Standardisierung kryptographischer Dienste?

Standardisierung kryptographischer Dienste?

J.L. Massey

Die Bedeutung von Datensicherheit wird kurz diskutiert und eine Übersicht über die mathematischen Werkzeuge des Kryptologen gegeben. Es wird darauf hingewiesen, dass die Sicherheit aller praktisch anwendbaren Chiffriertechniken gegenwärtig nur auf Vermutungen beruht. Es wird der Standpunkt vertreten, dass, solange nicht nachweisbar sichere Techniken zur Verfügung stehen, kryptographische Dienste nicht standardisiert und ihre Anwendung den Benützern überlassen werden sollten.

L'importance de la sécurité des données est brièvement discutée et un aperçu des outils mathématiques du cryptologue est donné. Actuellement, la sécurité de toutes les techniques de chiffrement pratiquement applicables n'est basée que sur des suppositions. L'auteur estime que, tant que l'on ne dispose pas de techniques réellement sûres, les services cryptographiques ne devraient pas être normalisés et leur application devrait être laissée à leurs utilisateurs.

Dieser Aufsatz entspricht dem Vortrag, den der Autor in englischer Sprache an der Tagung «Sicherheitsaspekte in Datennetzen» der Schweizerischen Vereinigung für Datenverarbeitung gehalten hat. Die Übersetzung besorgte dipl. El.-Ing. H.-A. Loeliger, ETH Zürich.

Adresse des Autors

Prof. *J.L. Massey*, Institut für Signal- und Informationsverarbeitung, ETH-Zentrum, 8092 Zürich.

1. Einführung

Datensicherheit im hier verwendeten Sinn umfasst Geheimhaltung, Authentizität und Integrität von Nachrichten, die in einem digitalen Datennetz ausgetauscht werden. Geheimhaltung bedeutet, dass nur die beabsichtigten Empfänger die Nachricht in verständlicher Form erhalten können. Authentizität bedeutet, dass den beabsichtigten Empfängern die wahre Identität des Senders bekannt gemacht wird. Integrität bedeutet, dass der Inhalt der Nachricht während der Übermittlung durch das Netz in keiner Weise verändert wird. Manchmal wird der Begriff der Datensicherheit erweitert um «Geheimhaltung von Diensten» (d.h. die Tatsache, dass die Einheit A der Einheit B eine Nachricht sendet, darf der Einheit C nicht bekannt werden) und um «Authentizität von Diensten» (d.h. keine andere Einheit darf in der Lage sein, sich für eine Netz-einheit auszugeben, um Nachrichten zu ändern, zu verzögern, zu verdoppeln oder zu zerstören). Diese weiteren Aspekte der Datensicherheit gehen aber über den Rahmen dieses Beitrags hinaus.

Die Wissenschaft oder auch Kunst der Kryptographie hat zum Hauptziel, die Geheimhaltung, Authentizität und Integrität von Nachrichten sicherzustellen. Man sollte daher meinen, dass man, um Datensicherheit in einem Computernetz zu erreichen, nur die geeigneten Chiffriertechniken wählen und sie an den am günstigsten scheinenden Stellen in der Netzstruktur implementieren muss. Ein grosser Teil der gegenwärtigen Diskussion (über welche das «*IEEE Communications Magazine*» vom Juli 1985, das ganz der Datensicherheit gewidmet ist, einen guten Überblick gibt) konzentriert sich auf die zweite Frage, d.h. in welchen Schichten des ISO-Referenzmodells die verschiedenen kryptographischen Dienste angeboten werden sollten. Viel weniger Aufmerksamkeit wird der ersten Frage gewidmet, d.h. der Frage, welches die geeigneten Chiffriertechniken sind. Diese wird ganz ähnlich gestellt, wie man etwa nach geeigneten Techniken zur Fehlerkontrolle fragen könnte; tatsächlich besteht aber ein grundlegender Unterschied. Für irgendeine gegebene, in der Praxis verwendbare Technik zur Fehlerkontrolle kennt man das damit erreichbare Zuverlässigkeitsniveau, wenn auch nicht immer der beste Code bekannt ist. Hingegen gibt es *keine praktikable* Chiffriertechnik, deren Sicherheitsniveau heute abgeschätzt werden kann. Im nächsten Abschnitt wird diese Behauptung genauer erläutert und im letzten Abschnitt deren Bedeutung für die Netzwerkstandardisierung betrachtet.

