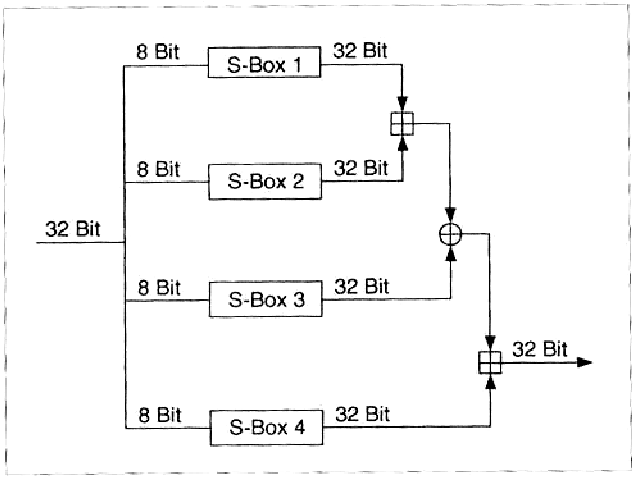


Abb. 14.3: Die Funktion F

Ein weitverbreiteter und sicherer Algorithmus ist der RSA- Algorithmus. Dieser wurde 1978 erstmals von Adi Shamir und Leonard Adlemann vorgeführt. Seine wesentliche Aufgabe ist es, die Sicherheit von digitalen Signaturen anzuwenden. RSA ist ein Public-Key-Verfahren.

2.2.2 Funktionsweise

In der nächsten Übersicht wird DES in seiner Funktionsweiße erklärt.

Der Klartext wird durch die Eingangspermutation gemischt, durchläuft dann 16 Runden und am Ende wird die Chiffre durch die Schlusspermutation vollendet. Die Schlusspermutation ist invers zur Anfangspermutation, weil in den Permutationen schlüssel-unabhängige Operationen angewendet werden, die zur Sicherheit beitragen. Für den Schlüssel K werden 16 Teilschlüssel generiert, für jede Runde einer, mit einer Schlüssellänge von 56 Bit. Eine Runde bei DES: In der Eingangspermutation wird der 64 Bit Block in zwei 32 Bit Blöcke geteilt. In jeder der 16 Runden wird die rechte Hälfte unverändert als linke Hälfte der nächsten Runde übernommen. $\rightarrow L_i = R_{i-1}$

Auf den Teilschlüssel K_i und die rechte Hälfte R_{i-1} wird die Funktion f angewendet. Das Ergebnis wird mit der linken Hälfte L_{i-1} XOR verknüpft und als rechte Hälfte der nächsten Runde übernommen. Dieser Prozess wird nun 16mal wiederholt. Die Berechnungen einer Runde lauten daher folgendermaßen:

$L_i = R_{i-1}$

$R_i = L_{i-1}$ XOR f (R_{i-1}, K_i)

Innerhalb der Funktion f werden die rechten 32 Bit R_{i-1} durch Expansionspermutation auf 48 Bit aufgeweitet und dann mit ebenfalls 48 Bit langen Teilschlüsseln K_i XOR verknüpft. Ein sehr wichtiger Sicherheitsteil im DES-Algorithmus ist die S-Box Transformation, bei der alle 48 Bit in acht Sechserblöcke aufgeteilt werden. Je ein Block steht als Eingabe für eine S-Box. Das jeweils erste und letzte Bit eines Blocks wird als Zahl interpretiert und bestimmt Zeile und Spalte der zugehörigen S-Box. Alle S-Boxen liefern zusammen ein 32 Bit-Wort, dass durch P-Box Permutation verschlüsselt wird und als Ergebnis von f mit L_{i-1} XOR verknüpft wird. Die 16 Teilschlüssel, mit der ursprünglich 64 Bit langen Schlüssellänge, werden durch Schlüsselpermutation auf 56 Bit verkürzt und in zwei gleiche Hälften aufgeteilt: X_0 und Y_0. Beide Hälften X_{i-1} und Y_{i-1} werden in Runde i abhängig vom Rundenindex zyklisch um ein oder zwei Bits nach links verschoben und dienen in der nächsten Runde als neue Hälfte X_i und Y_1

Durch die Kompressionspermutation werden 48 Bits der 56 Bits aus X_i und Y_i ausgewählt und als Teilschlüssel K_i an die Funktion f übergeben. Der gleiche Algorithmus funktioniert auch beim Entschlüsseln der Chiffre. Die Teilschlüssel müssen nur in umgekehrter Reihenfolge angewendet werden, d.h. eine Schlüsselverschiebung in eine andere Richtung: rechts. Die Sicherheit von DES ist durch den Lawineneffekt in den S-Boxen zu erklären. Aus dem Grund, das DES auf der Konstruktion der S-Boxen basiert, bewirkt eine minimale Änderung des Klartextes eine maximale Änderung der Chiffre. Der schnellste Angriff gegen DES gelang im Jahr 1999. Dabei wurde ein Brute-Force Angriff auf alle Schlüsselmöglichkeiten durchgegangen. Ein Super-Rechner berechnete und testete $9{,}22*10^{10}$ DES - Schlüssel pro Sekunde. Der Rechner benötigte ca. 4,52 Tage zum Knacken des Algorithmus.

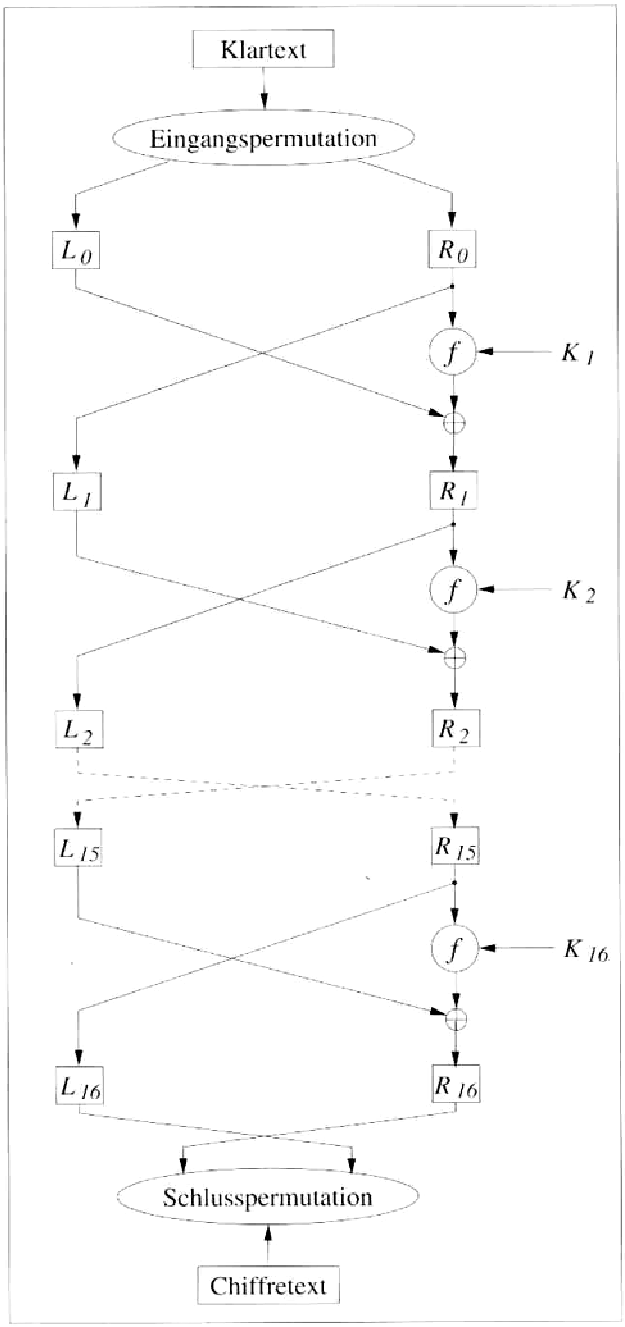


Abbildung 4.1: Die 16 Runden von DES

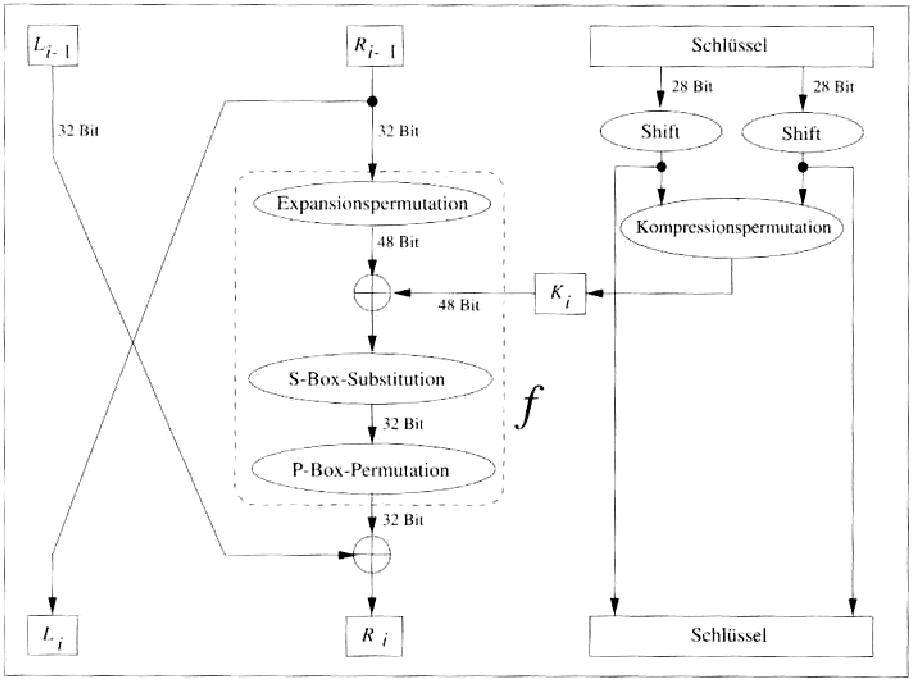


Abbildung 4.2: Eine Runde von DES

Eingangspermutation:

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Schlusspermutation:

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Kompressionspermutation:

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Expansionspermutation:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P-Box-Permutation:

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Schlüsselpermutationen:

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Schlüsselverschiebungen:

Runde	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Anzahl	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

S-Box 1:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-Box 2:

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S-Box 3:

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S-Box 4:

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S-Box 5:

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S-Box 6:

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S-Box 7:

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S-Box 8:

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tabelle 4.3: Die S-Boxen von DES

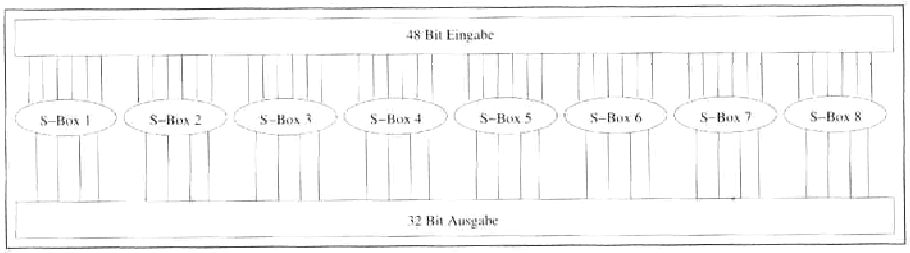


Abbildung 4.3: Die S-Box-Transformation

Ein wichtigster Teil des **RSA- Algorithmus** ist die Schlüsselerzeugung. Bei dieser werden 2 sehr große Primzahlen (zwischen 384 und 512 bit) ‚p' und ‚q' gewählt. Danach wird das Produkt aus ihnen berechnet: *n = p * q.* Als drittes wähle man eine kleine ungerade natürliche Zahl *e,* die zu

ϒ (n) = (p-1)*(q-1) relativ prim ist, d.h. das der größte gemeinsamer Teiler gleich 1 ist. Im vierten Schritt wird die Gleichung e * d = 1 mod ϒ(n) aufgestellt und (mithilfe des euklidischen Algorithmus) nach d um gestellt und berechnet: d ergibt sich aus : e^{-1} mod ((p-1)(q-1)). Der öffentliche Schlüssel besteht aus e und n : P = (e,n). Der geheime Schlüssel setzt sich aus d und n zusammen: S = (d,n).

