Kryptographische Grundlagen

0.) Gliederung / Allgemeines

1.) Ziele
2.) Grundlagen
3.) Symmetrisches Verfahren
4.) Asymmetrisches Verfahren
5.) Sicherheit

Dieser Vortrag stellt eine Einführung in die Kryptographie dar, wobei es in den ersten beiden Punkten hauptsächlich um die Ziele, um Grundbegriffe und die Mathematik geht, im dritten und vierten Teil geht es meist allgemein um die zwei Hauptverfahrensweisen und deren Geschichte und der letzte Teil schließt mit einem Blick auf die derzeitige Sicherheit den Vortrag ab.
Die Begriffe Kryptologie und Kryptographie stammen aus dem Griechischen, wobei „kryptos“ soviel wie „geheim“ bedeutet, „logos“ das „Wort“ oder der „Sinn“ ist und „graphein“ etwa mit „schreiben“ zu übersetzen ist.
Früher wurde die Kryptographie eher als Grauzone des Spionagebereichs gesehen, heute im Zeitalter des Internets ist die Bedeutung der Kryptographie auch für den einfachen Nutzer stark angestiegen. Jeder benutzt Kryptographie, bewusst oder unbewusst, zum Beispiel in Form der EC-Karte, des Handys, von Pay-TV und vieles mehr.

1.) Ziele

Eine offensichtliche Anwendung der Kryptographie ist die **Geheimhaltung** von Daten aller Art. Sie dient der vertraulichen Kommunikation von zwei oder mehreren Teilnehmern. Anwendungen in der Praxis sind beispielsweise vertrauliche Bank- oder Börsengeschäfte, Bewerbungen via Internet und Firmengeheimnisse wie etwa Forschungsergebnisse und geheime Informationen zu neuen Produkten.
Die Funktionsweise ist einfach: Man hat einen Ausgangstext bzw. *Klartext* (engl. plaintext), dieser wird verschlüsselt (oder auch chiffriert) auf eine bestimmte Art, zu der wir später noch mal kommen. Als Ergebnis wird ein sogenannter *Geheimtext* (engl. ciphertext) erzeugt, der für einen Ausstehenden nicht (sinnvoll) lesbar ist und der an den bzw. die Teilnehmer übertragen wird. Dieser wird durch den Empfänger wieder entschlüsselt (oder auch dechiffriert), so dass der Klartext wieder sichtbar wird.

Ein *Schlüssel* bezeichnet eine geheime Information, die zum verschlüsseln bzw. entschlüsseln benutzt wird. Ein weiterer Begriff ist *Chiffre* bzw. *Code*, dass das Verfahren hinter der *Verschlüsselung* (engl. encryption) und *Entschlüsselung* (engl. decryption) kennzeichnet. Hier unterscheidet man zwischen den sogenannten symmetrischen Chiffren und den asymmetrischen Chiffren. Beim *symmetrischen Verfahren* wird ein- und derselbe Schlüssel für die Verschlüsselung und Entschlüsselung benutzt, während beim *asymmetrischen Verfahren* (oder *Public-Key-Verfahren*) unterschiedliche Schlüssel benutzt werden. Genaueres zu den Verfahren werden in Teil drei bzw. vier erklärt.

Ein weiteres Ziel der Kryptographie ist die **Authentifikation**. Der Begriff kennzeichnet gleich mehrere Anwendungen, die am Beispiel besser zu verstehen sind. Erste Anwendung am Beispiel der Bank ist, dass nur der Kontoinhaber über sein Bankkonto (zum Beispiel am Bankautomat) verfügen darf, er sich also als Inhaber identifizieren muss. Eine weitere Anwendung erklärt sich am Beispiel von Internettransaktionen bzw. Internetverträgen: Man kann und soll sicher nachweisen, dass man eine bestimmte Person auch wirklich ist, weiterhin kann so auch die Verbindlichkeit eines Vertrages festgeschrieben sein. Und die letzte Anwendung ist die Feststellung der Integrität der Daten, Beispiel hierfür ist wiederum die Bank, bei der eine elektronische Überweisung nachträglich von dritter Seite nicht verändert werden kann.
Das Verfahren hierzu ist, dass man einen Klartext mit einem Schlüssel (ähnlich einer Unterschrift) versehen wird (engl. *signing*), dieser Text wird mit dem Schlüssel an den Empfänger verschickt. Der Empfänger überprüft den Schlüssel (engl. *verifying*) und wird somit von der Echtheit des Dokuments überzeugt.
Man prophezeit, dass die sogenannte ‚*Elektronische Unterschrift*" als Signierungsverfahren der wichtigste Anwendungsfall der Kryptographie in der Zukunft sein wird.

