HAMFU
HISTORY

KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1986/1987
Leitung:
Bundesamt für Übermittlungstruppen
Divisionär J. Biedermann, Waffenchef der Übermittlungstruppen

Von der Funkerkennung bis zur Zahlentheorie
Verteidigungsstrategien gegen Hacker

Referent: H. Mey, Prof., Dr. sc.techn. ETHZ

Diese Vorlesung wurde durch die Stiftung HAMFU digitalisiert und als
PDF Dokument für www.hamfu.ch aufbereitet.

VON DER FUNKERKENNUNG BIS ZUR ZAHLENTHEORIE: VERTEIDIGUNGSSTRATEGIEN GEGEN HACKER

H. Mey, Prof., Dr. sc. techn. ETH

INHALTSVERZEICHNIS

1. Problemstellung und Begriffe

2. Systematik von Authentifikationsmöglichkeiten
   2.1. Individuen und Objekte als Berechtigte
   2.2. Echtheitsprüfung von Objekten
   2.3. Echtheitsprüfung von Individuen
   2.4. Grundproblematik der Individualauthentifikation

3. Public Key-Systeme als Authentifikations-Basis
   3.1. Prinzip der Public Key-Methode
   3.2. Anwendungsbeispiel für die Atomtestüberprüfung

4. Authentifikation gegenüber Rechenzentren
   4.1. Authentifikation mit unverschlüsseltem Passwort
   4.2. Authentifikation mit verschlüsseltem Passwort
   4.3. Authentifikation mit Public Key
   4.4. Authentifikation mit "Funkerkennung"

5. Anmerkungen zur Sicherheit

Adresse des Autors:

H. Mey, Prof., Dr.sc.techn.ETH
Institut für Informatik und angewandte Mathematik der Universität Bern
Länggassstrasse 51
3012 Bern

"Krieg im Aether", Folge XXVI

1. PROBLEMSTELLUNG UND BEGRIFFE

Das erst einige Jahre alte Fachwort "Hacker" beschreibt eine Spezies von EDV-Fachleuten oder -Hobbyisten, die es sich zum Ziel machen, den Zugriff auf ein Computersystem zu erzwingen oder zu erschleichen, ohne dazu berechtigt zu sein. Je nach den verschiedenartigen Motiven (Fig. 1) handelt es sich dabei um mehr oder weniger deliktische bis kriminelle Handlungen. Die Hacker sind mit der Ausweitung von Computeranlagen zu offenen Systemen zum Problem geworden, wozu auch der allgemeine Ausbildungsstand in Informatik beigetragen hat.

Hacker	Erschleicht Zugriff auf ein Computersystem, ohne dazu berechtigt zu sein	≙ Einbruch
	zum Vergnügen und zum Training	≙ Sport
	aus Zerstörungslust	≙ Vandalismus
	zur Benützung von Ressourcen	≙ Diebstahl
	zur Ermittlung von Daten	≙ Spionage
Authentifikation (engl. Authentication)	Beglaubigung Ueberprüfung eines behaupteten Rechts, speziell: Zugriffsberechtigung	

Fig. 1 Hacker-Motivation

"Authentifikation" heisst eigentlich "Beglaubigung", nämlich die Festlegung der Authentizität eines Individuums, das aufgrund seiner Identität gewisse Rechte in Anspruch nehmen kann. Im Fall von Zugriff und Zugriffsschutz handelt es sich dabei um ein Recht oder um ein behauptetes Recht zum Zugriff auf ein Computersystem bzw. dessen Programme, Daten und Rechenleistungen. In diesem Zusammenhang wird heute "Authentifikation" als Begriff für jene Verfahren verstanden, mit denen Zugriffsberechtigungen überprüft werden können, und zwar in der Regel von Benützern bzw. Individuen, die über eine Datenleitung vom Rechenzentrum, dessen Zugriffsrecht sie behaupten, örtlich weit abgesetzt sind. Es gibt eine ganze Reihe allgemeiner und anerkannter Sicherheitsprinzipien (Fig. 2), die einzuhalten bzw. nach denen im Rechenzentrumsbetrieb zu verfahren ist, um unerlaubte Zugriffe abzuwehren.

① Daten/Programme nur kennen, speichern, archivieren, sofern (solange) man sie (noch) benötigt
② Passwort-Vorschriften peinlich genau kennen und einhalten
③ Zugriffsrechte teilen nach Ort (Anschluss-Nr), Personen (ID/PW) und eventuell Zeit
④ Strikte personelle Trennung Entwicklung/Produktion
⑤ Fehlerabfangen auf die sichere Seite (Error/No failure)
⑥ Keine vermeidbaren Verkettungen
⑦ Automatische Buchführung über alle Sessionen (zwecks eventueller späterer Rekonstruktion)
⑧ Einwandfreie Chiffrier- und Authentifikations-Verfahren

Fig. 2 Allgemeine Sicherheitsprinzipien

Nachfolgend wird nur der eine Punkt "Authentifikations-Verfahren" weiter diskutiert, alle anderen Punkte aus Figur 2 sind nicht Gegenstand der Ausführungen.

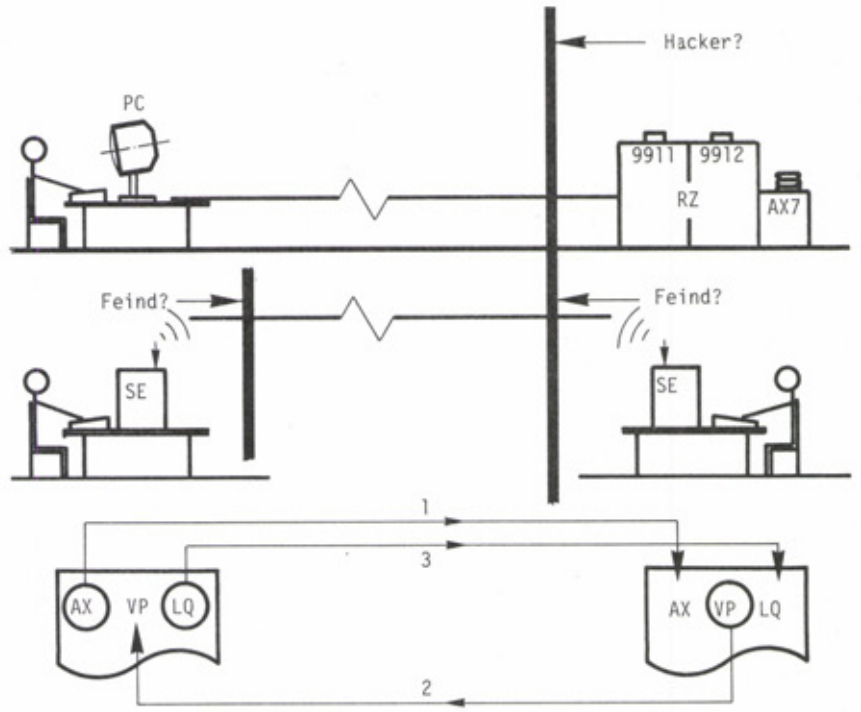


Fig. 3 Authentifikations-Situationen

In Figur 3 ist im obersten Bildteil die allgemeine Situation zwischen Rechenzentrum und abgesetztem Benützer dargestellt: Im Rechenzentrum stellt sich die Frage, ob dieser Benützer ein Hacker ohne Zugriffsrechte oder ein berechtigter Teilnehmer sei. Da der Benützer jedoch räumlich und logisch abgesetzt ist, besteht vom Rechenzentrum aus keinerlei Transparenz in Richtung Peripherie, mit Ausnahme jener, die durch die Datenübertragungsleitung gewährleistet werden kann. Im mittleren Bildteil von Figur 3 ist angedeutet, dass diese "moderne Situation" eine schon recht alte Vorläuferin hat: Es handelt sich um die Situation der Verbindungsaufnahme im Funkverkehr, wo ebenfalls der Verbindungspartner nicht sichtbar ist und wo ebenfalls nur auf der Basis übermittelter Informationen zu entscheiden ist, ob es sich beim Funkpartner um die vermeintliche Gegenstation oder allenfalls um den Feind handelt. Die Sache ist sogar noch komplizierter und schwieriger als bei der Hackersituation, weil es sich hier um eine symmetrische Unsicherheitssituation handelt derart, dass beide Seiten in diesem Kommunikationsprozess von der jeweilig anderen Seite nicht wissen, ob sie mit den Zugriffsrechten versehen sei oder diese erschleiche oder erzwinge. Zur Entschärfung dieser symmetrischen Unsicherheitssituation ist von altersher ein Sicherungsmittel erdacht worden, das auch heute noch als recht raffiniert angesehen werden darf: Die "Funkerkennung". Im untern Teil von Figur 3 ist das Prozedere an einem Beispiel kurz beschrieben: Beide Partner verfügen je über eine gleiche, geheime Liste mit vielen Zeilen sechsstelliger Worte, die sogenannte "Funkerkennungstabelle" (Fig. 4).

Das Verfahren beruht darauf, dass jede Zeile nur einmal verwendet werden darf und nach Verwendung zu streichen ist. Nehmen wir an, eine solche, bisher nicht verwendete Zeile sei jene vom unteren Teil in Figur 3. Dann übermittelt in einem ersten Schritt der eine Funker dem anderen die erste Zweiergruppe, dieser antwortet mit der zweiten Zweiergruppe der Zeile und in einem dritten Schritt repliziert wieder der erste Funker mit der dritten Zweiergruppe derselben Zeile. Man erkennt unschwer, wie sich sukzessive die Wahrscheinlichkeit reduziert, dass eine Zeile bzw. ein Zeilenteil zufällig stimmt, auch wenn etwa ein unbefugter Dritter die Funkerkennungstabelle nicht zur Hand hätte.