Die Nachricht M wird mit folgender Formel zu einem Chiffretext C verschlüsselt: $E(M) = M^e$ mod n und mit $D(C) = C^d$ mod n entschlüsselt. Ein kleines Beispiel demonstriert die Funktionsweiße von RSA. Wir setzen p = 61 und q gleich 97. Das Produkt n aus beiden Zahlen beträgt 5917. Aus der Formel ϒ (n)= (60)*(96) ergibt sich 5760. Wir wählen uns die Zahl e, die teilerfremd zu 5760 sein muss. e = 47. d= 47^{-1} mod 5760 = 1103. Der öffentliche P wird als P = (47,1103) bekannt gegeben.

Die Nachricht M = 348613407195771184 wird in Blöcke zerteilt. Die Blocklänge beträgt 3.

M = 348 613 407 195 771 184

Als nächstes wird der erste Block verschlüsselt: 348^{47} mod 5917 = 4479

Das Resultat, der verschlüsselte Text heißt C = 4479 1333 3931 2523 3725 1038

Am Ende verschlüsseln wir den ersten Block: 4479^{1103} mod 5917 = 348
Das Problem bei RSA besteht darin, das die modulare Exponentiation von RSA sehr aufwendig sein kann. Wenn die Nachricht M und die Zahl e alle beide 1024 Bit lang wären, wäre M^e mod n sehr aufwendig zu berechnen.

Eine Vereinfachung fußt auf den zahlentheoretischen Grundlagen dieses Beispiels.

$$\mathbf{A^{19} = a^{((2\wedge 4)+2+1)} = a^{2*2*2*2} * a^2 * a = (((a^2)^2)^2)^2 * a^2 * a}$$

Nach jedem Quadrieren wird der Rest modulo n berechnet. Ein Beispielalgorithmus berechnet

a^b mod n !

MODULARER-EXPONENT(a,b,n)

d:=1

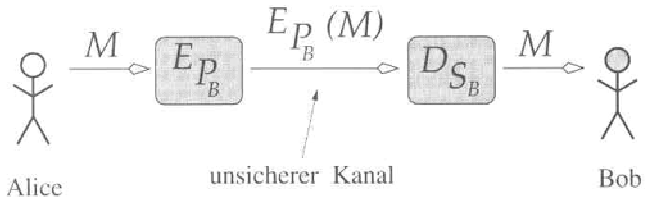
for i:= k downto 0 do

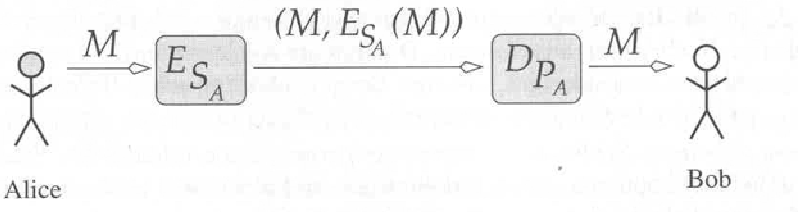
*d:= (d*d) mod n*

if b(i) = 1 then

*d := (d*a) mod n*
return d

Bei der Verschlüsselung benötigt man die sogenannte Public-Key-Infrastruktur. Sie richtet nach dem Schema: Erzeugung, Authentifizierung, Verteilung, Überprüfung öffentlicher Schlüssel, Speichern geheimer Schlüssel.





Die Authentizität wird mit Hilfe der Einweg-Hash-Funktion, die als Fingerabdruck dient, überprüft.

Der Schlüsseltausch beim Public-Key-Verfahren stellt ein weiteres Problem dar. Denn dabei benötigt man sichere Protokolle, die den Schlüsseltausch über unsichere Kanäle abwickeln. Das symmetrische Schlüsseltauschverfahren nutzt dabei eine dritte vertrauensvolle Person, bei der jeder Kommunikationspartner seinen eigenen geheimen Schlüssel vereinbart und seinen öffentlichen Schlüssel zertifizieren lässt, das sogenannte TRUST-Center. Die Authentizität von Schlüsseln spielt da eine wichtige Rolle, denn beide Kommunikationspartner müssen gleichzeitig ihre Authentizität prüfen. Alle beiden müssen sicher sein, das es auch wirklich genau der Partner ist, mit dem sie kommunizieren.

Ein Trust-Center funktioniert folgendermaßen. Alle Personen die das TRUST-Center nutzen, müssen ihr auch vertrauen, das sie die öffentlichen Schlüssel von Privatpersonen zertifiziert. Der Vorgang besteht darin, indem es die Authentizität der Person testet und die Signatur des Schlüssels P mit dem geheimen Schlüssel des Trust-Centers überprüft. Der öffentliche Schlüssel des Trust-Centers ist bekannt und somit ist auch eine Überprüfung des Zertifikats möglich. Der geheime Schlüssel des TRUST-Centers sichert dabei ab, das nur dies Zertifikate ausgeben kann.

Geheime Kommunikation:

1. Alice (Sender) besorgt sich Zertifikat bei TC

2. Bob (Sender) besorgt sich Zertifikat bei TC

3. Alice und Bob schicken sich gegenseitig ihr zertifizierten öffentlichen Schlüssel zu

4. Alice überprüft Zertifikat auf Bobs öffentlichen Schlüssel

5. Bob überprüft Zertifikat auf Alics öffentlichen Schlüssel

6. Alice und Bob können sich geheime und signierte Nachrichten zukommen lassen

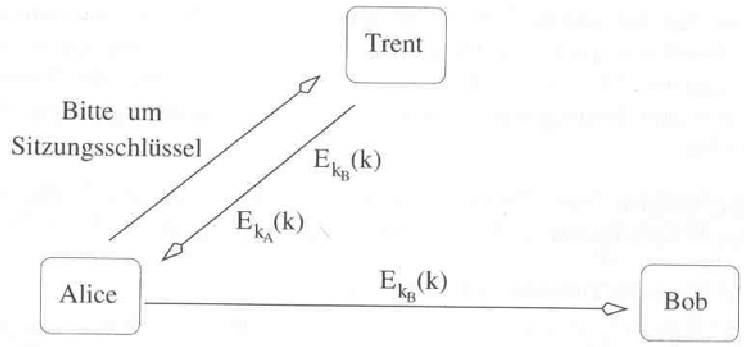


Abbildung 5.3: Schlüsseltausch via Trustcenter

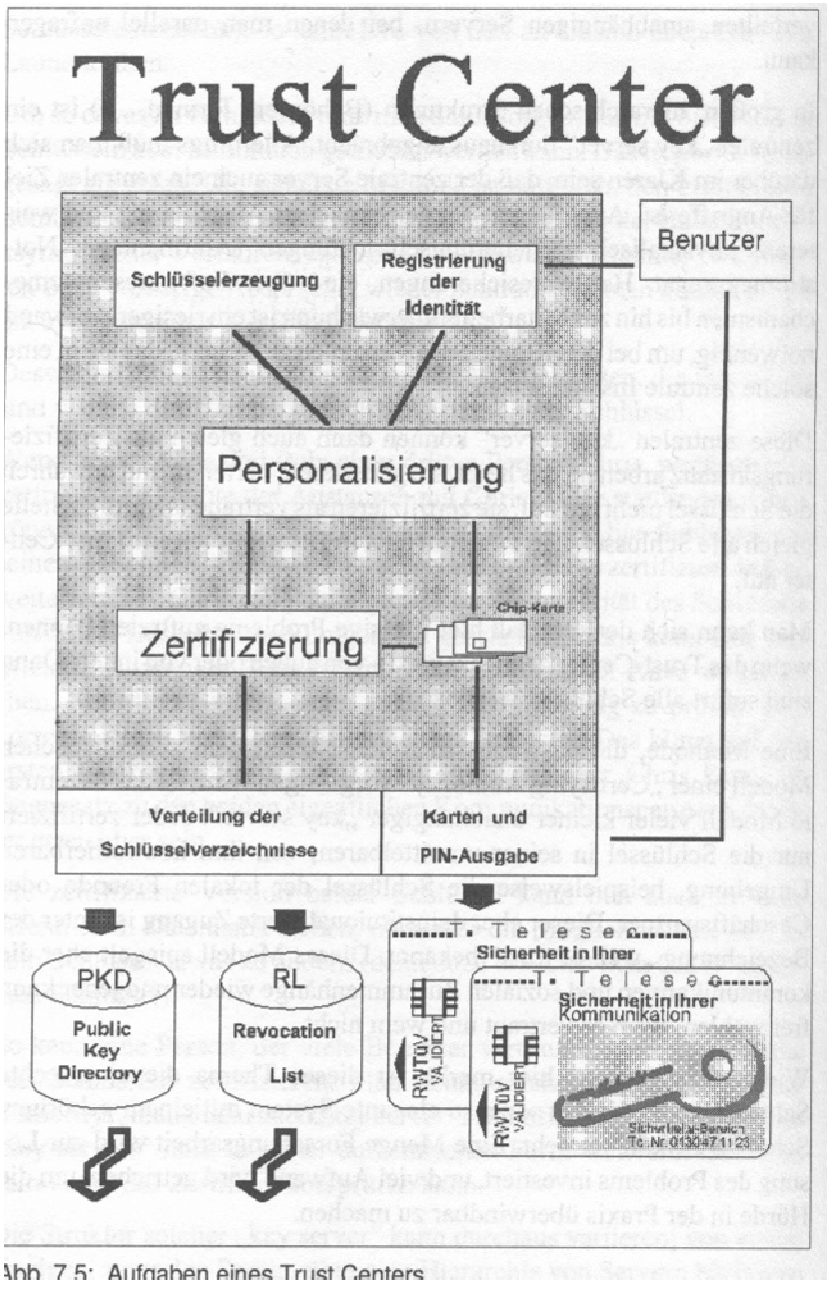


Abb. 7.5: Aufgaben eines Trust Centers

Doch warum brauchen wir digitale Signaturen und was sind sie im Allgemeinen?