2. Das Chaos in der Kryptographie

Die Techniken der Chiffrierung basieren auf drei Typen von mathematischen Funktionen, nämlich

1. Einwegfunktionen,
2. Trapdoor-Einwegfunktionen
3. Schlüssel-Einwegfunktionen.

Die beiden ersten Funktionstypen wurden von Diffie und Hellman [1] in ihrer bahnbrechenden Arbeit eingeführt, die das neue Gebiet der Public-Key-Kryptographie begründete. Der dritte Funktionstyp wird schon lange implizit in der klassischen oder Secret-Key-Kryptographie gebraucht, wurde aber erst kürzlich explizit von uns eingeführt [2].

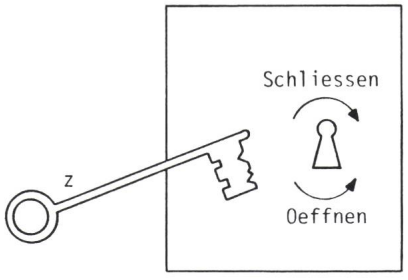


Fig. 1 Das mechanische Analogon einer Einwegfunktion

Mit dem Schlüssel kann nur geschlossen, nicht aber geöffnet werden.

Galois-Körper und Kryptographie

Die mathematische Theorie der endlichen Körper ist die Grundlage der Theorie der fehlerkorrigierenden Codes und spielt auch in der Kryptographie eine wichtige Rolle.

Ein *Körper* (engl. field) besteht aus einer Menge F von Elementen («Zahlen») und zwei Operationen, einer «Addition» und einer «Multiplikation». Die Apostrophe weisen darauf hin, dass den Begriffen eine umfassendere, nicht auf Zahlenkörper beschränkte Bedeutung zukommt. Die Menge F muss ein Nullelement (0) und ein Einselement (1) enthalten, und für die beiden Operationen müssen die für die normale Addition und Multiplikation gültigen Gesetze, d.h. Kommutativgesetz, Assoziativgesetz und Distributivgesetz gelten. Zudem müssen für jedes $a \in F, a \neq 0$, sowohl $(-a)$ als auch $(1/a)$ existieren, so dass $a + (-a) = 0$ und $a \cdot (1/a) = 1$. So bilden z.B. die reellen Zahlen zusammen mit der normalen Addition und Multiplikation einen Körper. Weitere bekannte Körper sind die rationalen Zahlen und die komplexen Zahlen. Die ganzen Zahlen stellen hingegen keinen Körper dar, weil der Kehrwert aller ganzen Zahlen ausser 1 und -1 keine ganze Zahl ist.

Ein *endlicher Körper*, auch *Galois-Körper* genannt, ist ein Körper, dessen Elementmenge F («Zahlenmenge») endlich ist. Alle bisher erwähnten Körper sind nichtendliche Körper, weil es unendlich viele rationale, reelle und komplexe Zahlen gibt. Hingegen bilden z.B. die ganzen Zahlen 0,1,2,3,4 einen Körper, wenn alle Additionen und Multiplikationen modulo 5 ausgeführt werden. In diesem Körper gelten z.B. folgende Gleichungen und Ableitungen, wie aus Figur F1 leicht ersichtlich ist:

$4 + 1 = 0 \rightarrow -4 = 1 \rightarrow 3 - 4 = 3 + 1 = 4;$
$2 \cdot 3 = 1 \rightarrow \frac{1}{2} = 3 \rightarrow \frac{3}{2} = 3 \cdot 3 = 4.$

Aus diesen und ähnlichen Ableitungen kann man zeigen, dass $-1 = 4$, $-2 = 3$, $-3 = 2$ und $\frac{1}{2} = 3$, $\frac{1}{3} = 2$, $\frac{1}{4} = 4$ ist.