Dazu kann man die Kryptographie zur Wahrung der **Anonymität** benutzen. Damit kann man seine Privatsphäre bei der Kommunikation, zum Beispiel bei einer Geschäftsabwicklung, schützen. Bei der normalen Bezahlung per Bargeld ist der Käufer dadurch nicht ausweisbar, ähnliches möchte man auch in anderen Bereichen. Weitere Anwendungsfälle sind Anrufe bei karikativen Organisationen, beispielsweise einer Telefonseelsorge, und deren Umsetzung im Internet via anonymen Newsgroups und Chiffreanzeigen in Zeitungen.

Ein letztes Ziel der Kryptographie ist die Erstellung von sogenannten **kryptographischen Protokollen**. Ein kryptographisches Protokoll stellt den Ablauf aller Aktionen der verschiedenen Teilnehmer von der Schlüsselgenerierung über den Schlüsseltransport bis zur Verschlüsselung und Entschlüsselung der Nachrichten dar. Ziel bei der Entwicklung guter Protokolle ist die Anpassung an die jeweiligen Erfordernisse, um so eine handhabbarere Verschlüsselung zu gewährleisten. Ein Beispiel findet sich im Bereich des Internets: Hier nutzt man häufig ein Protokoll, welches sich dadurch auszeichnet, dass man ein hybrides Verschlüsselungssystem benutzt, dass die Kombination von sicheren aber langsamen mit weniger sicheren, aber schnellen Verschlüsselungsalgorithmen umfasst. Gute Protokolle sind deshalb so wichtig, da eine gute Chiffrier- und Dechiffrierfunktion noch lange keine sichere Kommunikation gewährleisten, da es meist auch auf die Begleitumstände ankommt. Ein Beispiel hierfür findet man in der Geschichte: Die Enigma wurde im zweiten Weltkrieg von den Deutschen zur Verschlüsselung von Militärnachrichten benutzt. Diese Maschine wurde hauptsächlich nicht daher geknackt, also entschlüsselt, da eine schwache Verschlüsselung benutzt wurde, sondern da Codebücher mehrfach benutzt wurden und typische deutsche Armeenachrichten dieser Zeit kurz und monoton waren und dadurch die Entschlüsselung deutlich vereinfacht. Um eine sichere Verschlüsselung zu haben, braucht man also Protokolle, die Regeln zur einfachen, aber auch sicheren Handhabung bzw. deren Gebrauch aufstellen.

2.) Grundlagen

Die Grundlage der Kryptographie ist die Mathematik, deshalb werden als erstes **mathematische Grundlagen** gelegt:

*Eine Abbildung X => Y heißt **Einwegfunktion** f(x)=y, wenn für ein gegebenes x˛ X zwar y˛ Y leicht zu berechnen ist, aber für (fast) jedes y˛ Y es extrem schwer ist, ein Urbild x˛ X zu finden.*
Um diese Definition bildlich darzustellen, zwei Beispiele für eine Einwegfunktion:
1) In einem gedrucktes Telefonbuch ist es sehr einfach, mit einem Namen die passende Telefonnummer herausfinden, da die Namen alphabetisch geordnet sind, dagegen ist es nur sehr schwer möglich, zu einer Telefonnummer den passenden Namen zu finden.
2) Es ist sehr einfach eine Vase aus zehn Metern auf den Boden fallen zu lassen, jedoch ist es sehr schwer, diese aus den zerbrochenen Einzelteilen wieder zusammenzusetzen.
Die Einwegfunktion ist eine wichtige Grundlage für die Kryptographie, allerdings ist die Existenz von Einwegfunktionen mit dem berühmten Komplexitätsproblem P-NP verknüpft. Das heißt, dass Einwegfunktionen nur dann existieren, wenn P ungleich NP.
Mathematische Beispiele für Einwegfunktionen sind nach dem heutigen Wissensstand die diskreten Exponentialfunktionen und das Quadrieren modulo n mit n=pq.

*Eine **Falltürfunktion** ist eine Einwegfunktion, deren Funktionsinvertierung durch eine Geheiminformation wieder leicht möglich ist.*
Falltürfunktionen werden in der Literatur auch, dem Englischen angelehnt, Trapdoor-Einwegfunktionen genannt. Ein Beispiel für eine Falltürfunktion ist wiederum das Quadrieren modulo n mit n=pq, die ohne die Faktoren p und q nur sehr schwer zu invertieren ist, mit der Kenntnis von p und q ist es allerdings vergleichsweise einfach.