Diese Art der Authentifikation gehört heute noch zu den perfektesten, sofern man von einer korrekten Handhabung ausgehen kann. Das ist freilich in der modernen Hacker-Szene kaum mehr der Fall, denn es wäre schwer vorstellbar, dass jeder der vielen berechtigten Benutzer eines Rechenzentrums mit einer Erkennungstabelle versehen wäre, die absolut geheim zu bleiben hat. Zudem müsste man die entsprechenden Geheimhaltungsvorschriften auch für das Operating des Rechenzentrums voraussetzen, was aus heutiger Sicht, mindestens im nichtmilitärischen Bereich, als nicht gegeben betrachtet werden sollte.

CHEF UEM D V E R T R A U L I C H KP
********************** GUELTIG AB:

FUNKERKENNUNGSTABELLE FUER NR SEITE 1/2

16	17	18	19
AAMNQG ABNHJV ACQZCC	ADLKFZ AECIVO AFZBTV	AGPZDO AHJZTP AIZBGJ	AJHGKN AKVVSU ALVXGX
HABIHQ B8YVMK BCUSNO	BD*3CG 9LHAG1 BFU77M	BGAXHD BHEX2L BIOXAH	BJFX1T JAKKSD JLR4DB
CALE6E CBHCFQ CCXF2C	CDIFGF C2GSSD CFH6I5	CGJATF CHI52C CIFCDG	CJYG1G LAKBJL CLKE5L
DABLZ4 DBJJKB DCHMCK	DDHZMH DEYC93 DFWW3H	DGK3K9 DHRB4B DITKZ1	DJNNVN DKVJUD DLNUZC
EASXJE EBLON1 ECUT1D	EDQ1JZ EENPOB EFAEJ7	EGMFEK EHC9WZ EISTV1	EJUKV1 ZKGSIU ELLNGK
FAGP1Q FBD3GO FCY1XX	FDJ5KW FEMTCU FFWUTA	FGLSZF FHKEFI FINUXH	FJFG1G FKIAYU FLSXVJ
GALQUI GBOHCN GCCVKS	GDEVPH GEVMBL GFVPHR	GGHYKK GHSUGG GIGHYJ	GJYEAD GKZYYB GLUFTC
HAUMPT HBVQYL HCST9M	HDKABK HENJHD HFAKNG	HGYQJ7 HHOKZJ HIUPVF	HJGTRY HKGLVP HLKBDX
IAF4D6 I8Z3HP ICCANY	IGU27C IEPBEY IFFUMC	IGK55J INGUQZ IIUMK*	IJTURP IKFVWW ILTVC2
JAXKVZ JESBP5 JCCK9X	JEN2R7 JEASWC JFU3PF	JGE4MX JHA9CK JIHGXP	JJWKAN JABU77 JLK2AU

21	22	23	24
KAWJKV KBWYCE KCBOAH	KDUMFU KEVQG5 KFXJGX	KGENJI KHXXAD KIYTE9	KJXBIU KKY2KM KLTLH2
LAE623 LBD6D6 LCDNA6	LDTT3Z LEGYEC LFGVVU	LGNAZA LHM57U LISKFV	LJHSYN LKIPPA LLS4J1
MAIJ29 MBLMWQ MCWYAZ	MDLUVX MEHTOI MFYFPG	MGJHMK MHAZWR MIU2FG	MJYK9* MKA3ZA MLIIGO
NAZMMJ NBVPGP NCLM9O	NDXSU2 NEILBX NFZFRO	NGETNI NHRDMQ NISVT1	NJRAJN NKJAYN NLKKPI
OAPAIB OBECON OCEVU4	ODJ4BW OEFUQY OFWBPH	OGUB6J OHV2OO OIY3U*	OJFVMV OKLZ1J OLEXNA
PAUGCY PBFZLH PCFFLJ	PDP9H9 PEGW3V PFQHAE	PGPM8N PHF8X3 PIUYNA	PJA4E3 PARTIP PLWG1S
QASUMV QBP2KL QCCGJT	QDL4RD QEFO5Y QFZVNY	QGYXM2 QHM3MF QIB5LL	QJNKYA QKVYCP QLZ9ZA
RAP2XD RBX3Q4 RCFTMI	RDU3VQ RESXNN RFWJUO	RGMUB2 RHOU2Y RIKCIY	RJMLJL RKILJA RLAMZO
SASFQU SBD7BB SCCCSD	SDJX3A SZEG4Q SFPSFR	SGZK1U SHWUBJ SIVVAS	SJNIFR SKARUK SLSNAG
TAPYQO TBKIEN TCLVXS	TDYC9S TENTPV TFOBOW	TGWDCQ THVN1T TIUSSJ	TJLIAS IKYE*N TLJ0*O

25	27	26	29
UAZ03V UBYA3C UCNMO5	UDKBLM UEZZG8 UFSISS	UGHFIJ UHNXK1 UIFULA	UJKA2Z UKDIFL ULWISH
VAQ383 VBVZRO VCG9CH	VDH94I VES2NE VFHF5O	VGPAPC VHASXM VIRSGZ	VJDXRL VKMUZJ VLLQ4U
WATMG3 WBPNOU WCSNIY	WDUAAT WEIBIY WFHVST	WGPYZU WHTIFP WIDURV	WJY*L3 WKUUY5 WLUPYV
XAZR26 XBSWAB XCW5TM	XDA5DX XEM5UQ XFUUG3	XGKDUP XHF5GS XIVA1C	XJE5OL XK5KL9 XLFM*U
YAA3GY YBKJWI YCSY4P	YDF64E YENVE3 YFX495	YGWP6X YHMD5O YISXL4	YJZIWT YK*PUR YL6*JK
ZATUJP ZBHREI ZCPNPU	ZDHYLK ZEFGMW ZFS2H8	ZGCPYF ZHEGVS ZIT7QZ	ZJLUFN ZKXYYI ZLKTXP
1AUQOT 1BZBI6 1CHTIT	1DDUQM 1ENN7F 1FJX41	1GJAFG 1HJFDX 1IJSUZ	1JYUQR 1KTLCS 1LNLW4
2AYS2O 2BGJ8N 2CFZWL	2DX3TF 2EBBFQ 2FAMKV	2GXHK3 2HLYPD 2IBSSN	2JRKSC 2KHHIV 2LN171
3ARIGK 3BAUQD 3CHA4G	3DLM21 3ED1BQ 3FMUPF	3GD5EL 3HHPI3 3IUWJ*	3JOLPZ 3KW7FL 3LWU2H
4AWSAI 4BSHIC 4CBKCN	4DUD2Z 4ELJLS 4FC?AN	4GPHXP 4HCFC1 4IJ1EO	4JJU7L 4KXFV1 4LAZBH

Fig. 4 Beispiel einer Funkerkennungstabelle

2. SYSTEMATIK VON AUTHENTIFIKATIONSMOEGLICHKEITEN

Es lohnt sich, sich einmal grundsätzlich zu überlegen, welche Verfahren überhaupt zur Authentifikation, möglichst zur automatischen oder halbautomatischen Authentifikation, zur Verfügung stehen. Bei der entsprechenden Ideensuche berücksichtigt man zweckmässigerweise auch die zahlreichen Verfahren, die bisher schon ausgedacht und eingesetzt worden sind, ohne dass man sich bewusst wäre, dass es sich bei diesen Verfahren um solche der Authentifikation handelt. Nachfolgend wird versucht, eine gewisse Systematik in dieses Gebiet hineinzubringen.

2.1. INDIVIDUEN UND OBJEKTE ALS BERECHTIGTE

Sowohl ein Individuum wie ein Objekt (z.B. ein Ausweis) können Träger einer Berechtigung sein, dementsprechend ist zu unterscheiden zwischen der Individual-Authentifikation und der Objekt-Authentifikation. In Figur 5 sind die Grundfragen dieser Authentifikationsarten schematisch zusammengestellt.

Die Authentifikationsfragen, die dabei gestellt werden, können generell auch als Fragen über die "Echtheit" aufgefasst werden. Während die "Echtheit eines Objektes" ein wohlverstandener Begriff ist, wäre die "Echtheit eines Individuums" ein eher ungewöhnliches Attribut, in sachlicher Hinsicht ist dagegen aber kaum etwas einzuwenden, es mag ohne weiteres einsichtig und verständlich sein, was damit gemeint ist.

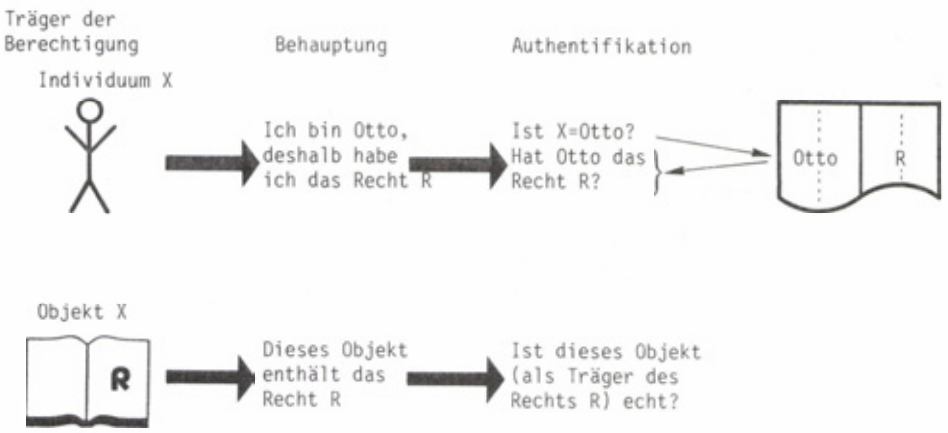


Fig. 5 Grundfragen zur Authentifikation

2.2. ECHTHEITSPRUEFUNG VON OBJEKTEN

Es lassen sich drei verschiedene Konzepte unterscheiden, die den Echtheitsprüfungen von Objekten zugrundeliegen, sie sind in Figur 6 zusammengestellt.

