

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreise



%! biohazard.ps
% Copyright 1993 by Jed Hartman.

Das

IMPRESSUM

Die Datenschleuder

wissenschaftliche Fachblatt für Datenreisende
Heft 44 (Zählnummer für Abonnenten)
September 1993

Da wir als Zentrale o.ä. sowieso nicht taugen, empfehlen wir immer und überall dezentrale Aktivität bzw. Kontaktaufnahme zu lokalen Gruppen / Menschen.

Adresse:

Die Datenschleuder

Schwenckestr. 85

D-20255 Hamburg 20

Tel.: +49-40-4903757

Vmb.: +49-40-497273 (Tonwahl erforderlich)

Fax.: +49-40-4917689

Mbx.: +49-40-4911085 (CHAOS-HH.ZER)

Internet/UUCP: ds-red@cccchh.ccc.de

Mailserver/UUCP: ccc-serv@mail.ccc.de

BTX: *CCC#

Redaktion: (A)ndy, Cash, rowue, Nomade

ViSdPg: Jan Schreiber

Herausgeber: Chaos Computer Club e.V.

Druck: Bernd Paustian, Schwenckestraße, Hamburg

Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder.

Einzelpreis 3,50 DM. Mitglieder des Chaos Computer Club e.V. erhalten die Datenschleuder im Rahmen ihrer Mitgliedschaft.

Abpreise siehe Bestellsetzen.

Adressänderungen von Abonnenten am besten schriftlich (Postkarte genügt).

(C)opyright 1993: Alle Rechte bei den AutorInnen. Kontakt über die Redaktion

Nachdruck für nichtgewerbliche Zwecke mit Quellenangabe erlaubt. Belegexemplar erbeten.

Eigentumsvorbehalt

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habnahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden.

Redaktorial

Neben mir liegen die letzten paar Seiten der DS, das Titelbild muß morgen noch eingeklebt werden. Der Rest der Redaktion ist schon vor einigen Stunden gegangen, es ist halb zwei, eigentlich wollte ich auch schon längst weg sein. Aber morgen ist einliefern angesagt. Mittlerweile leicht benebelt vom Fixogum sitze ich nun hier... gleich ist Feierabend. Um mich von meinem Platz zu bewegen muß ich durch Ausdrücke waten. Irgendwoher kenne ich das doch noch. Nunja, nochmal einen Kaffee klarmachen, und dann Endapurt - komisches Wort. Letztes Wochenende Congressvorbereitungstreffen in Berlin, dieses Wochenende Datenschleuder, nächstes endlich mal wieder „frei“ - bis jetzt.

Mal sehen, was auf diese DS mal wieder zurückkommt: „geschäftschädigend“, „Jungstalinisten“, „Schülerzeitungsniveau“ (Übrigens: wenn Ihr konstruktive Vorschläge habt, mitarbeiten wollt oder einfach mal Lust habt, mehr über dieses oder jenes zu erfahren: Einfach melden!!!).

App. Congress, der findet dieses Jahr auch wieder statt, wie üblich vom 27. - 29.12., wer noch Ideen hat, sollte diese über den Verteiler ccc93 auf der smoke.ccc.de an uns weitergeben.

Mittlerweile ist es halb drei, für die DS fehlt nur noch dieser Text und das Titelbild. Das Fixogum ist alle - ich auch.

Unser „Freund“ Kimble scheint wohl insgesamt seinen Kopf soweit hinausgelehnt zu haben. Ich kann ihm nur wünschen, daß er seinen Höhenflug genossen hat. Vielleicht können ihm ja seine Kölner Freunde weiterhelfen. Die kennen sich ja in solchen Spielen aus, unser Metier ist das eher nicht. (Warum, war der Tagespresse zu entnehmen...)

Nunja, letztendlich werde ich mich wohl jetzt ins Bett bewegen (ca. 30 min zu Fuß von hier - sch... Nachtbusse), eigentlich wollte ich heute Abend noch los, aber das kann ich mir jetzt wohl „abchminken“.

cu l8er (bis zur nächsten DS....)

rowue

Leserbrief

The previous *Datenschleuder* contained a leaflet about our 'Hacking at the End of the Universe' congress as well as a message from Rowue and Cash saying that they would not have included the leaflet because (basically) we do business with the intelligence community. Most of you have seen the text.

We were a little surprised to see that Rowue and Cash were taking an old matter so seriously. Their letter only cryptically speaks of 'technical equipment' being sold to 'Intelligence organisations' in 'large quantities'. Lets be a little more specific.

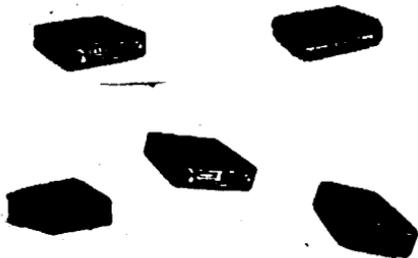
Somewhere in 1992 we got a call from a person that calls himself 'Kimble'. He is well known for selling phone-phreak tricks for DM 1000.- and doing other things that are both criminally lame and just criminal. I hear he is also in touch with people that are known to be in touch with the Bundesverfassungsschutz.