Eine Signatur ist ein Merkmal, mit dem man eine Person oder Objekt erkennen kann. Bestes Beispiel aus unserem Alltag ist der menschliche Fingerabdruck. Er dient der eindeutigen Feststellung einer Person anhand genetischer Muster und biologischer Faktoren in der Haut seines Fingers. Eindeutigkeit ist eine wünschenswerte Eigenschaft der digitalen Signatur. Eine andere wichtige Eigenschaft ist eine leichte und unkomplizierte Übertragbarkeit auf andere Objekte. Bestes Beispiel ist unsere Unterschrift, die wir benutzen, um Dokumente zu unterzeichnen, die unsere Glaubwürdigkeit nicht in Frage stellt. Der Unterzeichner überträgt somit seine Verantwortung auf den Inhalt des Textes im Dokument. Von der digitalen Signatur sprechen wir dann, wenn diese in digitale Form vorliegt und z. Bsp. in der digitalen Welt –dem Internet – benutzt wird.

Digitale Signaturen funktionieren auf dem Prinzip der Einwegfunktionen und Einweg-Hash-Funktionen, die wir jetzt betrachten werden.

Digitale Signaturen sind gleichzustellen mit sicheren Fingerabdrücken, die durch Hash-Funktionen erzeugt werden können. Der Text dient dazu als Ausgangsbasis und der Hash-Wert wird aus einer speziellen Hashfunktion berechnet. Aus dem Hashwert wird ein verschlüsselter Geheimtext gefertigt. Der Text und der verschlüsselte Fingerabdruck (Hashwert) werden übertragen und der Empfänger berechnet aus dem empfangenen Text den Hashwert. Danach wird der verschlüsselte Hashwert nach verabredeten Verschlüsselungserfahren entschlüsselt. Beide Hashwerte werden nun verglichen und bei Übereinstimmung ist keine Manipulation vorgenommen wurden.

Einwegfunktionen sind Funktionen *f,* die sich leicht berechnen lassen, aber ihre Umkehrung f^{-1} jedoch nicht oder nur schwer zu berechnen ist. Das Differenzieren einer Funktion ist nicht schwer zu berechnen, aber die Umkehrung des Differenzieren, das Berechnen oder das Finden der Stammfunktion einer Funktion ist sehr schwer berechenbar. Aus diesem Grund ist das Differenzieren eine Einwegfunktion. Man kann dieses Prinzip auf das Zerbrechen eines Tellers übertragen. Das Zerschlagen eines Tellers ist relativ einfach. Doch die Scherben wieder zusammensetzen ist relativ schwierig. Es existieren aber auch Einweg-Hash-Funktionen mit einer Hintertür, genauso wie man eine zerschlagene Armbanduhr mit Hilfe eines Bauplans wieder kompliziert zusammensetzen kann. Mathematisch gesehen gibt es ein geheimes y, mit dem sich x einfach aus f(x) berechnen lässt.

Ein anderes Problem stellen die Polynome fünften Grades dar.

$x^5+x^4+x^3+x^2+x^1$

Hierzu existiert kein allgemeines Verfahren zur Bestimmung der Nullstellen und kein Verfahren für Zerlegung in ihre Linearfaktoren.

Bei der RSA-Verschlüsselung ist es einfach, M^e mod n zu berechnen, doch ihre Umkehrung (modulare Wurzel) ohne Kenntnis des geheimen Schlüssels d ist sehr schwierig zu berechnen.

Der Sinn der Einweg-Hash-Funktion besteht darin, beliebig lange Klartexte auf einen Hash - Wert fester Länge abzubilden. Dabei muss es schwierig sein, 2 Klartexte mit dem gleichen Hash – Wert zu finden.

(f : Einwegefunktion, h : Hash-Wert, n: Länge des Hash-Wertes, m : feste Länge)

Die Klartexteingabe M wird in k Teile M_i der Länge m aufgeteilt (M = M_1 , M_2 , M_k).

Der Hash-Wert h von dem Klartext lässt sich aus der Funktion $h_k = f(M_k)$, h_{k-1} berechnen.

Bekannte Hash-Verfahren sind MD4(message digest), wo der Hash- Wert 128 Bit lang ist, MD5, der noch sicherer als MD4 ist und auch in PGP verwendet wird, und SHA-1 (Secure-Hash-Algorithm), der von der NSA (National Security Agency) entwickelt wurde und einen 128bit langen Hash- Wert besitzt.

Digitale Signaturen werden meistens in Public-Key-Algorithmen wie RSA angewendet. Dabei wird nur der Hash-Wert signiert, um die Originalität einer Nachricht festzustellen.

Das Signieren funktioniert folgendermaßen. Bei der Verschlüsselung wird nur eine Signatur zu dem Hash-Wert hinzugefügt. Beim Prüfen wird der HashWert mit dem öffentlichen Schlüssel entschlüsselt. Stimmen die beiden Klartextnachrichten überein, dann ist die Unterschrift gültig.

Signieren:(M, E[S(A)] f(M))

Prüfen: D[P(A)] (E[S(A)] f(M))

Im Falle der blinden Signaturen ist das Signieren und Verschlüsseln vertauschbar (kommutativ).

Am Beispiel des RSA-Algorithmus mit dem Modul n ist ein spezielles Verfahren in folgendem Diagramm erläutert. Bob, der Unterzeichner, hat den öffentlichen Schlüssel e und den geheimen Schlüssel d.

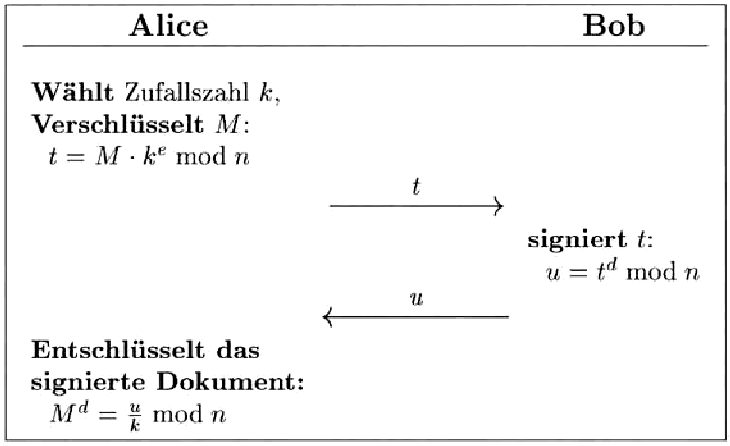


Abbildung 6.5: Ein Protokoll für blinde Signaturen

Was hier aussieht wie Zauberei, ist ganz einfach:

$$\frac{u}{k} \bmod n = \frac{t^d}{k} \bmod n = \frac{(M \cdot k^e)^d}{k} \bmod n = \frac{M^d \cdot k^{ed}}{k} \bmod n = M^d \bmod n.$$

Da M mit der Zufallszahl k^e multipliziert wird, hat Bob keine Möglichkeit, t beim Unterschreiben zu entschlüsseln, d. h. er signiert M blind. Blinde Signaturen wurden von D. Chaum [Cha85, Cha92] erfunden und in die Praxis umgesetzt. Sie werden hauptsächlich eingesetzt, um die Anonymität des Bezahlens mit elektronischem Bargeld sicherzustellen.

Eine nützliche Anwendung von Signaturen finden wir bei der MAC (Message-Authentication – Code) Adresse bei Netzwerkkarten. Die MAC-Adresse wahrt Integrität und Authentizität von Daten und Nachrichten und nicht den Absender!

Die derzeitige Zukunft der Signaturen tendiert zunehmend zu den biometrischen Verfahren. Die Authentizität von Personen werden aufgrund von unveränderlichen körperlichen Merkmalen wie Stimme, Gesicht, Fingerabdruck, Netzhautstruktur usw. bestimmt. Die moderne Bildverarbeitung und künstliche Intelligenz zukünftiger Computer machen diese Technik möglich. Die Eingabe von PIN's und Geheimcodes werden nun durch den Menschen an sich ersetzt. Missbrauch und Diebstähle können nun häufiger verhindert werden, denn im Gegensatz zur Biometrik, kann der Mensch sein PIN bzw. Daten vergessen oder falsch anwenden, indem er zum Beispiel wichtige Daten notiert.

2.2.3 Sicherheit

Die Sicherheit von RSA wurde schon oft von Kryptoanalytikern getestet. Dabei resultierten verschiedene Methoden, RSA theoretisch und praktisch zu knacken und den Algorithmus dadurch gleichzeitig zu verbessern. Eine wichtige Voraussetzung ist zum Beispiel die Geheimhaltung der beiden Primzahlen p und q. Diese müssen sehr große, zufällige und schwer zu erratene Primzahlen sein. Besitzt man diese, dann kann man die Nachrichten des Betreffenden so oft man möchte, ver- und entschlüsseln. Die Zahl n, die im öffentlichen Schlüssel enthalten ist, zeigt einen Angriffspunkt des Verfahrens. Doch die größte Schwierigkeit besteht darin, große Zahlen in ihre Primfaktoren zu zerlegen. Die Faktorisierung spielt dabei eine wichtige Rolle. Die einfachste Form zur Faktorisierung einer Zahl n ist das „Sieb des Eratosthenes". Dabei wird versucht, die Zahl n durch alle ungeraden Zahlen kleiner oder gleich √n zu dividieren. Kann man die Division verschiedener Zahlen als erfolglos bezeichnen, so können die vielfachen der Zahlen gestrichen werden. Bei diesem Versuch wächst die Rechenzeit direkt proportional zu √n.

Angriff	**Erkenntnis**
Chosen-Ciphertext-Angriff gegen RSA-Signatur.	1. Niemals beliebige, von Unbekannten vorgelegte Dokumente unterzeichnen. 2. Vor dem Signieren immer eine Einweg-Hash-Funktion anwenden (Abschnitt 6.3).
Angriff gegen RSA mit gemeinsamem Modul n.	Eine Benutzergruppe darf niemals den gleichen Wert für n wählen.
Bei kleinem Verschlüsselungsexponenten e (siehe Abschnitt 5.2.4) und kurzen Nachrichten ist ein Angriff möglich.	Nachrichten vor der Verschlüsselung auffüllen. Blöcke von M sollten etwa gleich lang sein wie n. PGP tut dies automatisch.
Angriff gegen RSA mit kleinem Entschlüsselungsexponenten d.	Großes d wählen. Dies ist bei kleinem e automatisch der Fall.
Angriff gegen Nachrichten, die zuerst verschlüsselt und dann signiert wurden.	Immer zuerst die Nachricht (Klartext) signieren und dann verschlüsseln.

Tabelle 5.1: Angriffe gegen RSA

Ein weiteres Verfahren, das bekannteste und schnellste, ist das Zahlkörpersieb, was sich durch das Prinzip des Probierens auszeichnet.

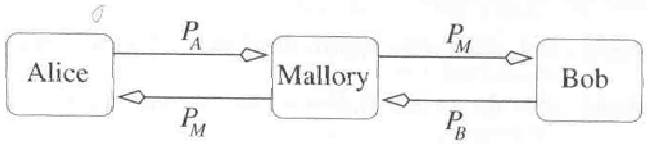
Der bekannteste Angriff auf Primfaktoren ist die Primfaktorzerlegung. Es kann natürlich theoretisch mehr Angriffe geben, doch keiner kann es genau sagen , ob zusätzliche existieren. Um diesen Angriffen effizient auszuweichen, benötigt man sogenannte Primzahltests. Die Primzahlen sollten möglichst zufällig berechnet werden und nach prim getestet werden. Ein statistischer Primzahltest für erlaubte Zahlen n wählt zuerst eine Menge an Zufallszahlen a(k) und berechnet $a(k)^{n-1/2}$

Falls $a(k)^{n-1/2}$ = +- 1, entscheidet man, ob n prim oder nicht prim ist.