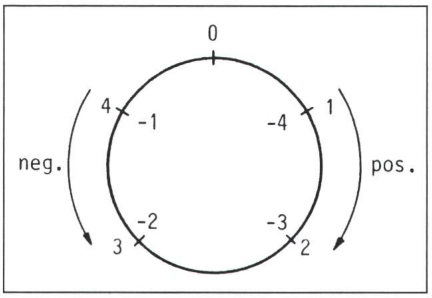


Fig. F1 Darstellung von GF(s)

Allgemein gilt, dass die ganzen Zahlen $0...p-1$ zusammen mit Addition und Multiplikation modulo p einen endlichen Körper bilden, wenn p eine Primzahl ist. Einen solchen Körper bezeichnet man mit $GF(p)$ (*G*alois *f*ield). Der kleinste mögliche Körper besteht aus den Zahlen 0 und 1, wobei die «Addition» einer ODER-Verknüpfung und die «Multiplikation» einer UND-Verknüpfung entspricht.

Eine Zahl α, $0 \leqslant \alpha < p$, wird *primitives Element* im Körper $GF(p)$ genannt, wenn die Potenzen $\alpha^1, \alpha^2, \alpha^3, ..., \alpha^{p-1}$ alle von Null verschiedenen Zahlen in diesem Körper darstellen.

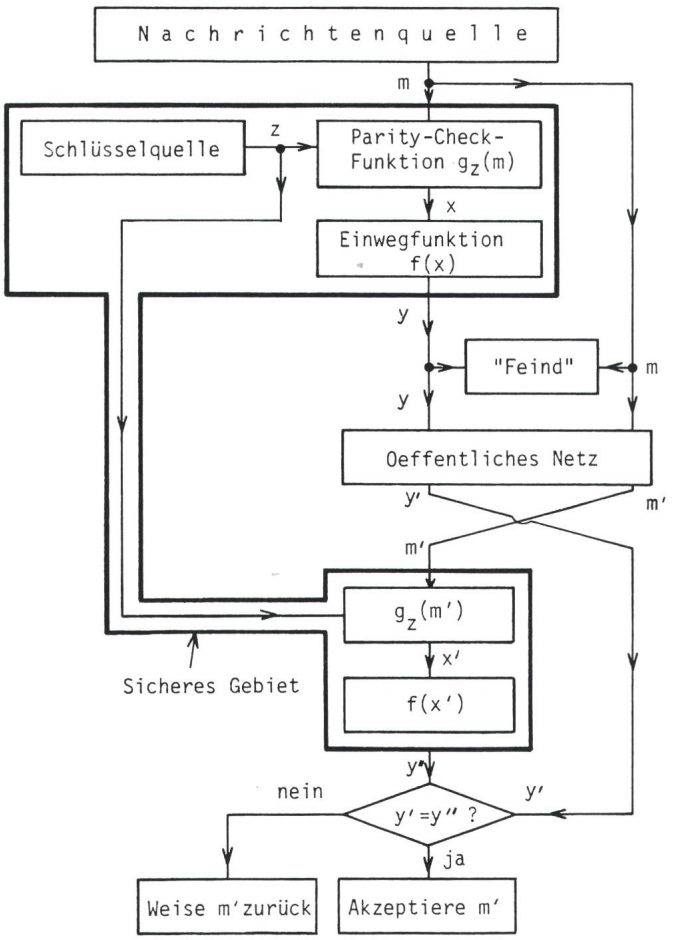
Beispiel: in $GF(5)$ ist 3 ein primitives Element, denn