*Definition: Eine Einwegfunktion f heißt **kollisionsfrei**, falls es praktisch unmöglich ist, zwei verschiedene Werte x˛ X und x'˛ X in der Urbildmenge X zu finden mit f(x)=f(x').*
Eine direkte Anwendung der letzten Definition ist die ‚*Kryptographische Hashfunktion*“:
Man hat einen Klartext von beliebiger Länge, auf den man die Einweg-Hashfunktion anwendet und als Ausgabe einen Hashwert (oder auch Komprimat) fester Länge bekommt. Diese Hashfunktionen sind „echte“ kollisionsfreie Einwegfunktionen, also deren Umkehrung soll nicht möglich sein. Mit Hashfunktionen kann man sowohl den Urheber als auch die Integrität einer Nachricht nachweisen, vergleichbar mit einem Fingerabdruck. Dabei muss sich auch bei geschickter Veränderung der Nachricht der Hashwert ändern, weshalb diese Hashfunktionen kollisionsfrei sein müssen.
Gute Einweg-Hashfunktionen sind deshalb auch nur sehr schwer zu finden. Es gibt derzeit zwei Standardverfahren, einmal das vom amerikanischen Geheimdienst NSA entwickelte SHA-1, was als amerikanischer Standard definiert wurde, und zum zweiten RIPEMD-160, was quasi zum europäischen Standard erkoren wurde. Beide benutzen 160-Bit-Hashwerte.

***Kerkhoff Prinzip**: Sowohl die Verschlüsselungsfunktion als auch die Entschlüsselungsfunktion sind (öffentlich) bekannt.*
Dieses Prinzip hört sich beim ersten Mal unlogisch an, schließlich will man ja was geheim halten, warum veröffentliche ich dann das Verfahren? Allerdings ist ein Verfahren, welches öffentlich bekannt ist, auch öffentlich von Experten auf Herz und Nieren geprüft worden, und wenn dieses Verfahren auch danach noch als sicher gilt, dann muss es auch richtig gut sein. Wenn das Verschlüsselungsverfahren nicht veröffentlicht wurde, kann es weiterhin sein, dass Hintertüren zur einfachen Entschlüsselung für dritte Personen eingebaut sind.

*Eine Verschlüsselungsfunktion f ist **sicher**, wenn sie folgende Attacken übersteht:*
1) Ciphertext-Only-Attacke (Angreifer hat nur Geheimtext)
2) Known-Plaintext-Attacke (Angreifer hat ein paar Geheimtexte und deren Klartexte)
3) Chosen-Plaintext-Attacke (Angreifer hat Zugriff auf Verschlüsselungsfunktionen samt Schlüssel, kann diesen allerdings nicht extrahieren, aber spezielle Klartexte verschlüsseln)
4) Chosen-Ciphertext-Attacke (Angreifer hat Zugriff auf Entschlüsselungsfunktionen samt Schlüssel, kann diesen allerdings nicht extrahieren, aber spezielle Geheimtexte entschlüsseln)

Eigentlich gilt diese Definition nur für symmetrische Verfahren, sie kann aber auch für asymmetrische Verfahren benutzt werden mit der Einschränkung, dass der dritte Punkt beim Public-Key-Verfahren durch Veröffentlichung seines Schlüssels die normale Situation.

3.) Symmetrisches Prinzip

Bei der symmetrischen Verschlüsselung sind, wie schon erklärt, der Schlüssel für die Chiffrierung und Dechiffrierung gleich. Deshalb muss der Schlüssel geheim bleiben und vor der Kommunikation zwischen den Teilnehmern ausgetauscht werden. Voraussetzung ist also eine Verschlüsselungsfunktion f mit deren Umkehrfunktion f*.
Prinzip der Verschlüsselung: Geheimtext := f (Schlüssel, Klartext)
Prinzip der Entschlüsselung: f* (Schlüssel, Geheimtext) = Klartext

Es gibt zwei einfache klassische Verfahren:

Transpositionsverfahren:
Zeichen des Klartextes werden lediglich in der Reihenfolge vertauscht.