Es gibt verschiedenartige Angriffe gegen Public-Key Algorithmen. Ein effizienter Angriff ist der Chosen Plaintext Angriff. Bei ihm ist der öffentliche Schlüssel bekannt und somit können beliebig viele Klartexte verschlüsselt werden und mit Anderen verglichen werden, vorrausgesetzt, der betreffende Geheimtext wurde abgefangen.

→ $E(P_a)(M) = CE(P_a)(M)$

Die Public-Key-Kryptographie lässt sich durch den MAN-IN-THE-MIDDLE-ANGRIFF sehr leicht aushebeln.



Der Angreifer „Mallory“ trennt dabei die Verbindung zwischen Alice und Bob, die beiden Kommunikationspartner, und täuscht dem Sender (Alice) vor, der Empfänger (Bob) zu sein und Bob täuscht er vor, Alice zu sein. Der Angreifer fängt die Daten während der Verbindung ab, verändert sie und leitet sie dann weiter. Die Funktionsweise besteht nur darin, indem er beide öffentliche Schlüssel abfängt und seinen eigenen öffentlichen Schlüssel an alle beide weiterleitet. Dieser Angriff lässt sich dennoch durch Prüfung der Authentizität des fremden öffentlichen Schlüssels vorbeugen. Der sogenannte Schlüsseltausch mit digitalen Signaturen.

Hierbei wird der Sitzungsschlüssel k mit dem geheimen Schlüssel vom Sender Alice signiert und so kann der Angreifer die Identität eines Kommunikationspartners nicht vortäuschen, denn der Angreifer besitzt den geheimen Schlüssel von Alice nicht. Gleichzeitig müssen die öffentlichen Schlüssel vorher sicher signiert und ausgetauscht wurden sein.

Das INTERLOCK -Protokoll stellt hierfür ein schönes Beispiel dar:

1. Alice sendet Bob ihren öffentlichen Schlüssel

2. Bob sendet Alice seinen öffentlichen Schlüssel

3. Alice chiffriert ihre Nachricht mit Bobs öffentlichem Schlüssel und sendet die Hälfte davon Bob zu

4. Bob chiffriert seine Nachricht mit Alice’s öffentlichem Schlüssel und sendet die Hälfte davon Alice zu

5. Alice schickt die 2.te Hälfte ihrer verschlüsselten Nachricht

6. Bob schickt die 2.te Hälfte seiner verschlüsselten Nachricht

7. Bob fügt beide Hälften von Alices Nachricht zusammen und dechiffriert sie mit seinem eigenen geheimen Schlüssel

8. Alice fügt beide Hälften von Bobs Nachricht zusammen und dechiffriert sie mit ihrem eigenen geheimen Schlüssel

Es gibt aber auch (Public-Key-)Algorithmen, die beim Austausch eines geheimen Schlüssels k zwischen Alice und Bob über einen unsicheren Kanal keine Mithilfe einer dritten Partei (TRUST- Center) benötigen. Der Diffie - Hellmann - Algorithmus stellt dabei ein passendes Beispiel dar.

Im ersten Schritt einigen sich Alice und Bob auf eine große Primzahl n und eine Zahl g. Diese beiden Zahlen dürfen öffentlich sein.

Im zweiten Schritt wählt Alice eine große Zufallszahl x aus und sendet das Ergebnis von $X = g^x \bmod n$ an Bob. Dabei ist X,g,n ihr öffentlicher Schlüssel und x,g,n ihr geheimer Schlüssel.

Als nächstes macht Bob das gleiche, nur das X gleich Y entspricht. Im vierten Schritt berechnet Alice den geheimen Schlüssel $k = Y^x \bmod n$. Und Bob berechnet seinen geheimen Schlüssel durch $k' = X^y \bmod n$

Dabei gilt k = k', d.h. $k = Y^x \bmod n = g^{x*y} \bmod n = X^y \bmod n = k'$

Falls der Kanal abgehört wird, dann kennt man n,g,X und Y, aber nicht den Sitzungsschlüssel k! Diese Verfahren ist natürlich nur bei großen Primzahlen sicher.

2.3 Anwendung

Eine wichtige Voraussetzung für eine sichere Anwendung des E-Commerce ist die praktische Kryptographie. Damit man im Netz Verträge, Geldtransaktionen und vertraulich-private Informationen der Kunden übertragen kann und diese auch dem Kunden anbieten muss, benötigt man starke Verschlüsselungen, damit diese Informationen nicht missbraucht oder verändert werden können. Bei verschieden Angeboten des Internets gibt es gleichzeitig auch unterschiedliche Zahlungsmöglichkeiten. Das elektronische Bargeld ist eine Methode, bei der man dem Anbieter einen bestimmten Geldbetrag überweißt und im Gegenzug eine bestimmte Anzahl von digitalen Münzen erhält. Eine übliche Methoden ist zum Beispiel, wenn man dem Händler eine Einzugsermächtigung erteilt, damit dieser von dem privaten Konto Geld abbuchen kann.

Elektronisches Bargeld ist gleichzustellen mit elektronischen Münzen. Das ist nichts anderes als Bitfolgen, die auf Chipkarten oder Computern abgespeichert werden. Ein kryptographisches Protokoll ist ein Verfahren zur Steuerung des Ablaufs von Transaktionen für bestimmte Anwendungen.

In Laufe der Zeit wurden schon verschiedene Protokolle vorgeschlagen, die schon gute Anwendungen besitzen. Ich werde auf ein spezielles näher eingehen. Dabei ist zu sagen, dass

der Austausch von Münzen bei Nutzung von Dienstleistungen und Services stets anonym und sicher gegen Betrug sein sollte. Das soll die Aufgabe der modernen Kryptographie sein!

Das Sicherheitsprotokoll E-Cash, dass auf der Grundlage von der E-Münze und E-Bank fußt, benutzt blinde Signaturen. Der Kunde erzeugt seine E-Münzen selber. Um zum Beispiel eine gültige 5 € Münze zu erhalten, generiert der eigene PC hundert Dateien, wo jeweils der Text „5€“ und große zufällig erzeugte Seriennummer geschrieben wird. Die Seriennummer muss daher groß sein, damit die Wahrscheinlichkeit für das zufällige Auftreten von 2 Nummern (weltweit) sehr klein ist.

Die Identität von Alice wird zuerst auf jeder ihrer Münzen gespeichert und gleichzeitig mit dem Secret-Splitting - Protokoll unkenntlich gemacht. Alice erzeugt danach n Münzen mit unterschiedlichen zufällig langen Seriennummern. Die Identität, die aus Name und Adresse besteht, wird mit dem Secret-Splitting –Protokoll, dass die Identität in Bitfolgen zerteilt, n-mal unterschiedlich geteilt und daraus n Identitätsfolgen berechnet.

Jede Identitätsfolge wird noch einmal in eine linke und rechte Folge geteilt. Jede Hälfte wird nochmals mit einer Einweg-Hash-Funktion überarbeitet, damit diese unerkenntlich und unveränderbar gemacht werden können und somit fast kein Betrugsversuch möglich ist. Alice verschlüsselt danach die n Münzen mit dem Protokoll für blinde Signaturen und verschickt diese nun an die Bank.

Die Bank verlangt nun von Alice bzw. dem Kunden die Entschlüsselung n-1 Münzen der zufällig gewählten Münzen. Die Bank wählt sich zum Beispiel 99 von 100 Münzen zufällig aus, die der Kunde offen legen muss. Sobald der Betrag 99 mal stimmt, dann wird die letzte Münze „blind“ signiert. Die Bank wird nun diese Münzen auf Betrag und Seriennummer überprüfen und bittet Alice die Identitätsfolgen offen zulegen. Wenn alles in Ordnung ist, wird die verbleibende Münze „blind“ signiert und zurückgeschickt. Alice macht die Münze lesbar und kann nun einkaufen gehen. Beim Einkaufen überprüft der Händler die Signatur der Bank der elektronischen Münze. Bei der Überprüfung muss Alice nur eine Hälfte jeder Identitätsfolge öffnen. Ist die Signatur wahrheitsgetreu, erhält Alice das gekaufte Produkt und der Händler bekommt die elektronische Münze und bringt diese zu seiner Bank und erhält dann eine Gutschrift auf sein Konto.

Die Bank überprüft nun wieder die Signatur und gleicht dabei in ihrer Datenbank ab, ob die Münze mit gleicher Seriennummer schon einmal eingegangen ist. Trifft der Fall nicht zu, dann bekommt der Händler sein Geld. Die Seriennummer und alle Identitätsfolgen werden nun in der Datenbank protokolliert. Findet man aber die Seriennummer schon in der Datenbank, dann rechnet man mit einem Betrugsversuch.

In Amerika ist es sogar üblich, Beträge von der Kreditkarte abzubuchen. Dabei besteht aber immer die Gefahr der richtigen Authentifikation des Kunden gegenüber dem Händler und die sichere Übertragung der Daten von der Kreditkarte. Im Internet herrscht der sogenannte „Cyber-Cash“ vor. Dies ist ein kreditkartenbasierendes Einkaufssystem, was per Internet verschlüsselt wird. Die Kreditkartentransaktionen müssen dabei sehr stark verschlüsselt, authentifiziert und mit Public - Key Paaren und einmaligen Zertifikaten besetzt werden.

Eine andere sichere Methode ist die Belastung der eigenen Telefonrechnung. Dabei wird der zu zahlende Betrag am Monatsende vom Telefonkonto abgebucht. Eine etwas moderne Art der Bezahlung ist die Benutzung einer Geldkarte. Dabei wird der elektronisch vorhandene Geldbetrag auf Chipspeicherbausteinen (meist auch auf der EC-Karte) gespeichert. Auf dieser

ist die Benutzerkennung, das Benutzerkonto und der Geldbetrag gespeichert. Bei Bezahlung bzw. Transaktionen wird der vorhandene Geldbetrag einfach subtrahiert. Zusammenfassend kann man sagen, dass es bis heute noch keinen einheitlichen Standard für den elektronischen Zahlungsverkehr gibt. Es werden noch zuviel unterschiedliche elektronische Zahlungsmöglichkeiten angeboten.

Verschiedene Systeme wenden die Technik des Public-Key-Verfahrens an. Ein Standardprogramm heißt OpenPGP. Nachdem PGP 6 Jahre erfolgreich im Einsatz war, wurde es 2000 und 2001 erfolgreich geknackt. Ein anderes System, welches für Zertifikate geeignet ist, nennt sich das S/MIME und X.509 Protokoll. Das "Secure Multipurpose Internet Mail Extension" Protokoll wird zum Verschlüsseln und Signieren von E-Mail benutzt.

Eine andere häufige Anwendung, auch häufig auf UNIX-Systemen zu finden, heißt SSH – Secure Shell. Sie ist die verschlüsselte FTP-Verbindung. Das FTP-Programm existiert schon seit den Anfängen des Internets, wo man an Verschlüsselung noch nicht dachte.