$3^1 = 3$
$3^2 = 3 \cdot 3 = 4$
$3^3 = 3 \cdot 3^2 = 3 \cdot 4 = 2$
$3^4 = 3 \cdot 3^3 = 3 \cdot 2 = 1$

Die Funktion α^x ist auch in sehr grossen Körpern effizient berechenbar. Die Berechnung der Umkehrfunktion (Logarithmus) hingegen ist für grosse p (wenn einer der Primfaktoren von $p-1$ gross ist) mit den bekannten Algorithmen nicht zu bewältigen. Man vermutet daher, dass $f(x) = \alpha^x$ eine Einwegfunktion ist.

Eine *Einwegfunktion* ist eine Funktion f mit der Eigenschaft, dass $f(x)$ für alle x im Definitionsbereich von f leicht berechnet werden kann, während die Berechnung der Umkehrfunktion $f^{-1}(y)$ für praktisch alle y im Wertebereich von f aufwandbedingt undurchführbar ist. Die Figur 1 zeigt das mechanische Analogon einer Einwegfunktion. Diffie und Hellman vermuteten, dass $f(x) = \alpha^x$, $0 \leqslant x \leqslant p-2$, wobei α ein primitives Element in $GF(p)$ und p eine grosse Primzahl ist, eine Einwegfunktion ist. Später wurde diese Vermutung dahingehend abgeschwächt, dass einer der Primfaktoren von $p-1$ gross sein muss (s. Fenster «Galois-Körper und Kryptographie») [3]. Diffie und Hellman zeigten auch, wie mit dieser (mutmasslichen) Einwegfunktion der öffentliche Austausch von geheimen Schlüsseln zwischen Paaren von Benützern eines Netzes bewerkstelligt werden könnte. Die Figur 2 zeigt, wie eine Einwegfunktion verwendet werden kann, um ein Authentizitätssystem aufzubauen, welches einem Empfänger, der einen geheimen Schlüssel z mit dem Sender teilt, sowohl die Authentizität des Senders als auch die Integrität der Nachricht garantiert. Hingegen sorgt dieses

Fig. 2
Auf einer Einwegfunktion basierendes Authentizitätssystem



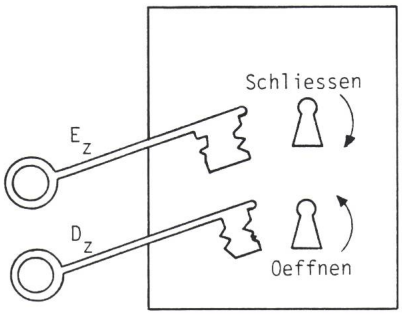


Fig. 3 Das mechanische Analogon einer Trapdoor-Einwegfunktion

System nicht für Geheimhaltung, da die Nachricht ja unchiffriert übertragen wird. Die Parity-Check-Funktion g_z muss nur die Eigenschaft haben, dass es zu jeder Nachricht m viele mögliche Werte $x = g_z(m)$ gibt; eine lineare Funktion erfüllt sehr schön diese Bedingung. Das System von Figur 2 erzeugt eine «Unterschrift» y für die Nachricht m. Diese Unterschrift kann vom Empfänger mit dem geheimen Schlüssel z überprüft werden, aber ohne z zu kennen, hätte niemand nur mit der Kenntnis von m y erzeugen können. Der «Feind» kann viele (m, y)-Paare beobachten, aber die Einwegfunktion hindert ihn daran, x zu berechnen, und somit kann er nicht bestimmen, welche Parity-Check-Funktion verwendet wird.