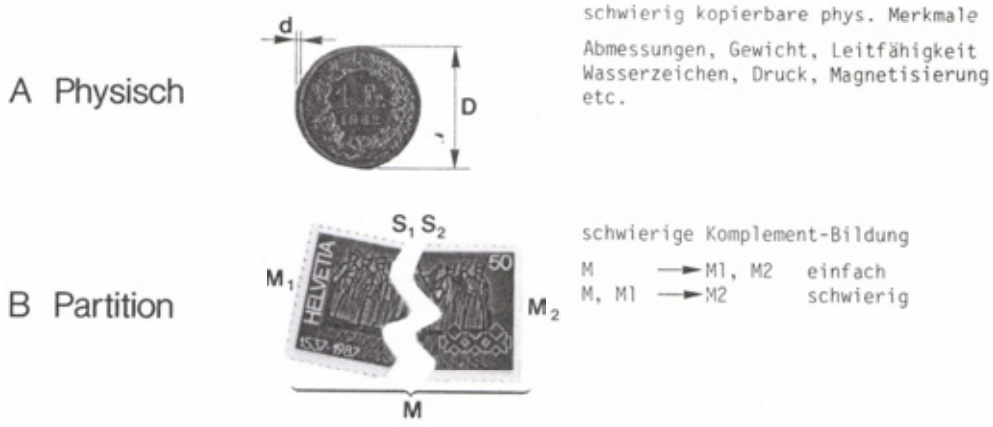


Fig. 6 Echtheit von Objekten

Da jedermann über die Kategorien A (Physisch) und C (Selektion) genügend eigene Beispiele aus der Praxis kennt, erübrigt sich wohl das weitere Eingehen darauf. Interessanter, weil erstens weniger bekannt und zweitens besonders wirkungsvoll, ist jedoch die Kategorie B (Partition): Man kennt dieses Verfahren etwa aus Kriminalgeschichten, wo eine Banknote entzweigerissen wird und wo die spätere Authentifikation darauf abstützt, ob ein vorgelegter Banknotenteil genau zu seinem Komplement passe. Das Verfahren beruht, wie in der Mitte von Figur 6 dargestellt, auf der Schwierigkeit der Komplementbildung oder allgemeiner (wie sich später noch zeigen wird) auf der Schwierigkeit, gewisse Funktionen umzukehren. So ist es beim Beispiel der Banknote (oder der Briefmarke in Figur 6) sehr einfach, eine Note in zwei Teile zu zerreissen, jedoch sehr schwierig, das fehlende Stück zu einem Banknotenabschnitt zu erzeugen, selbst wenn man das zusammengesetzte Resultat, nämlich die ganze Banknote, sehr genau kennt. Ein anderes hübsches Beispiel aus der Geschichte mittelalterlicher Authentifikation zeigt Figur 7: Es war zu jener Zeit, als die Marksteine einziges gültiges Merkmal der Landbesitzgrenzen waren, als es noch keine Grundbuchblätter gab, in denen diese Rechtskraft abgebildet werden konnte.

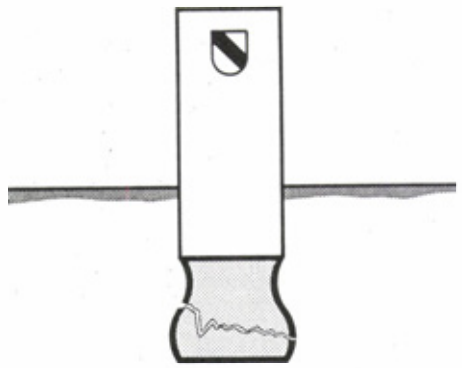


Fig. 7 Historisches "Authentifikationsverfahren"

Wenn jemand, was vorgekommen sein soll, Marksteine nächtlich versetzte, konnte er seinen Landbesitz vergrössern, falls seinem Nachbarn der Beweis nicht gelang, dass der Markstein versetzt worden war. Deshalb plazierte man unter kritische Marksteine Tonkrüge, die bei der unbefugten Versetzung eines Marksteins entzweisprangen. Aus diesem alten Verfahren lassen sich, übertragen auf die heutigen elektronischen Methoden, aktuelle Authentifikationsverfahren ableiten.

2.3. "ECHTHEITSPRUEFUNG" VON INDIVIDUEN

Die Begriffe "Authentifikation" und "Identifikation" kommen sich hier sehr nahe und überlappen sich in ihrer Bedeutung teilweise. Wir haben es hier mit vier Konzepten zu tun, wie sie in Figur 8 zusammengestellt sind.

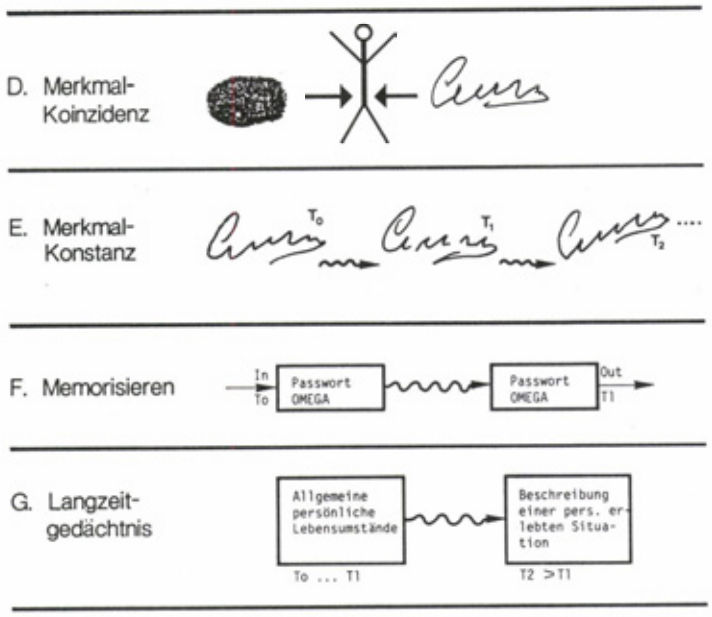


Fig. 8 "Echtheit" von Individuen

Bei der Merkmalkoinzidenz geht es darum, zwei verschiedene, individualgebundene Merkmale zu vergleichen, wie etwa Fingerabdruck und Unterschrift, Passbild und Gesicht usw. Die Merkmalkonstanz geht von der Individualeigenschaft aus, dass wichtige, individualgebundene Merkmale über der Zeit mehr oder weniger konstant bleiben, wie z.B. die Unterschrift. Dies ist offenbar darauf zurückzuführen, dass beispielsweise motorische Eigenschaften des Menschen an seine Individualität gebunden und deshalb unverlierbar sind. Das Memorisieren ist in bezug auf die Individualgebundenheit damit verwandt, jedoch werden hier nicht angeborene Eigenschaften, sondern gelernte und im Gehirn gespeicherte Merkmale verwendet, wie etwa ein Passwort. Die Verwendung des Langzeitgedächtnisses basiert zwar auch auf der Speicherfähigkeit des Gehirns, jedoch nicht auf dem bewussten Erlernen, sondern auf dem unbewussten Speichern von Erlebnissen und Eindrücken. Auch Militärfunker kennen dieses Verfahren und wenden es zuweilen an, wenn z.B. der Funkpartner zwecks Authentifikation oder Identifikation nach irgendeinem kürzlichen Erlebnis gefragt wird, das ein Dritter, Unbefugter nicht oder kaum kennen kann.

Das Checkwesen beruht wesentlich auf Individual-Authentifikationen, in der Regel und bis heute auf der Basis von individuellen Unterschriften. Die Beispiele von Fig.9,10,11 zeigen drei bekannte Verfahren für Kreditkarten (hier American Express, Eurochecks und Travellerchecks), wobei die Verfahren in der gleichen Reihenfolge besser und sicherer, damit auch komplizierter werden.