Dieses Programm dient dazu, um Zugriff auf entfernte Rechner zu bekommen (remote-Zugriff) und darauf zu arbeiten. Der Datenaustausch muss sicher sein und daher verschlüsselt werden. Darum besitzt das System sichere gegenseitige Authentifikation von Client und Server. Der Login auf den Rechner wird durch die Authentifizierung des Benutzers auf dem Server durch eine RSA Prüfung geschützt. Bei der verschlüsselten Kommunikation vereinbart das darin enthaltene symmetrische Verfahren RSA, IDEA, Blowfish, TRIPLE-DES usw. die Sitzungsschlüssel.

Eine von Netscape 1994 erfundene Anwendung im Internet, speziell für Internetbrowser ist das SSL-Secure Socket Layer – Protokoll. Der Internetbrowser kommuniziert über das http – Protokoll, indem HTML-Seiten vom Server zum Klienten verschickt werden, welches durch SSL nun abgesichert bzw. verschlüsselt wird.

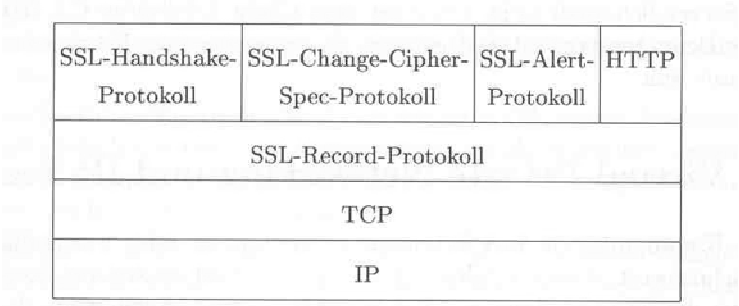


Abbildung 8.5: Die Protokollebenen von SSL.

Die Sicherheit und Verschlüsselung in Computernetzwerken gewinnt immer mehr an Bedeutung. Für solche Probleme wurde Virtual Private Networking und IP-Security entwickelt.

Die Funktionsweiße ist ganz einfach. Verschlüsselung und Authentifikation von ganzen Netzwerkschichten werden automatisiert und die Verschlüsselung von IP-Paketen wird realisiert.

Der Vorteil besteht darin, wenn jedes IP-Paket verschlüsselt wird, dann ist dieses Paket auch unabhängig vom übertragenen Protokoll. In der Praxis wendet man darum, seit 1994

veröffentlicht, IPSec (IP Security) an, dass für sicheren, kryptographisch verschlüsselten Verkehr sorgt.. Es arbeitet unter der Transportschicht, dem TCP Protokoll, des Netzwerkes und kann auch auf einer Firewall nicht umgegangen werden. Das Sicherheitsprotokoll IPSec arbeitet im Hintergrund, so das es der Benutzer gar nicht bemerkt.

Die Vorteile von dem am häufigsten verwendeten Nutzungsmittel des Internets, der E-Mail, zeigt, dass es auch bei ihr genug Möglichkeiten gibt, diese zu missbrauchen. Bei der E-Mail kann man mit geringem Aufwand sehr schnell Informationen austauschen. Heute werden aber immer häufiger wichtige und offizielle Dokumente wie Kaufverträge, Angebote und Rechnungen verschickt. Doch bei fehlender Authentifikation und (digitaler) Unterschrift, wie es auf Papier üblich ist, können Absender und der Inhalt der E-Mail beliebig verändert und manipuliert werden. Die Lösung nennt sich digitale und elektronische Unterschrift, welche wir oben im Kapitel FUNKTIONSWEISE besprochen haben. Die E-Mail wird durch eine riesige Anzahl von Knotenpunkten geschickt, bevor sie den eigentlichen Empfänger erreicht. Dieser Vorgang verläuft natürlich so rasant, das wir diesen schwer ergreifen können. Doch wenn eine Person Zugang zu einem Knotenpunkt, das kann ein beliebiger Rechner oder Server sein, besitzt, lassen sich gezielt Daten dieser E-Mail abrufen, weiterleiten oder verändern. Das selbe Prinzip gilt bei Online-Shopping, wenn diese Verbindung nicht verschlüsselt ist. Dabei sind jedoch sensiblere Informationen (wie Kreditkartennummer, Name, Adresse etc.) zum Abfangen möglich.

Die am häufigste verwendete Anwendung von Hash – Funktionen ist die Passwortverschlüsselung. In Betriebssystemen wie UNIX werden Benutzername und Kennwort zur Authentifizierung abgefragt. Das eingegebene Passwort wird verschlüsselt und wird mit einer Passwortdatei verglichen, die die Passwörter in verschlüsselter Form enthält. Der Benutzer von außen sieht in der Passwortdatei nur Buchstaben- und Zahlenfolgen. Die Berechnung der verschlüsselten Passwörter in ihre Klartextform dabei fast unmöglich. Ein Angriffsversuch, den man starten könnte, wäre der Wörterbuchangriff, der gleichzeitig sehr zeitaufwendig ist. Dazu benötigt man eine große Datei mit einer großen Anzahl häufig verwendeter Wörter, wie zum Beispiel Namen von Personen, Straßennamen usw. Die in dem Wörterbuch enthaltenen Namen werden nun alle einzeln verschlüsselt und einzeln mit der verschlüsselten Passwortdatei verglichen. Stimmen die beiden kryptografischen Namen überein, stimmt das zuletzt verwendete Wort.

In der Zukunft wird wahrscheinlich jeder Bürger eine eigene Chipkarte besitzen, wo seine eigene digitale Signatur und Unterschrift gespeichert ist. Der digitale Personalausweis steht hier für ein gutes und sehr reales Beispiel.

Ein europaweit einheitlicher digitaler Personalausweis ist das Ziel eines Projektes, das die EU-Kommission mit drei Millionen Euro fördert. Das Projekt FASME (Facilitating Administrative Services for Mobile Europeans) hat sich in einer Laufzeit von nur 18 Monaten ehrgeizige Ziele gesetzt.

Eine Chipkarte soll den herkömmlichen Ausweis ersetzen und die Abwicklung von Verwaltungsprozessen erheblich vereinfachen. Vorteile und Erleichterungen erhofft man sich vor allem bei Wohnungs- und Arbeitsplatzwechsel innerhalb Europas. Das bisher aufwendige Ummelden soll zukünftig durch das Einlesen der Chipkarte bei der entsprechenden Stadtverwaltung, später an beliebigen Chipkartenterminals per Internet, erfolgen. Gleichzeitig mit der Ummeldung des Wohnsitzes kann auch die Anmeldung bei der Müllabfuhr, den Stadtwerken sowie die Ummeldung des Autos geschehen.

Die Identifikation des Ausweisinhabers geschieht nach den bisherigen Plänen über seinen Fingerabdruck, der von einem auf der Chipkarte integrierten Sensor überprüft wird. Damit nur

berechtigte Stellen die Daten der Karte auslesen können, werden die Daten verschlüsselt abgelegt. Welche Verschlüsselungsalgorithmen zum Einsatz kommen werden, ist zum jetzigen Zeitpunkt allerdings noch nicht entschieden...

(URL: http://wiim.wiwi.tu-dresden.de/wist/hefte/0004/kb.html)

Das Ziel, wo Trust-Center immer mehr mit Einwohnermeldeämtern zusammenarbeiten, wird sehr stark angestrebt oder die Zertifizierung wird gleich ganz verstaatlicht.

Die Geldbörse mit elektronischen Münzen wird gerade im Internet ausgiebig getestet. Vielleicht treffen wir diese Technik bald auch im Alltag wieder. Dabei existiert dann kein Geld mehr aus Papier, welches man verlieren kann, sondern nur noch Geld aus Bits und Bytes, was wir mit uns herumtragen.

Die wichtigsten Anwendungen von „Fingerabdrücken“ ist die Sicherung der Benutzeridentifikation zum Beispiel bei Passwortabfragen. Sogenannte Identifikationskarten, zum Beispiel Chipkarten und Magnetsreifenkarten wahren die Identifikation durch die Abfrage eines 4-stelligen PIN’s. Passwortabfragen sind dennoch knackbar, weil ein bestimmter Code programmiert wurde, der zum Beispiel den PIN enthält. Neue Methoden, wie die Fingerabdrucksysteme, bei der der Wachsabdruck vermieden wird und der Hämoglobingehalt im Finger gesucht wird, die Netzhautanalyse, die wenig Raum für Manipulationen Platz lässt, und die Stimmanalyse, bei der das charakteristische Muster der Stimme gleichzeitig durch aufgezeichnete Mundbewegung bestimmt wird, stellen fast eine ideale und perfekte Sicherheit her.

Natürlich dürfen wir die Anwendung der Datenverschlüsselung in der Telekommunikation und Festnetz - Telefonie nicht vergessen. Der in den meisten Haushalten vorzufindende Telefonstandard heißt ISDN – Integrated Services Digital Network. Das Hauptanschluss oder das Terminal der ISDN-Anlage verwendet den Diffie-Hellman-Schlüsselaustausch, digitale Signaturen mit RSA und die Datenchiffrierung mit DES. Über die Telefonleitung kann man Sprache und Daten mit 64 Kilobit pro Sekunde übertragen und empfangen. Das Telefon enthält langfristig vorgesehene öffentliche und geheime Schlüsselpaare. Von 3 öffentlichen Schlüsseln dient einer als Identifikation des Telefons, der 2te zur Authentifikation von Befehlen des Eigentümers, der verändert werden kann, und der 3te dient als Schlüssel zum Netz. Der private Schlüssel des Benutzers ist in einem Hardware-Zündschlüssel gespeichert. Durch den Austausch und der Verifizierung der Beteiligten ist eine sichere Verbindung möglich.

3. Praxis Teil – Anwendung der Kryptographie

3.1 Gängige Software und Anwendungen

Im neuen Sicherheitsbetriebssystem von Microsoft, Windows 2000, wurde erstmals ein Verschlüsselungssystem für Dateien und Ordner integriert. Durch einfaches Klicken ist es möglich, seine Ordner und Dokumente zu verschlüsseln, um sie auf dem lokalen Rechner vor Unbefugten zu schützen. Werden diesen verschlüsselten Daten über das Netzwerk geschickt, so findet man bei heimlichen Abhören keinen Klartext vor. Nur unter hohem Zeit- und Rechenaufwand kann man die 128-Bit-Verschlüsselung in Windows 2000 knacken.

Im Explorer aktiviert man die Verschlüsselung für einen Ordner oder einer Datei als ein zusätzliches Attribut. Man klickt den Ordner mit der rechten Maustaste an und ruft dann die »Eigenschaften« auf, klickt auf »Erweitert« und wählt »Inhalt verschlüsseln, um Daten zu schützen«.



Verschlüsseln per Attribut: Schutz für Ihre Dateien.

Nach zweimaligem Klicken von »OK« fragt Windows, ob nur der Ordner oder auch die darin gespeicherten Dateien verschlüsselt werden sollen. Man wählt dann die zweite Option und bestätigt mit »OK«. Nun verschlüsselt Windows jede Datei, die man in diesen Ordner kopiert.

Man kann wie gewohnt mit den Daten arbeiten, während kein anderer Anwender auf den Inhalt Zugriff hat. Lediglich der Administrator besitzt noch einen Nachschlüssel.