Dies wird meist über eine Matrix realisiert, wie ein folgendes einfaches Beispiel zeigt:
Verschlüsselter Text

DOATERGGRTIUVRST

wird in eine 4x4-Matrix jeweils senkrecht geschrieben

D	E	R	V
O	R	T	R
A	G	I	S
T	G	U	T

und waagerecht gelesen und Sinneinheiten abgetrennt:

DER VORTRAG IST GUT

Die Verschlüsselung funktioniert genau nach dem gleichen Prinzip, der Schlüssel ist die Kenntnis der 4x4-Matrix und deren Anordnung (senkrechte / waagrechte Schreibweise). Mehrfache Anwendungen der Transposition und / oder die permutierende Anwendung ist deutlich komplexer und damit schwieriger zu entschlüsseln.

Substitutionsverfahren:
Zeichen des Klartextes werden durch Zeichen einer festen (monoalphabetischen) oder variablen (polyalphabetischen) Zuordnungstabelle ersetzt.

Beispiele für Substitutionsverfahren sind die Codes von Cäsar, Vigenère, Hill und Playfair, die Prinzipien der Verfahren kann man in einschlägiger Literatur nachlesen.

Die symmetrische Verschlüsselung ist das deutlich ältere Verfahren, schon 600 v. u. Z. wurde in Babylon ein Verfahren namens ATBASH benutzt, 500 v. u. Z. benutzten die Griechen ein Verfahren namens SKYTALE, beides sind Transpositionsverfahren.
50 v. u. Z. wurde der Cäsar-Code von Julius Cäsar zur Verschlüsselung benutzt, allerdings ist dies nicht hundertprozentig bewiesen, wird aber meist in der Literatur als Einstieg benutzt .
1466 veröffentlichte Leon Battista Alberti ein Buch zum Chiffrieren, er war Sekretär am päpstlichen Hof und beschäftigte sich dort mit Geheimschriften. Er wird oft als Vater der Kryptographie bezeichnet.
1586 entwickelte Blaise de Vigenère, ein Diplomat, den nach ihm benannten Vigenère-Code. Dieser Code ist wohl das bekannteste Verschlüsselungsverfahren und galt lange als nicht knackbar, bis 1863 ein preußischer General a.D. namens Friedrich Kasiski ein Verfahren zur Lösung des Codes entwickelte und veröffentlichte.
1795 entwickelte der Vater der US-Unabhängigkeitserklärung Thomas Jefferson den ersten Chiffrierzylinder, nutzte diesen allerdings nie, so dass dieser erst 1922 wiederentdeckt wurde und nach einer Weiterentwicklung der US-Marine noch bis 1945 zu Diensten stand.
1883 veröffentlichte Auguste Kerkhoff ein Buch, welches als Meilenstein der Kryptographie der Telegraphenzeit gilt. In diesem Buch wurden auch die nach ihm benannten Kerkhoff Prinzipien aufgeschrieben, die zusammen mit den später entwickelten Prinzipien Shannons die allgemeine Theorie der Kryptographie begründen.
1917 entdeckte und entwickelte Gilbert S. Vernam das One-Time-Pad, welches später noch beschrieben und deren Besonderheit erklärt wird.
1975 entwickelte IBM das DES-Verfahren („Data Encryption Standard“), welches ab 1977 als Standardverfahren der USA festgeschrieben wurde. DES ist das kommerziell am häufigsten eingesetzte Verfahren, dass später noch verbessert wurde („Triple-DES“).
1990 wurde von Lai und Massey das IDEA-Verfahren („International Data Encryption Algorithm“) entwickelt, was als Teil des bekannten Verschlüsselungsprogramm PGP benutzt wird.

Substitutionsverfahren kann man wiederum in zwei Bereiche einteilen:

Blockchiffre: *Nachricht wird in Blöcke fester Länge aufgeteilt, die dann einzeln verschlüsselt werden.*
Somit werden im Grundmodus gleiche Klartextblöcke durch gleiche Geheimtextblöcke ersetzt. Beispiele für (komplexere) Blockchiffren sind DES und IDEA.

Stromchiffre: *Nachricht wird zeichenweise verschlüsselt, wobei sich der Schlüsselstrom von Zeichen zu Zeichen ändert.*
Hier werden also gleiche Klartextzeichen meist durch unterschiedliche Geheimtextzeichen ersetzt. Letztlich ist aber bei genauerer Betrachtung ein Blockchiffre ebenfalls ein Strom- oder Flusschiffre mit periodischen Fluss. Ein Beispiel für ein Stromchiffre ist das One-Time-Pad, welches jetzt noch etwas genauer beleuchtet wird:

Das **One-Time-Pad** ist der mathematisch besondere Prototyp aller Stromchiffren.
Die Nachricht und der Schlüssel liegen als Bitfolgen vor, wobei der Schlüssel mindestens so lang wie die Nachricht ist. Die Verschlüsselungsfunktion addiert entsprechende Bits des Klartextes und des Schlüssels mittels „modulo 2“, die Entschlüsselungsfunktion läuft exakt genauso ab. Das besondere hierbei ist, dass bei einmaliger Schlüsselverwendung das Verfahren absolut sicher ist, was auch theoretisch bewiesen wurde. Nachteile sind allerdings, dass ein Schlüssel nicht mehrfach verwendet werden darf, da ansonsten mit einer Known-Plaintext-Attacke das Verfahren knackbar ist, und es normalerweise unpraktikabel ist, dass der Schlüssel genauso lang ist wie die Nachricht. Dazu kommen noch die allgemeinen Nachteile von symmetrischen Verfahren wie beispielsweise der vorherige Austausch der Schlüssel der Teilnehmer.
Eine Anwendung soll wohl früher die direkte Verbindung von Moskau (UdSSR) und Washington (USA) gewesen sein, wo man große Koffer mit Schlüsseln für immens wichtige direkte Kommunikation („rotes Telefon“) verwendete.

4.) Asymmetrisches Prinzip

Bei der asymmetrischen Verschlüsselung gibt es verschiedene Schlüssel für die Chiffrierung und Dechiffrierung. Der Schlüssel für die Chiffrierung ist öffentlich bekannt („öffentlicher Schlüssel“), so dass jeder, der Zugriff auf diesen hat, dem Empfänger verschlüsselte Nachrichten schicken kann. Der Schlüssel für die Dechiffrierung ist nur dem Empfänger bekannt („privater Schlüssel“), der Empfänger kann so die Nachricht wieder entschlüsseln. Voraussetzung ist also eine Chiffrierfunktion E aus dem öffentlichen Schlüssel und eine Dechiffrierfunktion D aus dem privaten Schlüssel.
Prinzip der Verschlüsselung: Geheimtext := E (Klartext)
Prinzip der Entschlüsselung: D (Geheimtext) = Klartext
Wie schon erklärt, benutzt das asymmetrische Prinzip Falltürfunktionen, der öffentliche und der private Schlüssel bilden ein Schlüsselpaar, wobei vom öffentlichen Schlüssel es sehr schwer ist, auf den privaten Schlüssel zu schließen, andersrum ist es aber sehr einfach.
Die Vorteile von asymmetrischen Verfahren liegen auf Hand: Es ist kein vorheriger Schlüsselaustausch notwendig, somit ist auch eine verschlüsselte Kommunikation von Personen möglich, die sich selber nicht kennen. Außerdem wird durch die Bereitstellung des öffentlichen Schlüssels die Kommunikation mehrerer vereinfacht, da jeder nur einen Schlüssel allen Teilnehmern geben muss, während beim symmetrischen Verfahren durch die Geheimhaltung des Schlüssels ein Schlüssel je Teilnehmerpaar benötigt wird.

Die asymmetrische Verschlüsselung ist erst jung, sie wurde erst in den 70er Jahren entwickelt.
1970 wurde das Konzept des Public-Key-Verfahren vom British Secret Service entdeckt, wurde aber als Militärgeheimnis behandelt, außerdem gab es keine weitere Entwicklung.
1975 entdeckten dann Whitfield Diffie und Martin Hellmann das Konzept und veröffentlichten ihren Beweis der theoretischen Möglichkeit 1976. Eigentlich wollten sie aber die theoretische Unmöglichkeit des Public-Key-Verfahrens beweisen.
1978 veröffentlichten Ronald Rivest, Adi Shamir und Leonard Adleman das RSA-Verfahren, welches das erste praktisch handhabbare Public-Key-Verfahren war und auf der Schwierigkeit der „Faktorisierung großer Zahlen" beruht.
1984 wurde eine weiteres praktisch handhabbares Public-Key-Verfahren durch Taher ElGamal veröffentlicht, das sogenannte ElGamal-Verfahren, welches auf der Schwierigkeit beruht, „diskrete Logarithmen" zu berechnen.
1985 entwickelten Shafi Goldwasser, Silvio Micali, Charles Rackoff die Zero-Knowledge-Protokolle, bei denen der Grundgedanke ist, jemanden zu überzeugen, dass man im Besitz eines Geheimnisses ist, ohne vom Geheimnis das geringste zu verraten.