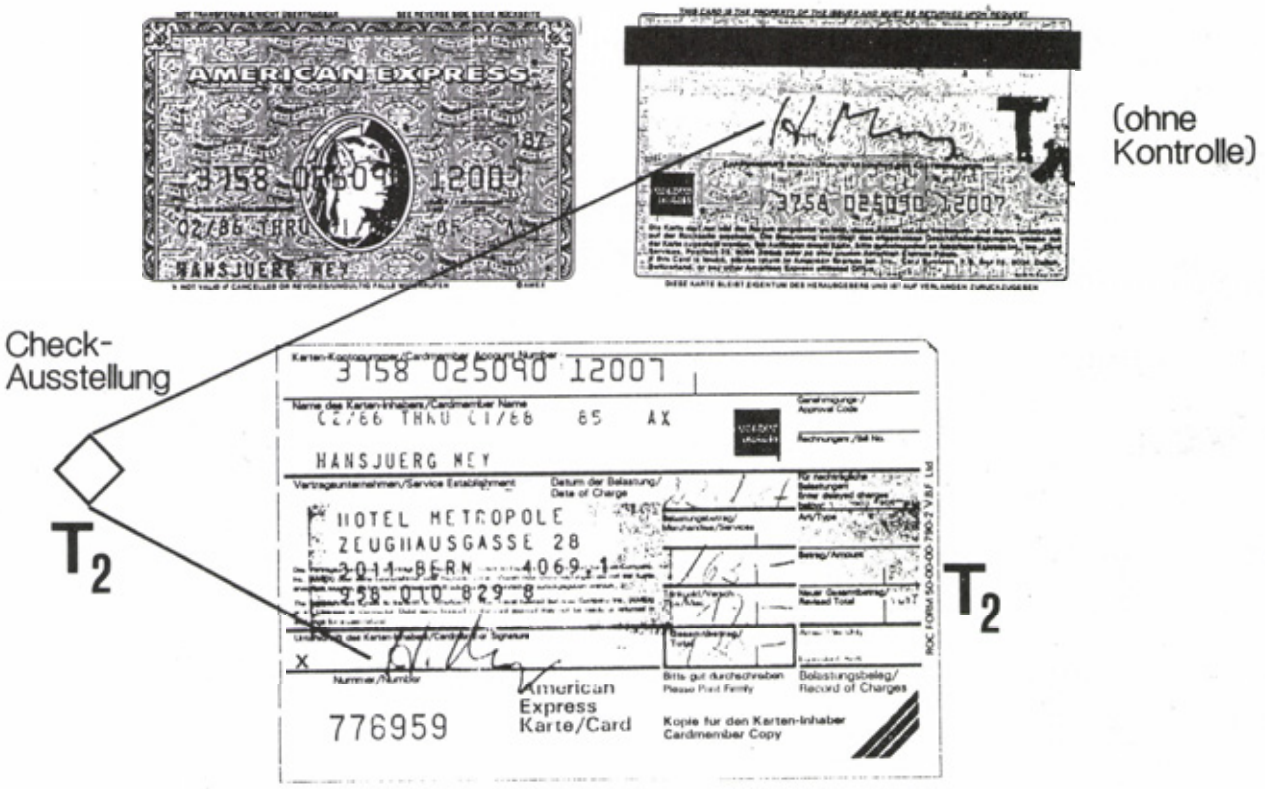


Fig. 9 Ueberprüfung beim American Express Check

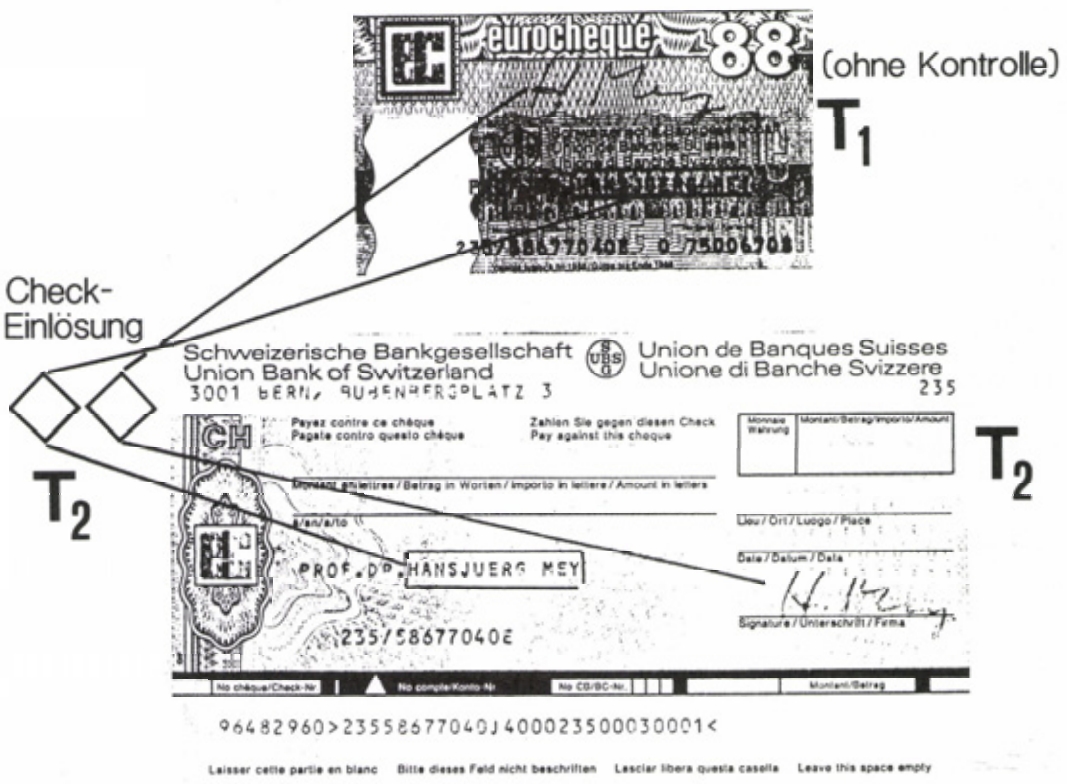


Fig. 10 Kontrollen beim Eurocheque

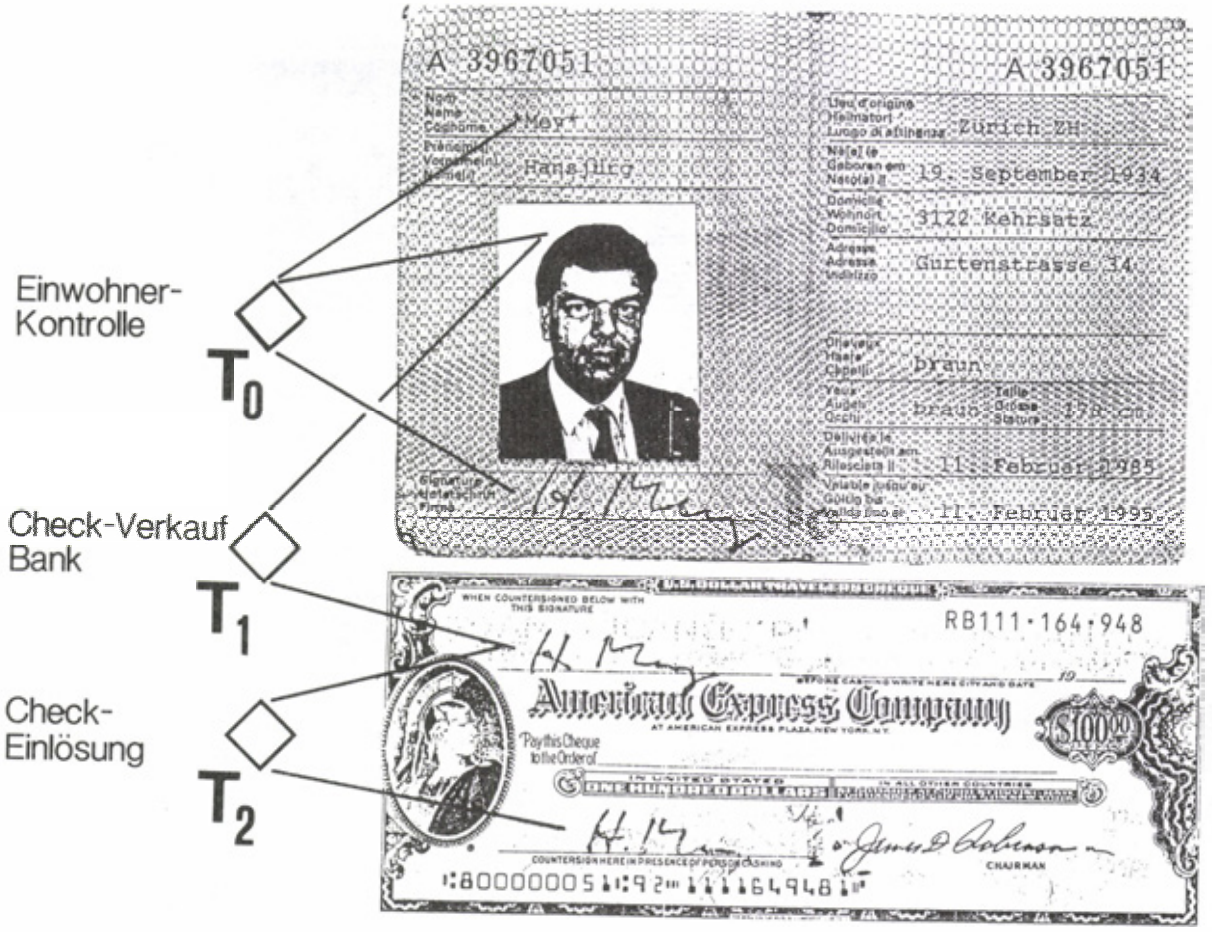


Fig. 11 Ueberprüfung beim "Traveller Check"

So erstaunt es etwa, wie unvollständig der Authentifikationsschutz bei Kreditkarten ist, wo nicht einmal die Uebereinstimmung von Name und Unterschrift des Berechtigten überprüft werden kann (dazu ein interessantes Detail: Das "Restrisiko", das mit diesem an sich ungenügenden Authentifikationsverfahren übrigbleibt, wird mit Versicherungs- und Strafmassnahmen abgedeckt).

2.4. GRUNDPROBLEMATIK DER INDIVIDUALAUTHENTIFIKATION

Anhand von Figur 12 wird in einem Uebersichtsschema darzustellen versucht, wie die verschiedenen Verfahren der Individualauthentifikation funktionieren. Die bisher beschriebenen Authentifikationsverfahren finden sich hier wieder, wobei hier besonders zu beachten ist, dass mit Ausnahme zweier direkter Methoden ("Brandmal" und unpersönliche Objekte wie Geld, Schlüssel usw.) alle Verfahren auf einem Vergleich zwischen einem Athentifikationsmerkmal (z.B. Unterschrift oder Magnetspur auf einer Ausweiskarte) und einer an das Individuum gebundenen Information (z.B. die echte Handschrift bzw. ein memorisierter persönlicher Code) beruhen. Alle rein technischen Authentifikationsverfahren, bei denen ja der Träger der Berechtigung nicht persönlich anwesend ist, müssen auf diese Vergleichsmöglichkeit verzichten, und genau darin liegt die eigentliche Grundproblematik der technischen Authentifikation. Es ist deshalb mindestens ungewiss, ob eine sichere Individual-Authentifikation unter den gegebenen Bedingungen eines "physisch nicht präsenten Individuums" überhaupt möglich ist.