Im Hintergrund erstellt Windows 2000 einen öffentlichen und einen geheimen Schlüssel nach dem RSA – Verfahren. Zur weiteren Verwendung der Schlüssel kann man diese sich auch ansehen oder exportieren. Man kann auch seine eigenen Schlüssel, die man vielleicht schon von anderen Verwendungszwecken besitzt, in die Schlüsselverwaltung von Windows 2000 importieren. Man öffnet hierbei die *Benutzer und Kennwörter* – Einstellungen unter der *Systemsteuerung* und klickt dann auf *Erweitert* und dann auf *Zertifikate*. In diesem Fenster kann man seine Zertifikate löschen, importieren, exportieren oder sogar Neue erstellen. Man sollte nie vergessen, diese Zertifikate an einem sicheren Ort extra zu sichern, wenn man das System neu installiert oder ein Virus die Festplatte befallen hat. In welchem Fall auch immer, wenn die Zertifikate einmal verschwunden sind oder gelöscht wurden, dann gibt es keine Möglichkeit mehr, auf diese verschlüsselten Daten zuzugreifen.

Es empfiehlt bei der Verschlüsselung von privaten E-Mails, das Programm **P**retty **G**ood **P**rivacy, kurz PGP, zu benutzen. Damit steht heute jedem Computer-Anwender eine starke und einfach zu bedienende Verschlüsselungs-Software zur Verfügung.

Die PGP-Geschichte:

Entwickelt wurde das Security-Tool 1991 von dem Amerikaner Phil Zimmermann. Für Privatanwender ist das Programm kostenlos erhältlich, sowohl für Windows als auch für MacOS und weitere Betriebssysteme. Der Optimierung und weiteren Verbreitung von PGP widmet sich eine Non-Profit-Initiative von Entwicklern. Wegen der unsicheren Zukunftsaussichten für die Freeware PGP, die vom Hersteller zwischenzeitlich schon einmal "stillgelegt" wurde, entstand das Open-Source-Projekt GnuPG. Es wird in Deutschland als GNU Privacy Guard Projekt vom Bundesministerium für Wirtschaft und Technologie unterstützt. Für den Anwender fallen die Unterschiede zwischen PGP und den Open-Source-Produkten nicht ins Gewicht. Grundsätzlich ist der Umgang mit der Verschlüsselungs-Software recht einfach - wie im Folgenden beschrieben.

PGP auf dem Computer einrichten:

Ist PGP auf der Festplatte installiert, überprüft es bestehende Verbindungen ins Internet. Fündig geworden, kann der User die Schnittstellen ins weltweite Netz gegen Angriffe absichern. Damit schützt das Programm vor Lauschangriffen oder dem "Mitschneiden" einer Schlüsselerstellung bei bestehender Internetverbindung.
Das Programm durchsucht die Festplatte automatisch nach bereits vorhandenen Vorgängerversionen und Schlüsseln. Ist noch nichts angelegt, startet der "Key Generation Wizar". Im Experten-Modus gibt man Namen und E-Mail-Adresse an. PGP erlaubt auch die nachträgliche Erstellung von Schlüsselpaaren, so dass für mehrere E-Mail-Adressen oder Personen, die sich einen Computer teilen, ein jeweils eigener Schlüssel vorhanden ist.
Man wählt dann das gewünschte Verschlüsselungsverfahren und die gewünschte Schlüssellänge. Man sollte nicht zögern, die größtmögliche Schlüssellänge anzugeben, da diese auch die maximale Sicherheit bietet.
Seinen privaten Schlüssel sollte man sehr gut schützen.
Zur Verwaltung des privaten Schlüssels ist es wichtig, eine geheime Passphrase (Zugangs-Password) zu erstellen, die unerwünschten Zugriff auf den heimischen PC oder Manipulationen verhindern soll, falls der Schlüssel in unbefugte Hände fällt. Je länger die Passphrase ist, um so besser ist Ihr privater Schlüssel geschützt. Am besten sollte man auch Umlaute, Sonderzeichen und Zahlen verwenden, da Namen, Zitate und rein alphabetische Buchstabenkombinationen für Cracker keine Probleme darstellen. Am besten denkt man sich einen unsinnigen Satz aus, und ersetzt zum Beispiel alle Selbstlaute durch eine Zahl. Garniert mit Sonderzeichen ist man dann auf der sicheren Seite.
Dann wiederholt man die Passphrase zur Bestätigung und bestätigt die Eingabe durch Drücken der Weiter-Schaltfläche. PGP erstellt nun automatisch ein Schlüsselpaar.
Nach der Fertigstellung der Schlüssel werden diese an einen virtuellen Schlüsselbund auf der Festplatte "angehängt". Zusätzlich hat man die Möglichkeit, den öffentlichen Schlüssel an einen Key-Server im Internet zu schicken.

Der virtuelle Schlüsselbund:

Unter dem Menüpunkt "PGP-Keys" der PGP-Tool Leiste kann man die eigenen Schlüssel verwalten, und zum Beispiel zusätzliche Schlüssel erstellen. Zugleich dient "PGP-Keys" als virtueller Schlüsselbund, an dem auch die öffentlichen Schlüssel von Kollegen, Freunden und anderen PGP-Anwendern "hängen" und zum Beispiel auf ihre Authentizität und Gültigkeit geprüft werden können. Ebenso kann man von hier aus den eigenen öffentlichen Schlüssel als circa drei KByte große Datei exportieren und via E-Mail an Freunde versenden.

Die erste verschlüsselte Mail:
Der Versand einer verschlüsselten E-Mail gestaltet sich unkompliziert. Die Mail schreibt man wie gewohnt, zum Beispiel in Outlook, und drückt vor dem Absenden auf das PGP-Icon in der rechten oberen Ecke. PGP sucht nun automatisch nach dem öffentlichen Schlüssel des Empfängers im Schlüsselbund und verschlüsselt dann die Mail. PGP integriert sich bei der Installation über Plug-Ins automatisch in die gängigsten Mail-Programme.

Mit Hilfe des Programms **Steganography 1.5** kann man beliebige ASCII Informationen in jedes beliebige Bild verstecken und so einen relativ sicheren steganographischen Austausch von Daten erreichen. Man benötigt nur ein Trägerbild, was die zu versteckenden Bilder „tragen“ soll und den Text, den man verstecken möchte. Zum Verstecken und Auslesen von Texten in Bildern benötigt man immer dasselbe Programm.
Dabei muss man jedoch einige Anforderung an das zu benutzende Bild beachten. Das Bild sollte möglichst viele verschiedene Farben enthalten. Manche Farbtöne (z.B.: grelles Rot) führen zu schlechteren Ergebnissen. Nur durch Ausprobieren kann man ein Gefühl für das ideale Trägerbitmap entwickeln. Je größer das Bitmap ist, umso mehr Informationen kann es aufnehmen.
Zum Verstecken einer Nachricht Verstecken gibt man unter "Quell-Datei" die zu versteckenden Daten an oder gibt in das untere Eingabefeld einen entsprechenden Text ein. Sollte letzteres der Fall sein, so betätigt man "Textfeld als Quelltext". Über "Trägerbild" kann man ein beliebiges Bitmap laden. Nun kann man die "Verschlüsselungsdichte" sowie "Verschlüsselungs-Abstände" angeben. Diese Werte beeinflussen die Menge der versteckbaren Daten, aber auch die Qualität des entstehenden Bildes.
Je kleiner die Werte der "Verschlüsselungs-Abstände" und "Verschlüsselungsdichte" sind, umso mehr Daten können versteckt werden, aber umso mehr wird auch die Qualität verschlechtert !
Mit "Verstecken" kann man nun die Daten im Bild verstecken lassen. Sollte das Ergebnis schlecht aussehen, betätigt man "Bild zurücksetzen" und wiederholt die obigen Vorgänge, wobei man die Verschlüsselungswerte ändern sollte. Ist das optimale Ergebnis erreicht, können man dieses (also das Bild mit den Informationen) unter "Bild Speichern" absichern. Dieses kann man nun zum Informationsaustausch (z.B.: E-Mail) einsetzen.



Hat man nun ein Bild mit versteckten Informationen erhalten, so lädt man es unter „Trägerbild / Bild mit versteckten Infos“ (Wichtig: Infos müssen mit diesem Programm versteckt worden sein!). Als nächstes betätigt man nun "Zeigen". Im Eingabefenster erscheinen nun alle Informationen. Diese kann man nun über "Textfeld speichern" absichern ("Quelle" zeigt evtl. den ursprünglichen Dateinamen an !).

Mit "Textfeld löschen" kann man immer das Eingabefeld löschen.
Mit "Kopieren" kann man den Text in die Zwischenablage kopieren.
Mit "Einfügen" kann man den Text aus der Zwischenablage in das Textfeld einfügen.

Zusätzlich sollte man beim Verstecken der Daten eine relativ sichere Textverschlüsselungen wie z.B. PGP (also z.B. Algorithmen wie IDEA, DES, Triple DES oder MDC) für die Quellinformationen (also vorher Quelldatei verschlüsseln oder verschlüsselten Text über Zwischenablage einfügen). Dadurch erhöht man die Sicherheit der Daten enorm! Auch das voreingestellte BMP Format sollte man nutzen , da durch nachträgliche Kompressionen (z.B. JPEG) Daten verloren gehen.
Für den Aufruf des „Verschlüsselungsprogrammes“ kann man den Programmpfad angeben und mit dem entsprechenden Button schnell auf ein Verschlüsselungstool zugreifen. Bei jedem Neustart von „Steganography 1.5“ wird diese Pfadangabe wieder geladen.

Das Programm kann man sich unter http://www.shadowhackers.de.vu herunterladen.

Das fortschrittliche Protokoll für Netzwerksicherheit, was nichts weiter ist als die verschlüsselte Form von IP (das **I**nternet **P**rotokoll: Unter der Verbindung mit dem TCP – Protokoll ist es die „Verständigungssprache“ im Internet), heißt **IPsec** bzw. IP Security (IP-Sicherheit). In den souveränsten Betriebsystemen, wie OpenBSD, ein weltweitverbreitetes UNIX-Betriebsystem, was sich durch sehr hohe Qualität in Sicherheit auszeichnet, und im neuesten Microsoft Produkt Windows 2000 kann es schon angewendet werden. Es dient dazu, Sicherheitsdienste auf der IP - Ebene anzubieten. Es stellt Methoden zur Authentifizierung und Datenverschlüsselung auf der Netzwerkebene bereit. IPSec kann heutzutage zur Einrichtung von **V**irtual-**P**rivate-**N**etworks genutzt werden.

Sicherheitsadministratoren bauen damit virtuelle und verschlüsselte logische Privatnetzwerke auf. Aufgrund mangelnder Kenntnis im Sicherheitsspektrum der Internetadministratoren und Anwender und das es sich bei IPSec weiterhin um ein relativ neues Erweiterungsprotokoll handelt, zeigt die Gründe es warum noch keine weite Verbreitung findet. In einigen Jahren könnte das ganz anders sein.