5.) Sicherheit

Sicherheitsbedenken:

Snake Oil (Schlangenöl):
Snake Oil sind Verschlüsselungsprogramme, bei denen der Anbieter den Verschlüsselungsalgorithmus nicht veröffentlicht. Dieses widerspricht den Kerkhoff Prinzipien, deshalb ist dies auch meist unsicher, da (eventuell) keine jahrelange Prüfung durch Experten vorgenommen wurde. Außerdem ist die Gefahr, dass Hintertüren (siehe unten) in den Algorithmus eingearbeitet wurden.

Exportbeschränkungen:
In den USA galt jahrelang ein Exportverbot für sichere Verschlüsselung, dass erst vor kurzem aufgehoben wurde. Verschlüsselungsalgorithmen galten in den USA als Waffen bzw. als militärisch sensible Technologie, so dass viele ältere Software-Programme aus den USA international nur mit unsicherer Verschlüsselung ausgeliefert wurden. Ein berühmtes Beispiel für die Exportbeschränkung war das bekannte Verschlüsselungsprogramm PGP. Diese Software durfte aufgrund der starken Verschlüsselung nicht exportiert werden, man fand allerdings eine aufwendige Lösung, indem man schließlich den gedruckten Sourcecode nach Europa geflogen hat und dort das Programm wieder eingescannt und kompiliert wurde.

Hintertüren / Key Escrow:
Manche Programme haben „Hintertüren" eingebaut, das heißt, dass eine einfache Entschlüsselung jeglicher Verschlüsselung mit dem Programm durch Kenntnis der Hintertür wieder möglich. Diese entstanden meist unter dem Druck des amerikanischen Geheimdienstes NSA, meist zum Zwecke der Wirtschaftsspionage, wie man vielfach auch aus der Presse erfahren konnte, beispielsweise unter dem Schlagwort „Echelon". Ein Beispielprogramm ist Lotes Notes, dass als Exportversion eine Hintertür für die NSA eingebaut hatte. Dies ist ein weiterer Grund für das Kerkhoff Prinzip der Veröffentlichung der Verschlüsselungsalgorithmen (hier des Quelltextes).
„Key Escrow" ist eine weiterer staatlicher Eingriff, bei dem der Benutzer seinen geheimen Schlüssel der Behörde übergeben muss. Dem Missbrauch wird damit natürlich Tür und Tor geöffnet, denn welche Behörde ist schon „berechtigt" oder wer schützt vor Bestechlichkeit?

Sicherheitsempfehlungen:

„Bundesamt für Sicherheit in der Informationstechnik“ empfiehlt im Bundesanzeiger 2001, dass eine sichere Hashfunktion mindestens eine Schlüssellänge von 160 Bit haben muss und eine sichere asymmetrische Verschlüsselung mindestens mit 1024-Bit-Schlüsseln arbeiten muss. Dies sind allerdings wirklich nur Mindestwerte, die Schlüssellängenempfehlung für eine asymmetrische Verschlüsselung liegt zur Zeit bei 2048 Bit. Zudem werden die Werte mit den Jahren sicherlich weiter ansteigen, so galt ein Mindestwert von 768-Bit-Schlüsseln bis Ende 2000 bei asymmetrischen Verfahren.

Zukünftige Sicherheit:

Ein Grund für die stetige Erhöhung der Schlüssellängen ist sicherlich, dass die künftige Entwicklung der Mathematik unklar ist. 1999 brauchte man 23 Stunden, um eine Nachricht, die mit dem DES-Algorithmus verschlüsselt wurde, zu knacken, wobei via Internet mehrere hundert Rechner „zusammengeschaltet“ wurden. Später brauchten 1600 Rechner via Internet 8 Monate, um eine 440-Bit-Zahl zu faktorisieren, auf die Faktorisierung bauen ja viele asymmetrische Verfahren auf. Dieses wurde mit einer ähnliche Methode wie die des „quadratischen Siebes“ realisiert. Man dachte auch lange, dass das Verfahren des quadratischen Siebes asymptotisch genauso schnell wie jede andere Faktorisierungsmethode ist. Aber unter Nutzung einer neuen Verfahren namens NFS („Number Field Sieve“) hätte man nur ein Zehntel der Zeit zur Entschlüsselung gebraucht. Das Zeitverhalten von NFS ist aber weiterhin exponentiell zur Anzahl der Stellen, so dass dies derzeit keine Gefahr für Public-Key-Verfahren ist, man muss halt einfach die Schlüssellängen weiter nach oben anpassen, um eine relative Sicherheit wiederherzustellen.