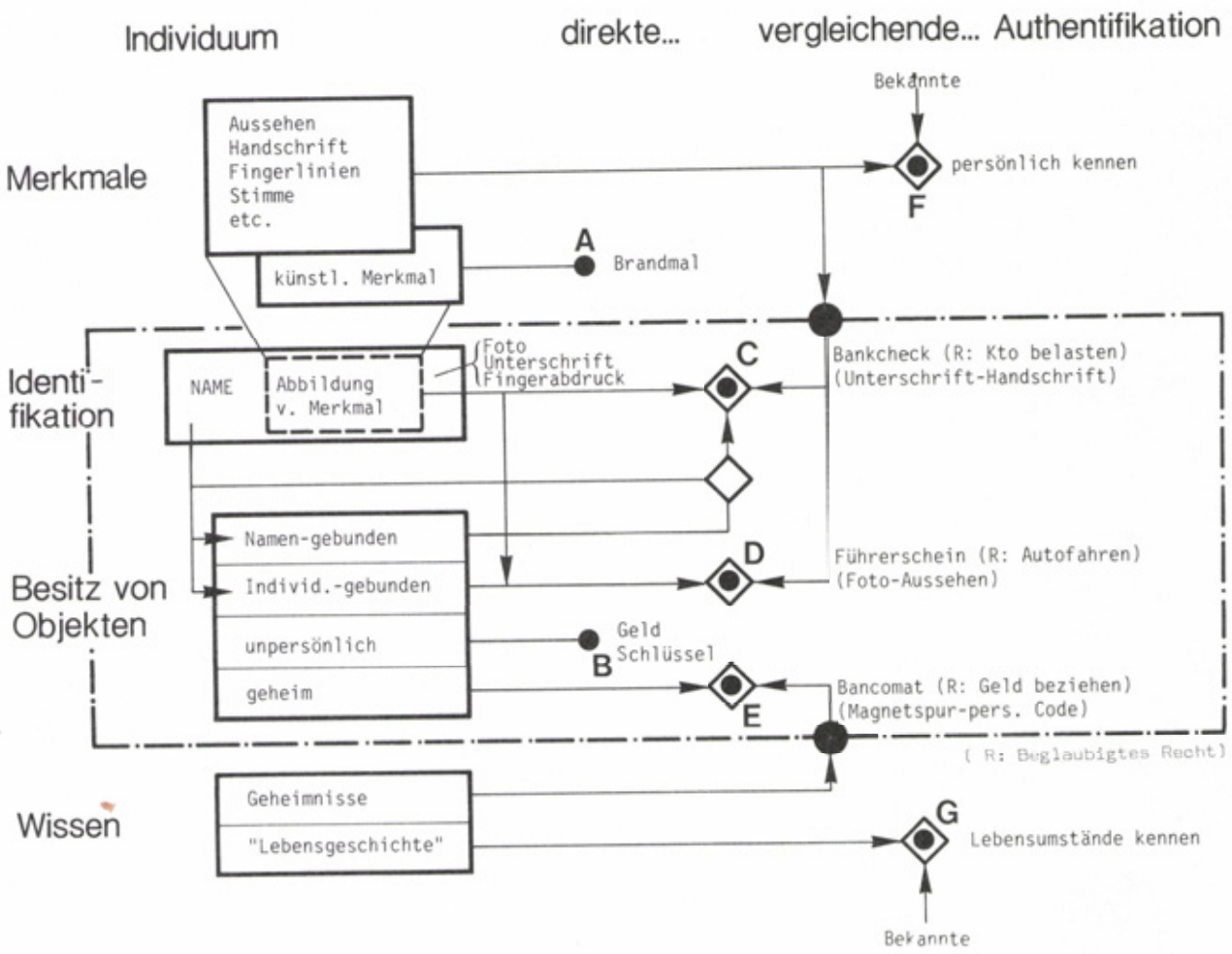


Fig. 12 Uebersicht über Authentifikationsverfahren

3. PUBLIC KEY-SYSTEME ALS AUTHENTIFIKATIONS-BASIS

Die Idee der Public Keys hat bekanntlich vor ungefähr zehn Jahren die Chiffriertheorie und -praxis revolutioniert. Von allem Anfang an war von den Erfindern des Public Keys-Systems auch auf die Möglichkeit hingewiesen worden, diese Verfahren der Authentifikation nutzbar zu machen.

3.1. PRINZIP DER PUBLIC KEY-METHODE

Da diese Methode schon oft dargestellt worden ist, soll anhand von Figur 13 und Figur 14 nur noch einmal kurz das Wesentliche zusammengestellt werden: Jeder Teilnehmer hat einen Schlüssel aus zwei Komponenten, von denen er die eine in einer allgemeine zugänglichen Datenbank veröffentlicht, während er die geheime Komponente unter Verschluss behält. Diese beiden Komponenten sind reziproke Funktionen, deren sukzessive Anwendung auf eine Variable diese in sich selbst abbilden.

In Figur 14 sind die Bedingungen, die an die Funktionenpaare gestellt werden, aufgelistet, wobei die wichtigste dahingehend lautet, dass die Umkehrungen schwierig zu berechnen sind, obwohl man weiss, dass ihr Produkt die Einheitsabbildung ergibt. Von dieser Eigenschaft leitet sich der Begriff "Einwegfunktionen" ab.

Jeder Teilnehmer i

- "würfelt" ein e_i und berechnet daraus d_i (oder umgekehrt)
- veröffentlicht e_i in einer allgemein zugänglichen Datenbank
- hält d_i geheim

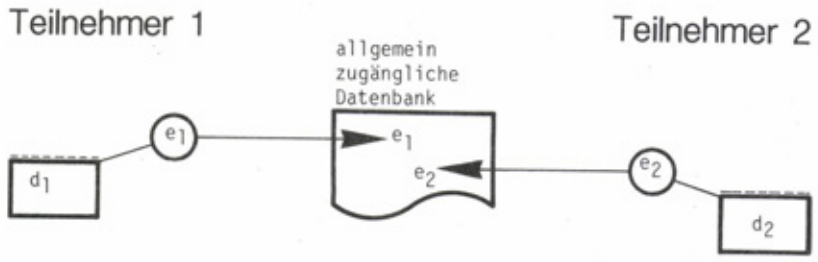


Fig. 13 Public-Key-System (1)

Teilnehmer	T_i
Chiffrierfunktion	e_i
Dechiffrierfunktion	d_i

e_i wird veröffentlicht (public key)

Bedingungen für e_i und d_i:

1. Leicht zu bestimmende Paare e_i, d_i, so dass

$$e_i\,(d_i\,(x)) = x \quad \text{und} \quad d_i\,(e_i\,(x)) = x$$

2. Leicht zu bestimmende Funktionswerte

$$y = e_i\,(x) \quad \text{und} \quad y = d_i\,(x)$$

3. Schwer zu bestimmende Umkehrungen

$$x = e_i^{-1}\,(y) \quad \text{und} \quad x = d_i^{-1}\,(y)$$

e_i, d_i sind reziproke Paare von "Einwegfunktionen"

Fig. 14 Public-Key-System (2)

In Figur 15 ist dargestellt, wie dieser Public Key zur Authentifikation bzw. zur Identifikation verwendet werden kann.

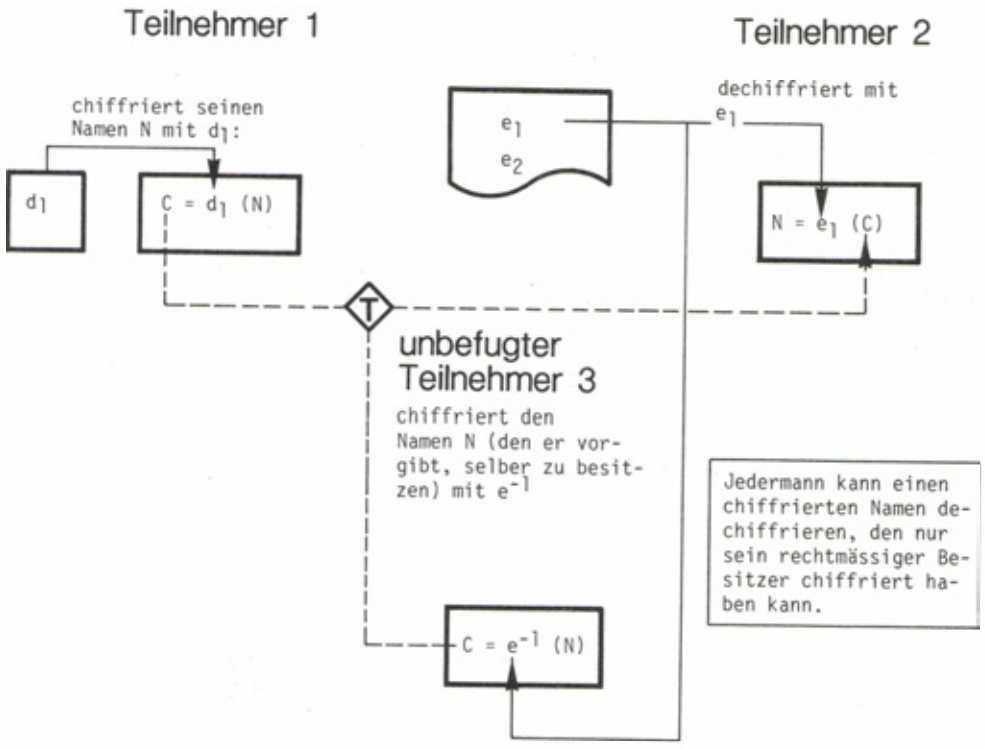


Fig. 15 Public-Key-System

Im wesentlichen geht es darum, dass ein bekannter Name (z.B. der Name des sich identifizierenden Teilnehmers) mit dessen geheimer Schlüsselfunktion chiffriert wird, wogegen der überprüfende Teilnehmer die Dechiffrierung mittels des veröffentlichten Schlüsselteils vornimmt. Der unbefugte dritte Teilnehmer müsste diese veröffentlichte Teilfunktion invertieren, was gemäss Voraussetzung aber nur mit sehr grossem Aufwand möglich ist (mathematisch gesprochen bedeutet dies, dass der Umkehralgorithmus von einer sehr grossen Komplexitätsordnung ist).

In Figur 16 sind ein derartiges reziprokes Funktionenpaar und seine Herleitung skizziert. Es handelt sich dabei um das berühmte RSA-System (Rivest, Shamir und Adleman).