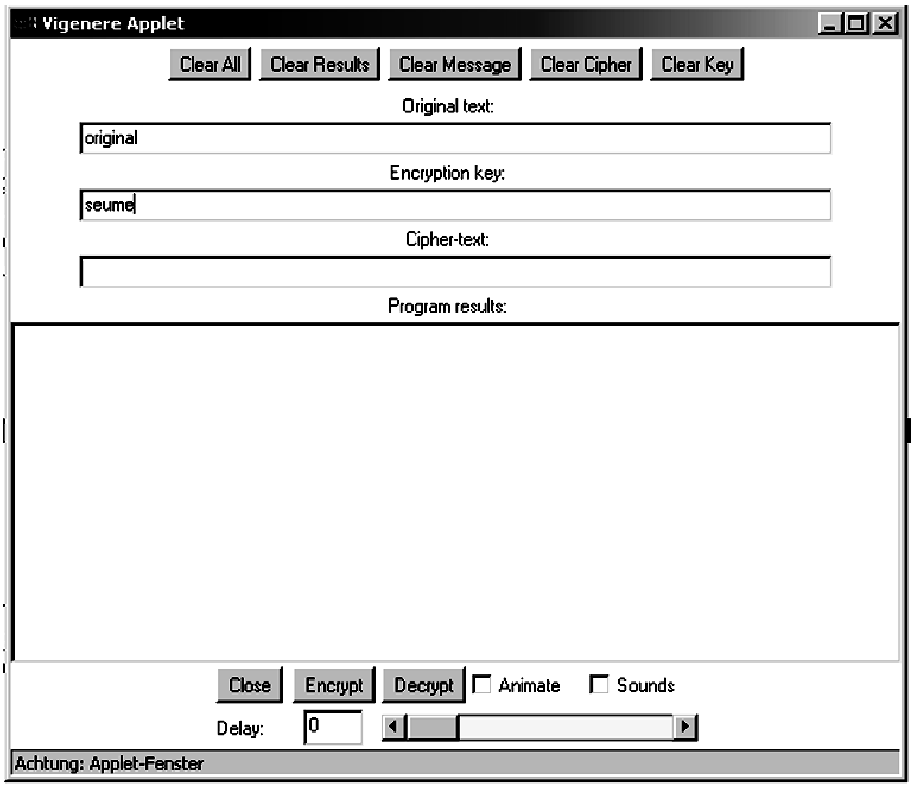
Der Verbindungsaufbau mit **IP-Sec** erfolgt immer in zwei Phasen. Die erste Phase handelt die Form der Authentifizierung aus. Windows 2000 unterstützt mit Kerberos, X.509 und vordefinierten statischen Texten drei Varianten, um den Austausch von Schlüsseln zu sichern. Nachdem die Authentifizierung definiert ist, lässt sich in der zweiten Phase ein symmetrischer Schlüssel für die Verbindung aushandeln und austauschen. Erst danach läuft die verschlüsselte Kommunikation.

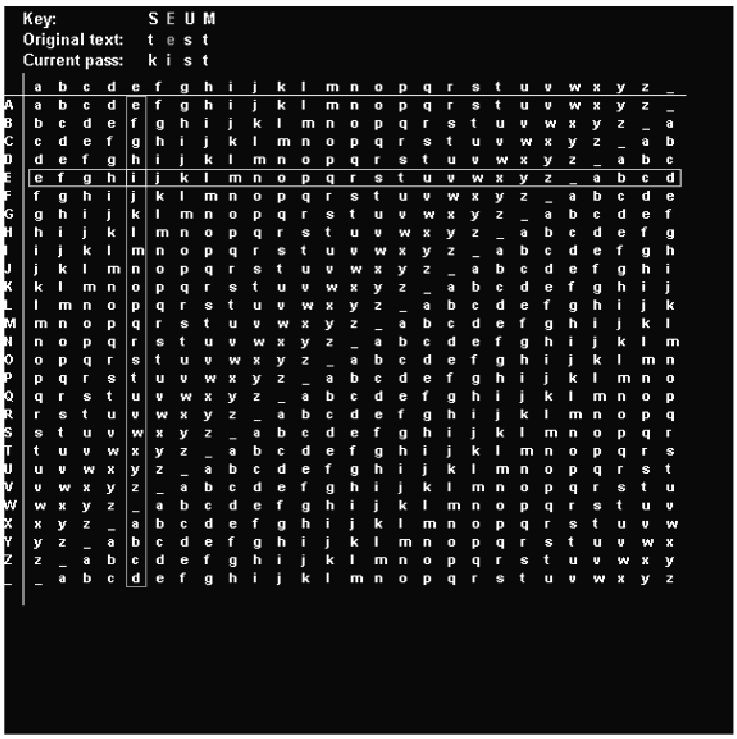
Die Konfiguration von **IP-Sec** erfolgt bei Windows 2000 über IP-Sec-Richtlinien, die im Active Directory abgelegt werden. Dort kann der Administrator die Richtlinien verwalteten, aktivieren und deaktivieren. Falls ein System nicht Mitglied einer Windows-2000-Domäne ist, werden die IP-Sec-Richtlinien in der lokalen Registry gespeichert.

Ein Richtlinienagent, der auf allen Windows-2000-Systemen ausführbar ist, überprüft, ob IP-Sec-Richtlinien für diese Workstation definiert sind. Dieser Agent übernimmt auch das Umsetzen der Richtlinien und übergibt die Informationen an die Treiber für IKE (Internet-Key-Exchange) und IP-Sec. IKE ist für die Aushandlung und den Austausch der Verschlüsselung zwischen den Kommunikationspartnern verantwortlich.

IPSec lässt sich unter den Einstellung der LAN-Verbindung unter dem Internetprotokoll TCP/IP aktivieren.

Wenn man sich mit seinen Freunden einfach verschlüsselte Nachrichten austauschen möchte, kann man im Internet ein Java - Applet benutzen, welches die Nachrichten mit dem Vigenère – Verfahren ver- und entschlüsselt. Auf der Website http://www.uncg.edu/mat/security/vigenere/vigenere.html gibt man den Originaltext und den jeweiligen Schlüssel ein. Wenn man auf die Schaltfläche „encrypt“ klickt, beginnt die Verschlüsselung. Die codierte Nachricht muss der Empfänger in das „cipher-text“ - Feld einfügen und natürlich den Schlüssel für die Entschlüsselung „decrypt“ wissen. Eine zusätzliche Option bietet sogar an, die Ver- und Entschlüsselung anhand einer Vigenère - Grafikanimation zu verfolgen. Damit kann man das Ver- und Entschlüsseln theoretisch sehr gut nachvollziehen.


Vigenere Applet
Clear All
Clear Results
Clear Message
Clear Cipher
Clear Key
Original text:
original
Encryption key:
seume
Cipher-text:
Program results:
Close
Encrypt
Decrypt
Animate
Sounds
Delay:
0
Achtung: Applet-Fenster


Key: S E U M
Original text: t e s t
Current pass: k i s t

Eine andere und sehr attraktive Anwendung wurde für den Fall entwickelt, wenn man einmal seine Geldbörse verliert. Denn dann sind auch gleichzeitig die ganzen Geldkarten bzw. und SmartCards verloren. Mit dem tragbaren Java-Ring – **Java-„iButton“** – macht man sich wirklich zum Herren seiner Kartenvielfalt. Man trägt ja schließlich alle Zugangsdaten sicher verwahrt am Finger.



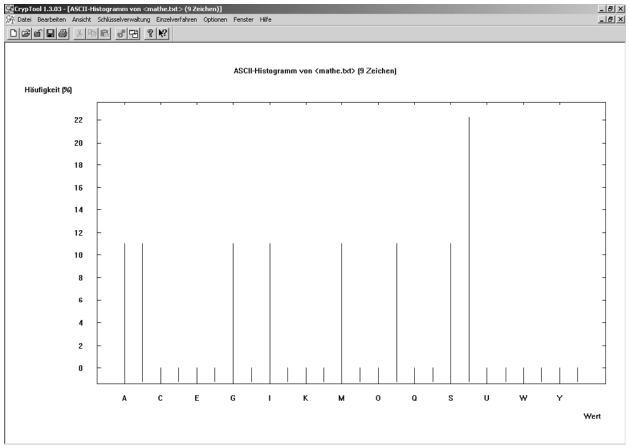
Derzeit gibt es für solche multifunktionale Chipkarten 3 Betriebssysteme: MULTOS, JavaCard und SmartCard für Windows. Doch einzig die Java-Lösung lässt derart komprimiert auf einen winzigen Ring platzieren, ohne dass die Funktionalität leiden müsste. Der Java-Ring ist ohnehin mehr als eine Karte. Das Herz des Ringes bildet der Java-“iButton“, der nichts weiter ist als ein Eine-Million-Transistor-Chip, der mit der leistungsstarken Javatechnik (JVM:Java Virtual Machine) ausgestattet ist. Neben dem winzigkleinen Hauptprozessor, ist auch der Arbeitsspeicher in einem Edelstahlgehäuse eingeschlossen. Zusätzlich arbeitet der „Ring“ mit einer Echtzeituhr und verfügt über ein 1024-Bit-Verschlüsselungsmodul nach dem RSA - Verfahren, bei dem jeder Partner über einen allgemein bekannten und einen geheimen Schlüssel besitzt. Jeder „Ring“ ist soweit eine Einzigartigkeit, als er mit einer einmalig vergebenen 8 Byte langen Seriennummer ausgeliefert wird. Der Datenaustausch erfolgt über einen 1-Kanal-Bus durch einfaches Anlegen an einen winzigen „Kartenleser“. Außerdem hält er eine spionageartige Finesse bereit. Wird der „Ring“ gewaltsam geöffnet, zerstört eine Säureschicht den Speicher innerhalb weniger Millisekunden. Gegen elektrostatische Aufladungen bis zu 25000 V und versehentlichen Waschgängen hält er stand. Als Alternative für das Speichern von Passwörtern und Zugangsdaten beispielsweise für das Online-Banking oder als Türöffner ist der Java-Ring sehr leicht einzusetzen.