Eine *Trapdoor-Einwegfunktion* ist eigentlich eine Familie von invertierbaren Funktionen f_z, indiziert mit einem Parameter z, so dass erstens, wenn z bekannt ist, leicht effiziente Algorithmen E_z und D_z zur Berechnung von f_z bzw. f_z^{-1} gefunden werden können, aber zweitens bei Kenntnis von E_z allein die Berechnung von $f_z^{-1}(y)$ für praktisch alle y im Wertebereich von f_z aufwandbedingt undurchführbar ist. Die Figur 3 zeigt das mechanische Analogon. Diffie und Hellman gaben zwar die Definition einer Trapdoor-Einwegfunktion an und zeigten, wie damit ein Public-Key-Chiffriersystem (Fig. 4) aufgebaut werden könnte, aber sie wagten nicht einmal, einen Vorschlag für eine solche Funktion zu machen. Es blieb Rivest, Shamir und Adleman (RSA) vorbehalten, die erste mutmassliche Trapdoor-Einwegfunktion vorzuschlagen [4]. Bei dieser mutmasslichen Trapdoor-Einwegfunktion besteht z aus drei positiven ganzen Zahlen $z = (p, q, e)$. Dabei sind p und q zwei verschiedene, grosse Primzahlen (mindestens 100 Dezimalstellen), so dass sowohl einer der Primfaktoren von $p-1$ als auch einer der Primfaktoren von $q-1$ gross ist. Die Zahl e muss kleiner als das Produkt $(p-1)(q-1)$ sein und darf mit diesem keinen gemeinsamen Primfaktor haben. Der Chiffrierexponent e und das Produkt $m = pq$ werden publiziert. Dies entspricht der Veröffentlichung eines Algorithmus zur Berechnung der RSA-Trapdoor-Einwegfunktion $f_z(x) = x^e$ mit $0 \leqslant x < m$, wobei die Exponentiation modulo m ausgeführt wird. Wer z kennt, kann leicht den Kehrwert d von e modulo $(p-1)(q-1)$ finden und somit leicht $f_z^{-1}(y) = y^d$ berechnen, wobei die Exponentiation wiederum modulo m ausgeführt wird. Für $e = 3$ ist die Bestimmung von d der Faktorisierung von m äquivalent. Es hat den Anschein, dass jede Methode zur Berechnung $f_z^{-1}(y)$ für die meisten y der Faktorisierung von m äquivalent ist, aber weder ist dies bewiesen, noch ist bewiesen, dass die anscheinend schwierige Faktorisierung von m tatsächlich inhärent schwierig ist (s. Fenster «Beispiel zum RSA-Public-Key-Chiffriersystem»).

Eine *Schlüssel-Einwegfunktion* ist eine Familie von invertierbaren Funktionen f_z, die so mit einem Schlüssel z indiziert ist, dass es erstens, wenn z bekannt ist, einfach ist, effiziente Algorithmen E_z und D_z zur Berechnung von f_z bzw. f_z^{-1} zu finden, aber dass es zweitens - selbst dann, wenn eine Black Box zur Verfügung steht, die zu jeder Eingabe x augenblicklich $f_z(x)$ berechnet - ohne Kenntnis von z für praktisch alle y im Wertebereich von f_z aufwandbedingt undurchführbar ist, $f_z^{-1}(y)$ zu bestimmen. Die Figur 5 zeigt das mechanische Analogon einer Schlüssel-Einwegfunktion. Es dürfte offensichtlich sein, dass man eine Schlüssel-Einwegfunktion zum Aufbau eines Secret-Key-Chiffriersystems wie in Figur 6 verwenden kann, das gegen eine *Attacke mit wählbarem Klartext* (chosen plaintext attack) sicher ist, d.h. eine Attacke, bei welcher der feindliche Analytiker das Chiffrat für jeden frei gewählten Klartext erhalten kann. Es ist eine unter Kryptologen verbreitete (aber nicht von allen geteilte) Vermutung, dass das Data Encryption Standard (DES) System [5] eine Schlüssel-Einwegfunktion darstellt. Die DES-Funktion hat eine Schlüssel z von 56 bit; sowohl der Klartext x als auch das Chiffrat sind 64 bit lang. Man glaubt allgemein, dass Mehrfachchiffrierung des Klartexts mit mindestens drei DES-Systemen mit verschiedenen Schlüsseln die Sicherheit noch erhöht, aber das ist nicht bewiesen.