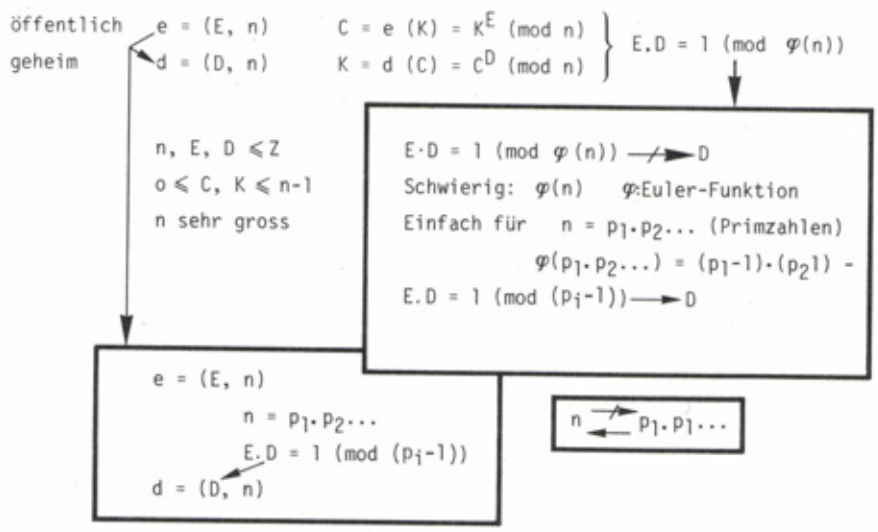


Fig. 16 RSA-Public Key-System von Rivest, Shamir, Adleman (1978)

Beide Teilfunktionen entsprechen einer Potenzierung mit einer ganzen Zahl modulo einer sehr grossen ganzen Zahl. Die Sicherheit des Verfahrens ist darin begründet, dass der eine dieser Exponenten aus dem anderen nur sehr schwer gewonnen werden kann, wenn man keine Aufschlüsse über die grosse Modulo-Zahl n hat. Dieses n ist nämlich das Produkt zweier grosser Primzahlen, die wohl dem geheimnistragenden Teilnehmer, nicht jedoch der Oeffentlichkeit bekannt sind. Deshalb beruht das Verfahren letztlich auf der Einfachheit, aus zwei grossen Primzahlen ihr Produkt zu bestimmen und aus der Schwierigkeit, dieses Produkt in seine beiden Primfaktoren zu zerlegen. Bis heute ist kein Algorithmus bekannt, der diese Zerlegung mit vernünftigem Rechenaufwand durchzuführen erlauben würde; es ist allerdings auch kein Beweis bekannt, wonach es keinen solchen Zerlegungsalgorithmus kleiner Komplexität gibt.

Man ist somit auch bei diesem Verfahren bei jenem Punkt angelangt, an dem man bisher bei jedem Chiffrierverfahren angelangt ist: nämlich beim Mangel eines Beweises einer unter Komplexitätsschranke, der Voraussetzung dafür wäre, dass die Sicherheit des Verfahrens mathematisch bewiesen werden könnte. Es ist eigenartig feststellen zu müssen, dass es bisher für kein einziges Chiffrierverfahren gelungen ist, einen derartigen Beweis zu liefern; es ist aus heutiger Sicht deshalb sogar fraglich, ob es jemals gelingen werde, das Problem der beweisbaren Chiffriersicherheit im mathematischen Sinn zu lösen.

3.2. ANWENDUNGSBEISPIEL FUER DIE ATOMTESTUEBERPRUEFUNG

Vor einigen Jahren ist ein interessanter Vorschlag gemacht worden, wie unterirdische Kernexplosionen vor Ort festzustellen wären, ohne dass sich jemand von der Gegenpartei dort aufhalten müsste. Dieser Vorschlag basiert auf dem Public Key-System bzw. auf einem Paar von Einwegfunktionen, wie das in Figur 17 sizziert ist.

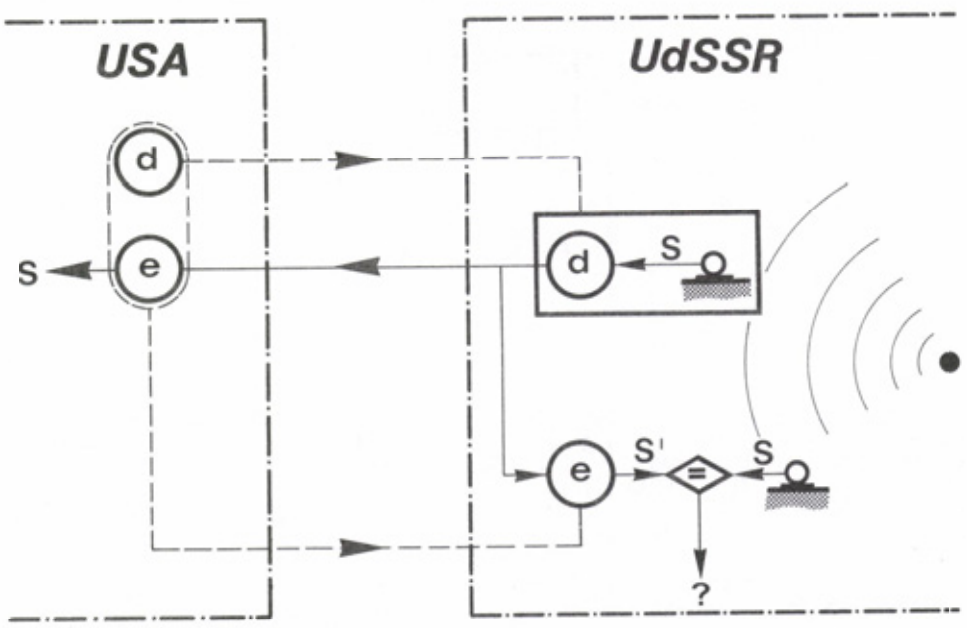


Fig. 17 Gegenseitige Atomtestüberprüfung

Dabei wird angenommen, dass die Amerikaner zuverlässig darüber informiert werden möchten, wenn in der UdSSR eine Kernladung unterirdisch gezündet wird. Mit einer einfachen Fernmessleitung zwischen einem in der UdSSR installierten seismischen Sensor und einer Empfangsstation in den USA ist es nicht getan, weil damit die folgenden Vertrauensmanki nicht behoben werden können: Die Amerikaner argwöhnen, die Russen würden den Sensor abstellen vor einer Kernexplosion, die Russen argwöhnen, die Amerikaner würden über dieses System allgemeine elektronische Aufklärung betreiben. Hier helfen nun die Einwegfunktionen wie folgt: In der UdSSR wird ein seismischer Detektor aufgestellt und dessen Signal über den geheimen Funktionsteil chiffriert und in dieser Form nach den Vereinigten Staaten übermittelt. Sensor und Chiffrierfunktion befinden sich in einem abgeriegelten Gebäude, die Chiffrierfunktion würde zerstört, wenn jemand unbefugterweise in das Gebäude eindringen würde, das von den Amerikanern aufgestellt worden ist. In der Nähe plazieren die Russen ihrerseits einen seismischen Detektor, dessen Signal sie mit demjenigen der Amerikaner vergleichen, das sie aus dem übermittelten Signal mittels Transformation über den veröffentlichten Funktionsteil gewinnen. Stimmen die beiden Signale nicht überein, so würden die Amerikaner andere Daten als jene des seismischen Detektors übertragen, also z.B. verbotenerweise elektronische Aufklärungssignale. Die Amerikaner ihrerseits transformieren das empfangene Signal ebenfalls mit dem veröffentlichten Funktionsteil und erhalten so das relevante Signal des seismischen Detektors.

4. AUTHENTIFIKATION GEGENUEBER RECHENZENTREN

Hier geht es um das "Hacker-Problem", wie es im oberen Bildteil von Figur 3 dargestellt worden ist. Verallgemeinert geht es dabei nicht nur um den Schutz gegenüber Hackern, sondern ebenso z.B. um den Schutz von Kontokarten-Inhabern, die sichergehen möchten, dass ihr Konto nicht durch einen unbefugten Dritten über ein Kundenterminal der Bank belastet wird.

4.1. AUTHENTIFIKATION MIT UNVERSCHLUESSELTEM PASSWORT

Figur 18 zeigt das zugehörige Verbindungs- und Speicherschema, wobei für das letztere (wie auch für die folgenden Beispiele) davon ausgegangen wird, dass im Rechenzentrum eine Authentifikationsdatei angelegt ist mit einem Datensatz pro Teilnehmer bzw. pro Teilnehmeridentifikation. Falls in einem derartigen Datensatz neben der Identifikationsnummer das Passwort abgespeichert ist, muss beim aktuellen Zugriff lediglich das momentan gesendete Passwort mit dem in der Authentifikationsdatei gespeicherten Passwort verglichen werden, bei Uebereinstimmung wird der Zugriff freigegeben. Man stellt hier zwei gefährdete Komponenten fest: Zum einen ist es der Uebertragungsweg, auf welchem das Passwort unverschlüsselt übertragen wird, zum andern die Authentifikationsdatei, zu der die Operators des Rechenzentrums zugreifen können.