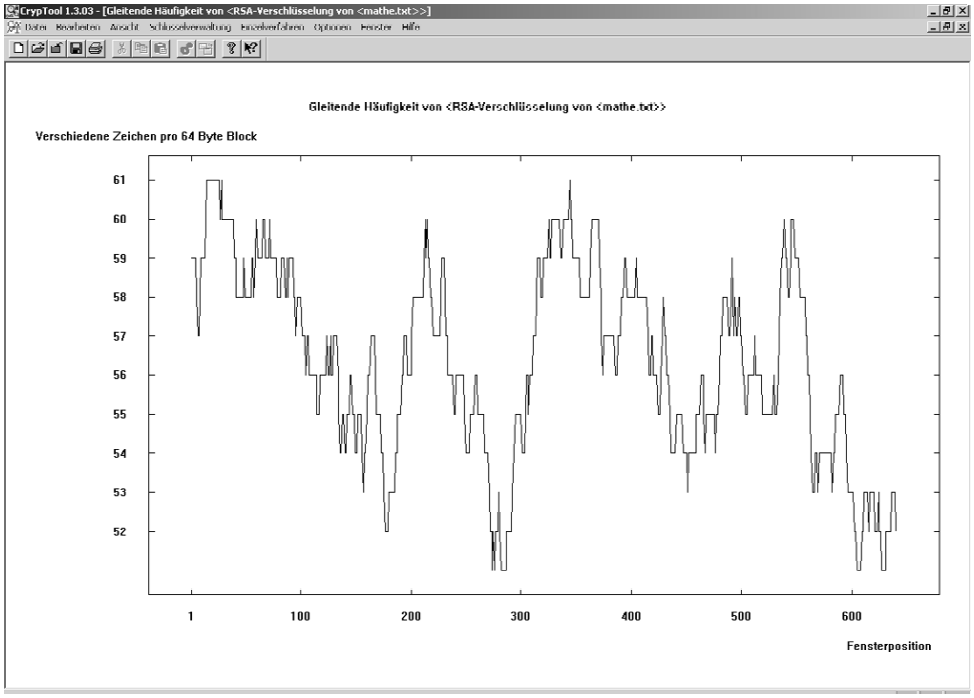


„Der Java-Ring ist ein fantastischer Ausgangspunkt für jede Konversation. Sie gewinnen schnell neue Gesprächspartner – mit 1024-Bit-Sicherheit.“

3.2 „Knacken“ in der Praxis

Dazu möchte ich das Programmpaket „**CrypTool**“ (http://www.cryptool.de) vorstellen, welches ein sehr gutes Werkzeug ist, was zum Erlernen und Erfahren von Kryptographie und zur Demonstration von Algorithmen und Analyse-Verfahren der Kryptographie gedacht ist. Neben den vielen klassischen und modernen Verschlüsselungstechniken, mit denen man beliebige Texte verschlüsseln kann, führt „CrypTool“ auch verschiedene Angriffe auf Verschlüsselungsverfahren durch (Kryptoanalyse). Es stellt Angriffe auf klassische Verfahren, wie zum Beispiel Caesar, Vigenère, Addition, XOR, monoalphabetische Substitution und viele weitere, bereit. Ein Brute-Force Angriff kann gegen symmetrische Verfahren genutzt werden. Eine Faktorisierung der Primzahlen wurde sogar integriert, um das RSA-Modul und die RSA-Signatur zu knacken. Weiterhin kann man Texte kryptographisch analysieren lassen und Zufallsdaten auf Qualität testen. Das Programm bietet die Option die von den meisten Algorithmen verschlüsselten Texte automatisch analysieren zu lassen, um somit den Schlüssel zu finden; oder man lässt den zu untersuchenden Text manuell analysieren, mit deren Hilfe man von Häufigkeitstabellen und komplizierten Analyseverfahren erste Lösungsansätze und Regelmäßigkeiten erkennen kann, damit man die Kryptoanalyse so besser nachvollziehen kann.





4. Schlusswort – Blick in die Zukunft

Niemand weiß heute, in welche Richtung sich das zukünftige Internet entwickelt. Eine bedeutende Anzahl von Nutzern haben einen Zugriff auf Hochgeschwindigkeitsverbindungen zum Internet. Die Hochgeschwindigkeitsleitung DSL (Digital Subscriber Line) ereicht Geschwindigkeiten zwischen 128 Kbps und mehr als 2Mbps, die wegen den unterschiedlichen Entfernungen zu den zentralen Niederlassungen des Anbieters variieren. Es ist höchstwahrscheinlich, das die Bandbreiten und die Geschwindigkeiten des Telefonnetze sehr stark ansteigen werden und infolge dessen noch moderne Technologien entstehen werden. Durch den Bedarf eines noch schnelleren Zuganges über Telefonleitungen zum Internet und der ständig wachsenden Anzahl neuer Internetnutzer ist diese Entwicklung immens notwendig. Das Internet entwickelt sich immer mehr zu einem wichtigen Teil im Leben eines Menschen. Standleitungen, die einen Zugang 24 Stunden am Tag zum Internet gewährleisten, sind heute schon Realität und werden überproportional zunehmen und führen zu neuen Sicherheitsproblemen am Computerarbeitsplatz. Banken und andere Finanzinstitutionen bieten ihre Bankgeschäfte über das Internet an. In 5 Jahren könnte der Gang zu Bank höchstwahrscheinlich komplett ersetzt sein.

Das Thema eines „papierlosen“ Büros wird heute schon sehr heiß diskutiert. Man schaut heute von dieser Technologie weitestgehend ab, da das Papier in den meisten Situation noch bequemer und schneller zum Bearbeiten verschiedener Aufträge genutzt wird. In einigen Firmen findet man aber schon erste Ansätze, in denen man Arbeitsvorgänge von Mitarbeitern in den Computer speichert. Zusätzliche Entwicklungen in der digitalen Signatur könnten den Abschluss von Verträgen und Dokumenten mit der Hand vollkommen ablösen und eine schnellere Abwicklungen von Verträgen garantieren. Denn Zeit ist Geld und viel Geld möchte jeder haben.

Wie sieht es denn nun mit der Sicherheit in der Zukunft aus? Und wie wird diese gelöst?

Den weltweiten Nutzern des Internets möchte man eine rechtliche Anonymität sichern, die jedoch schwer zu kontrollieren ist. Wenn wir uns im Netz befinden, sind wir jedes mal auf einem Server eingeloggt, der wichtige Daten von uns speichert. Viele Anbieter treten noch mehr in die Intimsphäre ein und legen spezielle Statistiken an, die dabei Surfcharakteristiken erstellen und somit ein Anlegen eines Kundenprofils ermöglicht, dass der gezielten Werbeeinblendung des jeweiligen Surfers dienen soll. Die Möglichkeit, seine eigenen Produkte besser zu vermarkten, steigt dabei erheblich an. Doch was ist, wenn wir diesen „Service“ überhaupt nicht in Anspruch nehmen wollen? Die meisten Internet Service Provider halten sich nicht oder müssen sich gar nicht mehr an die Verbote der Datenprotokollierung ihrer eigenen Kunden halten. Der Schritt zur vollen Kontrolle wird dabei immer näher gerückt. Letztendlich müssen wir Wege finden, um uns selber zu schützen und abzusichern.

Ein anderes Problem stellt immer noch die elektronische Überwachung weltweit dar. Einer Zwischenstudie zufolge werden in Europa alle E-Mail-, Telefon- und Faxverbindungen routinemäßig von der Nationalen Sicherheitsagentur der Vereinigten Staaten angezapft, und alle Zielinformationen werden vom Europäischen Festland über das strategische Zentrum in London und über das wichtige Zentrum in Menwith Hill in den North York Moors des Vereinigten Königreiches über Satellit nach Fort Meade in Maryland weitergeleitet.

Einerseits werden so zwar viele Informationen über potentielle Terroristen gesammelt, es gibt aber andererseits auch viele wirtschaftliche Einsätze, insbesondere für die intensive Überwachung all jener Länder, die an den GATT-Verhandlungen teilnehmen. Das sind 5 Länder, Großbritannien, Kanada, Neuseeland und Australien und die USA, die unter Vertrag Geheimdienstaktivitäten betreiben.

Mit der explosionsartigen Zunahme der Internetnutzung auf der ganzen Welt hat sich dessen Bedeutung für die private und geschäftliche Kommunikation, d. h. für die Möglichkeit, sich über eine Vielzahl von Quellen zu informieren, als weiterer Aufklärungskanal für Presse und Organisationen zu wirken und das Medium zum Nachrichten- und Informationsaustausch schlechthin zu werden, drastisch erhöht.
Diese Entwicklung wird sich fortsetzen.
Die Entwicklung des Internets führt dabei parallel zu einer Zunahme von Überlegungen und Begehrlichkeiten auf Seiten derer, die politische Kontrolle ausüben, das Internet und alle anderen Kommunikationswege zu kontrollieren und zu zensieren, da das Internet als Bedrohung staatlicher Autorität und politischer Machtausübung verstanden wird und sowohl mit, als auch neben dem Internet detaillierteste Daten über dessen Nutzer zu sammeln und zu verwerten oder die durch Überwachung gewonnenen Daten von Unternehmen anderer Länder zur Vorteilsnahme für die Unternehmen im eigenen Land zu missbrauchen.
Auch diese Entwicklung wird sich, verstärkt durch technologische Neuerungen, fortsetzen.
Die Entscheidungen, ob wir bald in einer Welt agieren werden, die keine "Privacy" und keinen ungehinderten Zugang zu Quellen aller Art mehr kennt, oder in einer Welt, wo die Freiheit auf Information und Selbstentfaltung, das Recht auf informationelle Selbstbestimmung und die Wahrung der Privatsphäre geachtet wird, fallen jetzt.

Ohne Verschlüsselung sind die modernen Kommunikationssysteme transparent für fortschrittliche Abhörvorrichtungen, die zum Mithören eingesetzt werden können.

"Der Computer ist zu einem universellen Arbeitsmittel geworden, das keine intellektuellen, politischen oder bürokratischen Grenzen kennt; eine allgegenwärtige Notwendigkeit, die die Welt umspannt und alle (politischen) Standpunkte übergreift."

Zitat: Clifford Stoll, Resultat nach dem er 1986 einem deutschen Hacker auf die Spur kam, welcher in amerikanische und militärische Computernetzwerke einbrach. Die gewonnen Informationen wurde dem KBG (russicher Geheimdienst) ausgeliefert. Die Suche sowie die Festnahme des Hacker wurden erfolgreich beendet.

[Buch: "KUCKUCKSEI-Die Jagd auf die deutschen Hacker, die das Pentagon knackten" 4. Auflage Sebtember 2000, Fischer Taschenbuch Verlag]

5. Quellenangaben

1. Verschlüsselungs-Verfahren für PC-Daten
   Schönleber, Claus
   1995 Franzis-Verlag GmbH
2. Algorithmenentwurf in der Kryptographie
   Gollmann Dieter
   Wissenschaftsverlag
3. Internet-Kryptographie
   Richard E. Smith
   ADDISON-WESLEY
4. Algorithmen und Datenstrukturen
   T. Ottmann / P. Widmayer
   Wissenschaftsverlag
5. Lehr- und Übungsbuch INFORMATIK | Band 2: Theorie der Informatik
   Christian Horn | Immo O. Kerner
   Fachbuchverlag Leipzig
6. Zum Thema: Computerkriminalität
   Rolf Günter
   bhv Verlags GmbH
7. Kryptographie - Verfahrn, Ziele, Einsatzmöglichkeiten (ausleihen!!!!)
   Gisbert W. Selke
   O'Reilly Verlag
8. Angewandte Kryptographie (Informationssicherheit) Protokolle,
   Algorithmen und Sourcecode in C
   Bruce Schneier
   Addison-wesley
9. Der neue Hacker's Guide - Sicherheit im Internet und im lokalen Netz
   anonymous
   new technology – Sams

Webseiten:

http://www.nsa.gov

http://www.vnunet.de/pc-pro/default.asp

http://www.ibutton.com

http://www.computec.ch/

http://www.cryptool.de/

http://www.kryptocrew.de/home/

http://www.sias.de/

http://www.pgpi.org/

http://www.uncg.edu/mat/security/vigenere/

http://www.shadowhackers.de.vu

Zeitschriften:

FUNK Amateur | Das Magazin für Funk Elektronik und Computer (52. Jahrgang Februar 2003)

Hiermit beglaubige ich, dass diese Arbeit ohne fremde Hilfe angefertigt wurde und nur die im Literaturverzeichnis angegebenen Quellen genutzt worden sind.

_____

Peter Weigel