Die einfach Wahrheit ist, dass heute kein praktisch anwendbares und beweisbar sicheres Chiffriersystem irgendeines Typs existiert. Bis heute ist weder eine Einwegfunktion noch eine Trapdoor-Einwegfunktion, noch eine Schlüssel-Einwegfunktion nachweisbar demonstriert worden. Tatsächlich gibt es bis heute keinen Beweis dafür,

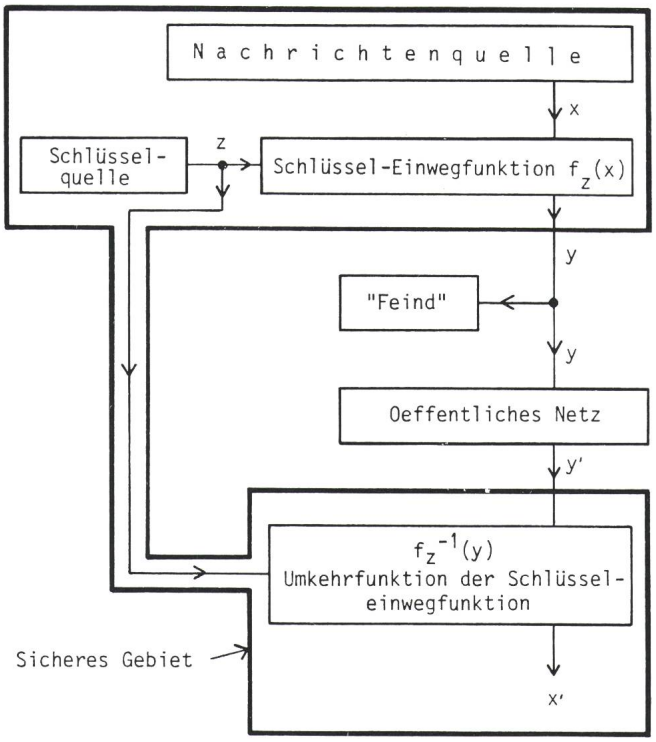


Fig. 4 Auf einer Trapdoor-Einwegfunktion basierendes Public-Key-Chiffriersystem

Beispiel zum RSA-Public-Key-Chiffriersystem

A möchte *B* die Nachricht [1,1,0,0,1,0] senden. Dazu wird die Nachricht als binäre Zahl 110010 interpretiert. Die entsprechende Dezimalziffer ist

$$x = 32 + 16 + 2 = 50$$

In einem öffentlichen Verzeichnis findet *A*, dass *B* die Werte $e = 17$ und $m = 77$ bekanntgegeben hat (bei einem brauchbaren Chiffriersystem müsste m viel grösser sein). *A* berechnet nun $x^e = 50^{17}$ modulo 77:

$$\begin{aligned} 50^2 &= 36 \\ 50^4 &= (50^2)^2 = 36^2 = 64 \\ 50^8 &= (50^4)^2 = 64^2 = 15 \\ 50^{16} &= (50^8)^2 = 15^2 = 71 \end{aligned}$$

$$50^{17} = 71 \cdot 50 = 8$$

Also sendet *A* an *B* die Nachricht $y = 8$, z.B. in der Form [0,0,1,0,0,0].

Der Empfänger *B* kennt als einziger die Primfaktorzerlegung von $m = p \cdot q$ und konnte deshalb den Kehrwert d von e modulo $(p-1)(q-1)$ berechnen. Damit kann er nun über

$$(x^e)^d = x \pmod{m}$$

die ursprüngliche Nachricht entschlüsseln. Die Methode beruht auf dem bekannten Satz aus der Zahlentheorie

$$x^{1+k(p-1)(q-1)} = x \pmod{pq}$$

wobei k eine beliebige ganze Zahl ist. Mit $p = 7$, $q = 11$ und $(p-1)(q-1) = 60$ lässt sich mittels eines bekannten, effizienten Algorithmus $d = 53$ berechnen.