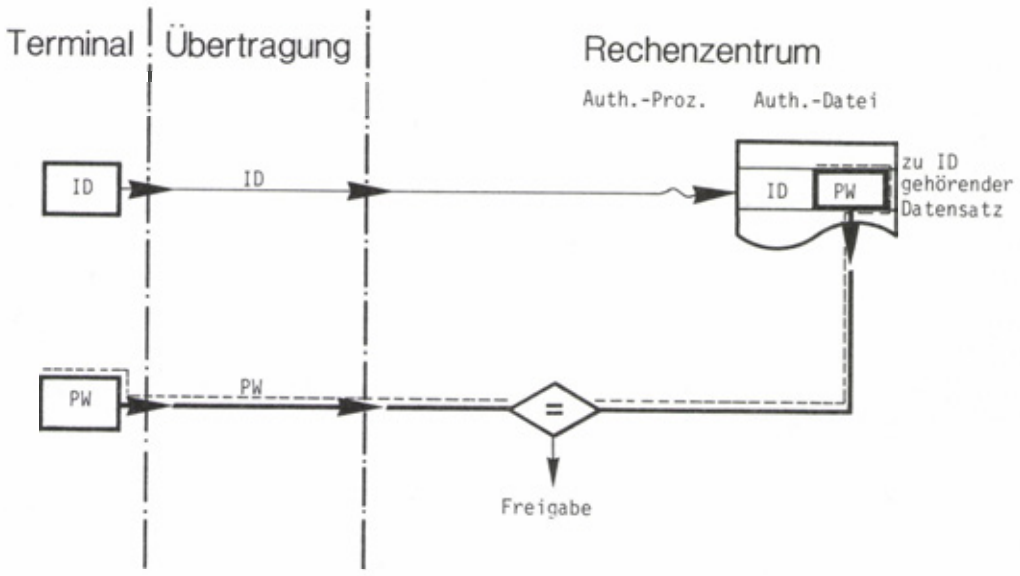


Fig. 18 Authentifikation mit unverschlüsseltem Passwort

4.2. AUTHENTIFIKATION MIT VERSCHLUESSELTEM PASSWORT

Ein besseres Verfahren zeigt Figur 19: Hier wird das Passwort sowohl im Datensatz der Authentifikationsdatei wie bei seiner aktuellen Verwendung vor einer Terminalsession "verschlüsselt", was konkret dessen Transformation mittels einer nur schwer umkehrbaren Funktion bedeutet.

Man erkennt hier unschwer die Funktionsweise der Einwegfunktion, wie sie anhand des Public Key-Verfahrens geschildert worden ist. Das schwache Glied in der Authentifikationskette ist hier lediglich noch die ungesicherte Uebertragungsstrecke, wogegen die Sicherung gegenüber unbefugten Operators-Zugriffen sehr gut ist (sofern die Nichtumkehrbarkeit der Funktion f als gewährleistet angenommen wird). Selbstverständlich sind gewisse Sicherheitsvorkehren zur Isolation der Freigabe-Vorrichtung notwendig, um zu verhindern, dass Rechenzentrums-Personal das Freigabesignal direkt nachbilden kann. Dieses Verfahren wird derzeit als gut und sicher qualifiziert, weshalb es in der Praxis breite Anwendung gefunden hat. Die Schwäche der nicht gesicherten Passwortübertragung bleibt natürlich bestehen, sie ist allerdings zu relativieren: Ein unbefugter Dritter müsste Zugriff haben auf die Uebertragungsstrecke (z.B. auf eine Telefonleitung) und dies erst noch zu jenem Zeitpunkt, da Identifikationscode und Passwort miteinander bzw. nacheinander übertragen werden.

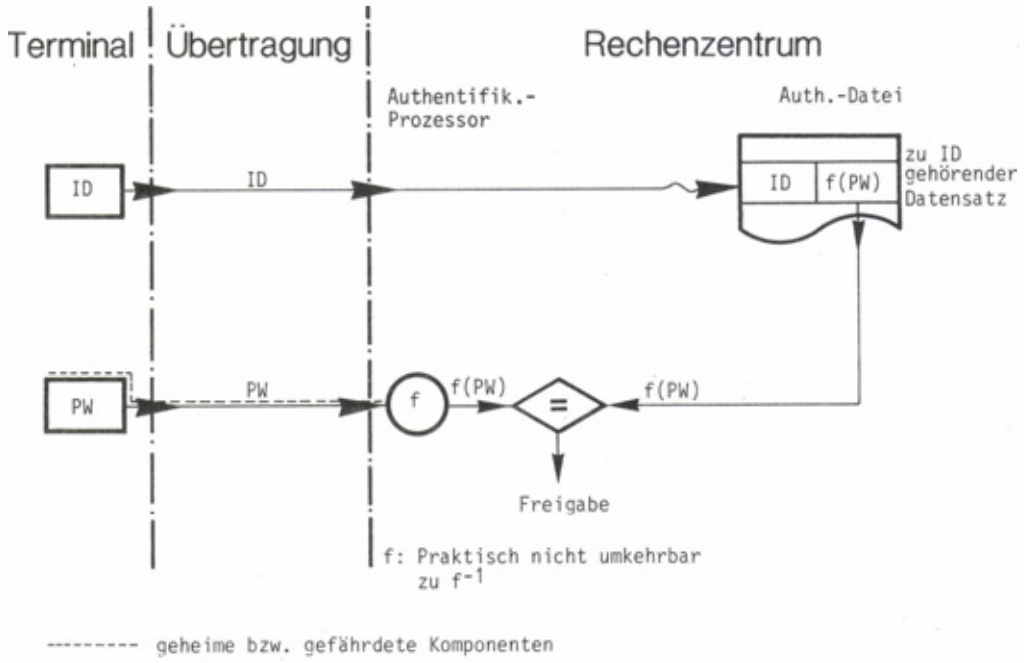


Fig. 19 Authentifikation mit verschlüsseltem Passwort

4.3. AUTHENTIFIKATION MIT PUBLIC KEY

Eine Erweiterung des eben beschriebenen Verfahrens mit chiffriertem Passwort führt zur Anwendung des Public Key-Verfahrens von Figur 20.

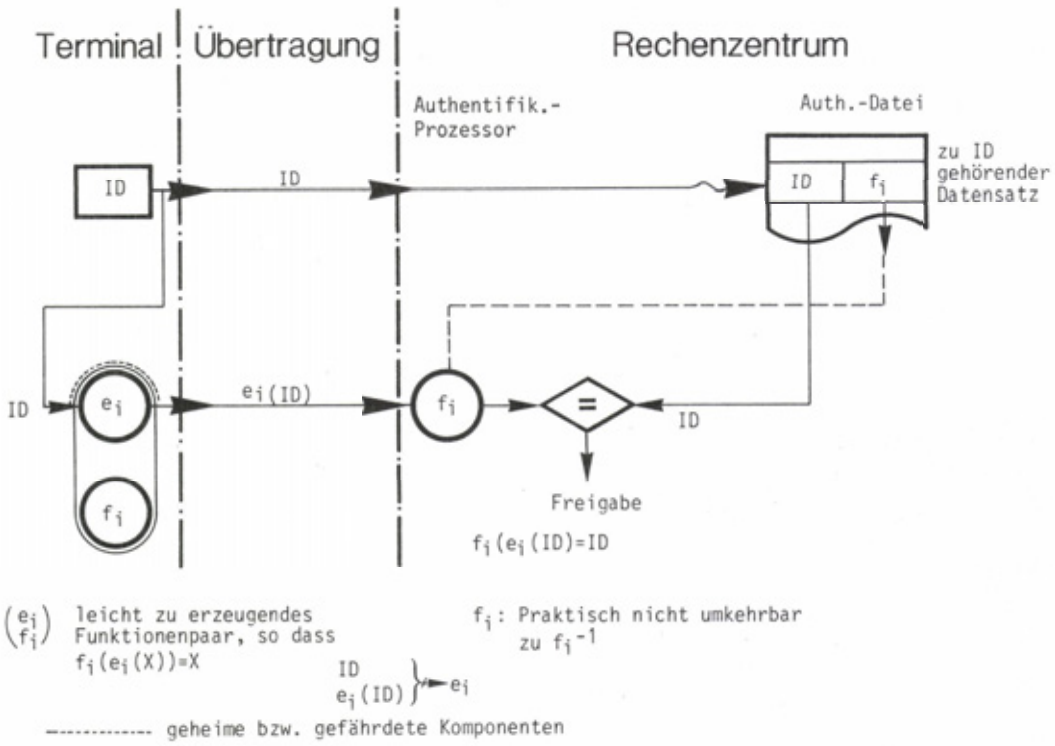
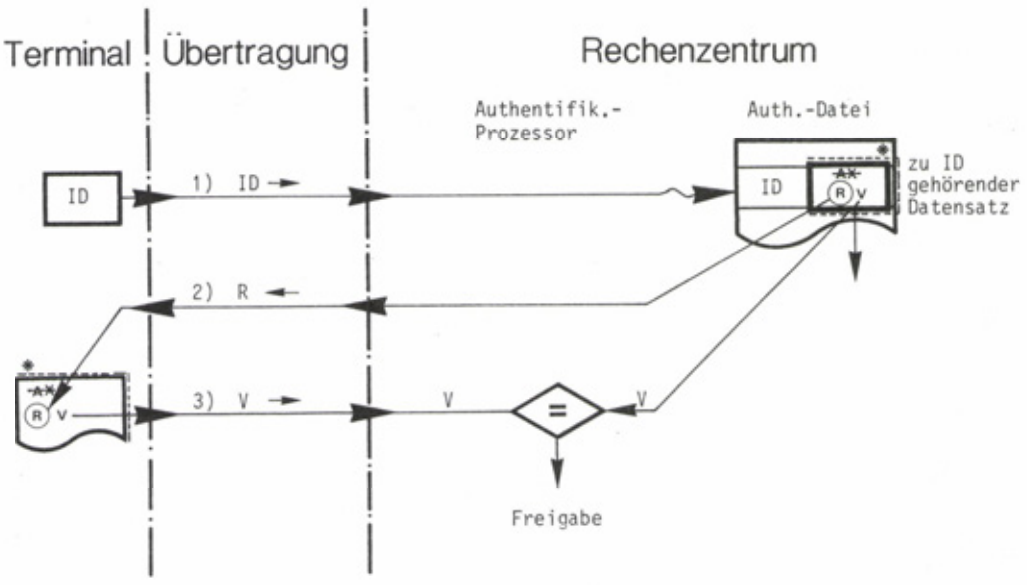


Fig. 20 Authentifikation mit Public Key

Hier wird nicht ein Passwort, sondern jener Funktionsteil im Datensatz der Authentifikationsdatei gespeichert, der im normalen Public Key-Verfahren veröffentlicht wird; damit ist er natürlich nicht geheim und es besteht keine Gefahr des Missbrauchs durch Operators. Chiffriert wird hier mit dem geheimen Funktionsteil, wie das anhand von Figur 15 für die Public Key-Identifikation gezeigt worden ist. Die Sicherheitsverhältnisse liegen gleich wie bei jenen des chiffrierten Passworts von Figur 19, d.h. das Rechenzentrum gehört zwar zum sicheren Bereich, die Uebertragungsstrecke bleibt jedoch nach wie vor ungesichert: Gelänge es einem unbefugten Dritten, zu Beginn einer Terminalsession sowohl den Identifikationscode wie dessen Transformation mittels des geheimen Funktionsteils aufzuzeichnen, so könnte er später mit diesen Daten jederzeit den unrechtmässigen Zugriff erschleichen.