B empfängt $y = 8$ und berechnet x aus $x = y^d$ modulo 77 mit

$$\begin{aligned} x &= 8^{53} \\ 8^2 &= 64 \\ 8^4 &= (8^2)^2 = 64^2 = 15 \\ 8^8 &= (8^4)^2 = 15^2 = 71 \\ 8^{16} &= (8^8)^2 = 71^2 = 36 \\ 8^{32} &= (8^{16})^2 = 36^2 = 64 \end{aligned}$$

$$x = 8^{53} = 8^{32} \cdot 8^{16} \cdot 8^4 \cdot 8 = 64 \cdot 36 \cdot 15 \cdot 8 = 50$$

Damit hat *B* die richtige Nachricht $x = 50$ erhalten.

dass eine Funktion von irgendeinem dieser drei Typen überhaupt existiert! Vielleicht suchen wir nach nichtexistenten Wesen. Im besten Licht betrachtet, haben wir heute einige Chiffriertechniken, deren Sicherheit gegen diejenigen Attacken nachgewiesen werden kann, die in der Vergangenheit gegen andere Chiffriersysteme Erfolg hatten. Es gehört eine beträchtliche Portion Glauben dazu, anzunehmen, dass wir tatsächlich «alle Löcher verstopft» haben und dass unsere Systeme den unorthodoxen Attacken nicht erliegen werden, die wir von dem wachsenden Heer der «Hacker» und von denjenigen böswilligeren Personen erwarten können, die von der Möglichkeit grosser finanzieller Gewinne angezogen werden, die sich aus der widerrechtlichen Aneignung, Änderung oder Zurückhaltung von Information in ausgedehnten Computernetzen ergeben können.

3. Einige Ansichten

Heute darüber zu diskutieren, wie wir Chiffriertechniken in öffentlichen Computernetzen einsetzen sollten, ist für den Autor etwa das gleiche, wie darüber zu diskutieren, wie ein Impfstoff gegen Krebs zu verteilen wäre. Das Beste, was man heute tun kann, ist, vor gewissen Dingen zu warnen, die das Krebsrisiko erhöhen. Ganz ähnlich scheint es heute um die Datensicherheit zu stehen; das Beste, was man tun kann, ist, jedermann davor zu

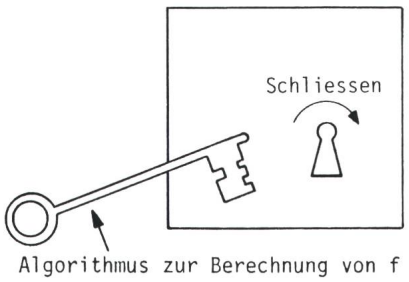


Fig. 5 Das mechanische Analogon einer Schlüssel-Einwegfunktion

warnen, auf die Datensicherheit öffentlicher Netze zu vertrauen. Es scheint dem Autor grundsätzlich falsch, Garantien für Datensicherheit zu geben, die nur auf Vermutungen beruhen; solche Garantien können Benützer nur zu Unvorsichtigkeiten verleiten, die sie sonst vielleicht vermeiden würden.

Um die Sache in Begriffen des ISO-Referenzmodells zu fassen: Der Autor empfiehlt, vorläufig alle kryptographischen Dienste der Applikationsschicht, also dem Benützer selbst, zu überlassen. Applikationseinheiten, die geheime Nachrichten austauschen wollen, werden die Schlüsselverteilung selbst organisieren und selbst ihre Lieblingschiffrier-Algorithmen bereitstellen müssen. Dieser Mangel an Standardisierung hat zwei Vorteile. Erstens erschwert er die Aufgabe des angehenden Eindringlings, und zweitens vermindert er den Schaden, wenn sich ein bestimmtes Chiffrierschema

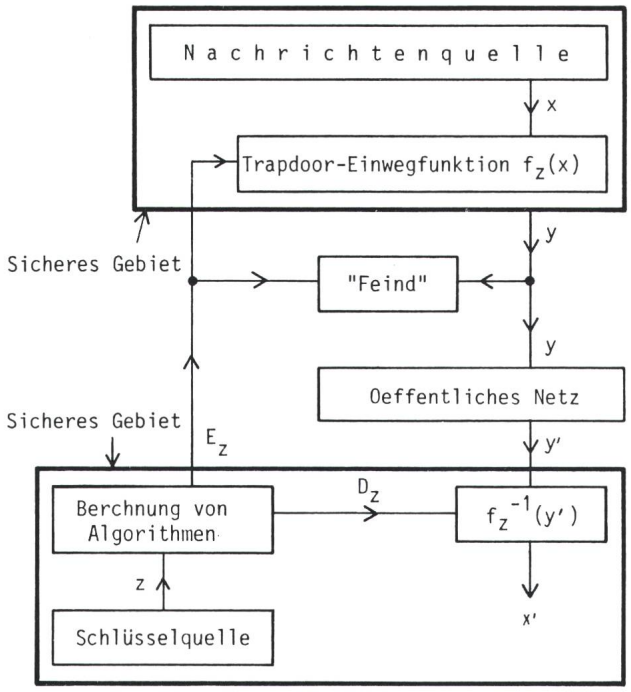


Fig. 6 Auf einer Schlüssel-Einwegfunktion basierendes Secret-Key-Chiffriersystem

als unsicher erweist.

Ein Impfstoff gegen Krebs scheint in weiter Ferne zu liegen. Im Vergleich dazu sind beweisbar sichere Chiffriertechniken nach Meinung des Autors schon fast in Reichweite. Auf signifikantem Niveau betriebene, wirklich wissenschaftliche kryptographische Forschung im öffentlichen Sektor ist weniger als ein Jahrzehnt alt - die Arbeit von *Diffie* und *Hellman* [1] markiert die Geburtsstunde der Kryptographie als Wissenschaft, und seither wurden viele Fortschritte gemacht. Zusammen mit *I. Ingemarsson* von der Linköping-Universität, Schweden, hat der Autor kürzlich ein Secret-Key-Chiffriersystem mit nachweisbarer Sicherheit gegen eine Attacke mit wählbarem Klartext vorgestellt, das aber wegen der astronomischen Dechiffrierverzögerung völlig unpraktikabel ist [6]. Trotzdem wagt der Autor jetzt die unbesonnene Vorhersage, dass praktikable und nachweisbar sichere Chiffriertechniken innerhalb der nächsten zehn Jahre erhältlich werden, und er nimmt mit Nachdruck Stellung gegen irgendeine Standardisierung, bevor solche Techniken zur Verfügung stehen.

Literatur

[1] *W. Diffie* and *M. E. Hellman:* New directions in cryptography. IEEE Trans. IT 22(1976)6, p. 644...654.

[2] *J. L. Massey:* Cryptography—A selective survey. Proceedings of the 1985 International Tirrenia Workshop on Digital Communications, Tirrenia/Italy, September 2...6, 1985.

[3] *S. C. Pohlig* and *M. E. Hellman:* An improved algorithm for computing logarithms over GF lp) and its cryptographic significance. IEEE Trans. IT 24(1978)1, p. 106...110.

[4] *R. L. Rivest, A. Shamir* and *L. Adleman:* A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(1978)2, p. 120...126.

[5] Data encryption standard. Federal Information Processing Standards (FIPS) Publication 46. Washington, National Bureau of Standards.

[6] *J. L. Massey* and *I. Ingemarsson:* The Rip van Winkle cipher—a simple and provably computationally secure cipher with a finite key. IEEE International Symposium on Information Theory, Brighton/England, June, 23...28, 1985.