4.4. AUTHENTIFIKATION MIT "FUNKERKENNUNG"

Das Prinzip der Funkerkennung ist bereits anhand von Figur 3 erläutert worden, Figur 21 zeigt nun die Anwendung dieses Verfahrens auf die Authentifikation eines am Rechenzentrum angeschlossenen Terminals. Man erkennt daraus, dass die Sicherheitsverhältnisse gerade umgekehrt liegen im Vergleich zu den beiden vorangegangenen Verfahren von Figur 19 und 20: Hier ist die Uebertragungsstrecke vollständig gesichert, da ein unbefugter Dritter mit dem Informationsaustausch zu Beginn einer Session nichts anfangen kann, selbst wenn er ihn lückenlos aufzuzeichnen in der Lage gewesen ist. Dafür wird aber die Authentifikationsdatei im Rechenzentrum zum ungesicherten Bereich, denn jeder Datensatz, der einem Terminal zugeordnet ist, muss nun über eine "Funkerkennungstabelle" verfügen, die vom Computer so handzuhaben ist, wie das anhand von Figur 3 erläutert worden ist.



..... geheime bzw. gefährdete Komponenten

* Jede Zeile nach Gebrauch löschen

Fig. 21 Authentifikation mit "Funkerkennung"

5. ANMERKUNGEN ZUR SICHERHEIT

Die letzten Authentifikationsbeispiele haben gezeigt, dass es sehr darauf ankommt, welchen Teil des Gesamtsystems von Terminal, Uebertragung und Rechenzentrum man gegen unbefugten Zugriff schützen will oder muss. Offensichtlich unterscheiden sich hier auch die Anforderungen je nach dem, ob der Betrieb ziviler oder militärischer Art ist. So wäre es wahrscheinlich wenig vernünftig, im militärischen Bereich ein Authentifikationsverfahren mit verschlüsseltem Passwort oder mit Public Key nach Figur 19 oder 20 einzurichten, da in beiden Fällen die Uebertragungsstrecken ungesichert sind, die im militärischen Einsatz als besonders verletzlich gelten. Es sei denn, die Uebertragungsstrecke werde an sich schon chiffriert, dann können diese Verfahren als sicherheitsmässig gut beurteilt werden.

Andererseits gibt es verschiedene Gründe, wonach im militärischen Bereich Rechenzentren ohnehin als "klassifiziert" handzuhaben sind, wie etwa Knoten in einem Uebermittlungsnetz, bei dem nur die Uebertragungsstrecken chiffriert sind, währenddem die Knoten selber (aus technischen Gründen) Klarinformationen vermitteln. Unter dieser Annahme wäre die Authentifikation mit "Funkerkennung" nach Figur 21 die adäquate Lösung, da hier die Uebertragungsstrecke schon vom Authentifikationssystem her gesichert ist. Allerdings ergeben sich Probleme mit dem "Schlüssel-Management", da es z.B. im militärischen Einsatz nicht einfach ist, laufend neue Funkerkennungstabellen zu editieren sowie sicher zu verteilen und aufzubewahren.

Schon früher ist darauf hingewiesen worden, dass es bisher nicht gelungen ist, die "Chiffriersicherheit" mathematisch streng zu beweisen, da diese Frage mit dem noch ungelösten Problem eines mathematischen Beweises von unteren Komplexitätsschranken zusammenhängt. Dies gilt grundsätzlich auch für die Authentifikationsverfahren, deren Sicherheitsprobleme aus heutiger Sicht dieselben sind wie für die Chiffrierverfahren.

Selbst abgesehen von diesen (noch) ausstehenden Beweisen gilt es festzuhalten, dass Chiffrier- bzw. Authentifikationssicherheit ein quantitatives und nicht ein grundsätzliches Mass ist; es gibt also nicht Sicherheit oder fehlende Sicherheit, sondern mehr oder weniger Sicherheit. Dahinter verbergen sich komplexe Optimierungsprozeduren, denen sich Chiffriertheoretiker anzunehmen haben.

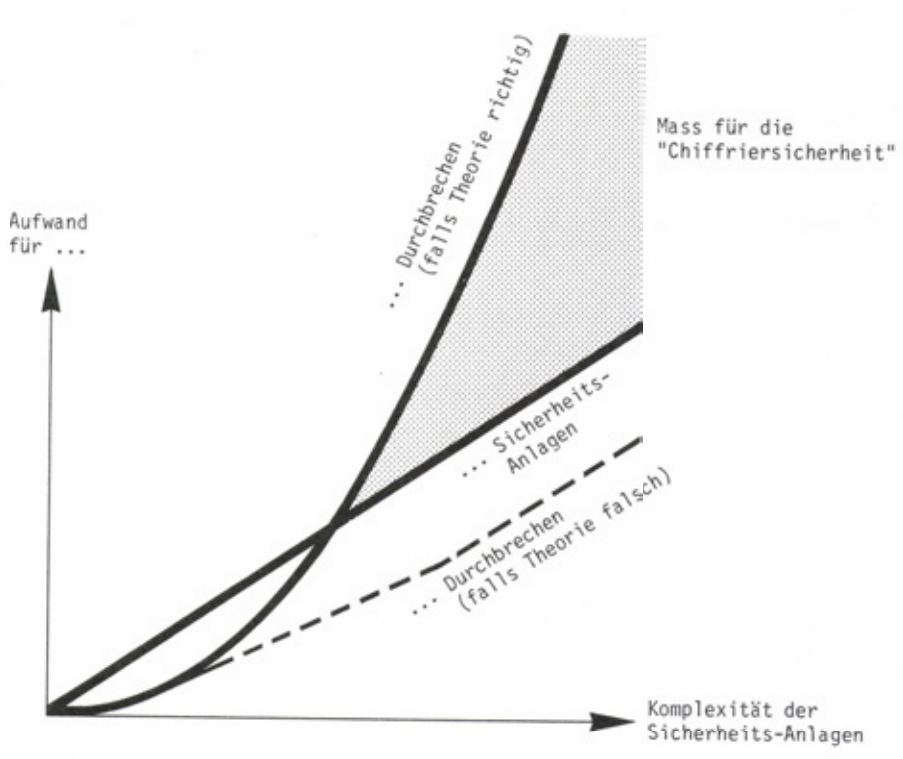


Fig. 22 Kosten/Nutzen für Sicherheitsanlagen

Figur 22 illustriert grob die Annahmen, die dabei zugrundegelegt werden: Man darf annehmen, dass mit wachsender Komplexität oder mit wachsender Perfektion eines technischen Sicherheitskonzepts der technische Aufwand zur Realisierung desselben anwächst, vielleicht in erster Näherung proportional damit. Der unbefugte Dritte hat seinerseits einen Aufwand zu leisten zum Durchbrechen der Sicherheitsschwelle, wobei dieser Aufwand, so die Grundannahme, stark progressiv anwächst mit wachsender Komplexität des Sicherheitskonzepts.

Ein Beispiel dazu ist gezeigt worden anhand des RSA-Systems von Figur 16, wo der unbefugte Dritte einen ungeheuren Rechenaufwand zu erbringen hat, um eine sehr grosse Zahl in ihre beiden Primfaktoren zu zerlegen. Dieser Aufwand wächst in der Tat exponentiell mit der Grösse der beteiligten Primzahlen oder auch mit der Anzahl der Primfaktoren, wenn man mehr als deren zwei zu einer grossen Zahl ausmultipliziert. Allerdings (und darauf ist bereits hingewiesen worden): Das stimmt nur insofern und allenfalls nur solange, als es (noch) nicht gelingt, Zerlegungsalgorithmen mit einem viel kleineren Komplexitätsmass zu finden.

Auf der einen Seite ist damit die Frage nach der Chiffrier- bzw. Authentifiziersicherheit so offen, wie sie es immer gewesen ist in der Theorie der Chiffrierung. Andrerseits muss man aber berücksichtigen, dass die heute modernen Verfahren bei korrekter Anwendung einen so grossen Sicherheitsabstand gegenüber heutigen Theorien, die diese Sicherheit in Frage stellen könnten, aufweisen, dass die Drohung grundsätzlicher Unsicherheit nicht allzu schwer genommen werden darf. In der Tat zeigt die Erfahrung seit dem Bestehen der modernen Verfahren, von denen einige gezeigt worden sind, dass die mathematisch gestützte Chiffrier- bzw. Authentifiziersicherheit keineswegs mehr das schwächste Glied in der Sicherheitskette ist. Vielmehr sind es viel primitivere Verletzungen von einfachen Betriebsvorschriften oder Sicherheitsvorkehrungen (vgl. dazu etwa Figur 2), die heute ins Gewicht fallen. Wenn die heute bekannten und bewährten allgemeinen Sicherheitsprinzipien diszipliniert angewendet werden, droht bis auf weiteres bestimmt keine Gefahr von der Seite der unbewiesenen mathematischen Sicherheit. Dies gilt insbesondere für die eigentliche Hacker-Szene, denn bei diesen Delinquenten handelt es sich ja kaum um hochmathematisch geschulte Spitzenfachleute mit frei verfügbaren Supercomputern, denn ohne enorme Ressourcen an Wissen und an Computerapparaturen ist es (mindestens aus heutiger Sicht) undenkbar, aus der mathematisch-theoretisch unsicheren Sicherheitssituation heraus Kapital zugunsten der Hacker-Tätigkeit zu schlagen.