I had talked to him once before because I had refused to talk to him together with Donn B. Parker and Kenneth Linndup from SRI international. The two of them were doing a study on 'telephone system security' for AT&T. I am always willing to talk to anyone about anything. This talk was not very productive however because Donn was continually asking questions like 'who are your contacts in'. Anyway, they wanted to bring Kimble to this meeting, he was already in Holland, but I said I had no interest in meeting someone that was selling phreak-tricks. So Kimble went back to Germany pissed off.*

Back to this Kimble character: He wanted to have a Demon-Dialer(tm), and he wanted us to send it to him with a bill (for DM 350) attached. I told him that this was to be an advance payment deal. Then he wanted to know how much 50 Demon-Dialers(tm) would cost him. I said 'well, $50 \times 350 = 17500$ '. He said that he would order this 50 after evaluating a free sample. Again, I said 'No'. That was the end of our conversation and of all contacts between Hack-Tic and this Kimble person.

When Rowue heard this whole story at the 1992 Chaos Communication Congress he was shocked that I was willing to sell Demon-Dialers to this person. We had a long argument where we both repeated our arguments several times over.

Our argument for selling Demon-Dialers to whoever wants them is that they are a tool, merely useful for making the tones necessary for manipulating the phone system (or doing many other useful things). We have no way of checking what every individual does with her or his Demon, and we don't want to know. We sell the Demon like someone else would sell a soundblaster card (useful for the same things), and we use the money to develop new products to serve the hack/phreak community.



Rowue could not live with our point of view and chose to include his standpoint with the previous *Datenschleuder*. I regret that we were not asked to give our side of the story back then so we could have placed the whole thing in perspective.

Basically: we never did any business* with any intelligence organisation, but we reserve the right to do so in the future. Dear intelligence person: you'll find our prices to be most reasonable, call us for a brochure.

* The dutch BVD subscribes to Hack-Tic, but that's about it.

Rop Gonggrijp,

Hack-Tic

Rop Gonggrijp (rop@hacktic.nl) fax: +31 20 6900968 voice: +31 20 6001480

Meinungen

Reaktion auf Leserbrief u.s.w.

Da es wegen dieser Geheimdienst/Kimbel/HEU Geschichte zu immer mehr hin- und hergeschreibe, kommt fühlte ich mich dazu gedrängt, einmal meine Meinung, die sich wohl ein wenig von den anderen unterscheidet, zu überdenken und kund zu tun.

Also, prinzipiell ist mir klar, daß die Nachrichtendienste sich diese Geräte auch anderswie beschaffen können, und daß der Kimbel evtl. nur ein Exemplar „schnorren“ wollte.

Womit ich Probleme habe, ist der „sorglose“ Umgang mit dieser Problematik, denn ein Verkauf von Gerätschaften bedeutet halt nicht nur, daß die Leute eher dran kommen, sondern läßt auch bei einigen Kids das Bild entstehen, daß „die von der HackTic“ ja irgendwie mit denen was machen, und daß das folglich schon ganz o.k. ist, dies auch zu tun. Eine Organisation wie die HackTic sollte sich ihrer Vorbildfunktion bewußt sein und dementsprechend handeln, denn die Kids werden bei den Nachrichtendiensten sicherlich den Kürzeren ziehen.

Daß ich die HEU-Einladungen nicht verschicken wollte und nen bisserl grummelig war läßt sich hauptsächlich wie folgt erklären:

Nach der übernächstigen Fertigstellung und Verpackung der Datenschleuder entschloß sich der Redakteur, der die HEU's unbedingt in der DS haben wollte, dazu uns telefonisch aufzufordern dies nun auch noch zu tun, da er keine Zeit, Lust oder was auch immer hatte. Da dazu aber keine Energie mehr vorhanden war, mußte der Mensch sich neu paar andere Einpacker suchen. Um meinen Unwillen über oben genannte „Sorglosigkeit“ und meinen Frust loszuwerden, habe ich mich dann telefonisch an der Erstellung des beigelegten Textes beteiligt, welcher, da „Argumentensammlung“, sicherlich nicht nur meine Meinung verkörpert.

also bis zum Congress ?
cash (cash@cashh.ccc.de)

BookNote

Practical Unix Security Simson Garfinkel,
Gene Spafford O'Reilly & Associates IGSBN
0-937175-72-2

Das gute Stück fand seinen Weg neben mein Terminal, als ich mich tatsächlich mal mit *ix-Security herumschlagen mußte...

Die Autoren haben zwar (wie im Vorwort erwähnt) auf die minutiöse Schilderung der etwas geschickteren Versuche verzichtet, beschreiben aber sehr umfassend die diversen potentiellen Löcher gebräuchlicher *ix-Systeme.

Das Buch vermittelt ein sehr umfassendes Bild der möglichen Schwachstellen und beschränkt sich dabei durchaus nicht nur auf technische Aspekte, sondern spricht auch Themen an wie mangelndes Sicherheitsbewußtsein der Benutzer - inkl. Vorschlägen zur Abhilfe. Angenehm fällt auf, daß die Autoren durchgängig das Wort „Attacker“ benutzen, was mir - auch unter Berücksichtigung der Wortähnlichkeit - unangenehm verdeutlichte, wie nahe auch mein Gebrauch des „Hackers“ schon dem *ILD-Zeitungsniveau gekommen ist (war :-).

btw: Finger weg von der deutschen Ausgabe...

*ix is a registered bell of AB&C Trademark Laboratories (unknown)

-bkr



Betr.: Leserbrief

Um hier auch mal meinen Senf dazuzugeben: Als einen Punkt sehe ich, daß Rop von Kimbles Verbindungen zur NaDi-Szene wußte, und trotzdem relativ sorglos hiermit umging, wohlwissend der Erfahrungen, die nicht nur wir mit dieser Szenerie gemacht haben, und diese, im, milde ausgedrückt, nicht nur positiven Sinne.

Aus diesen Gründen habe ich z.B. Gespräche mit der SRI und den LfV [Landesamt für Verfassungsschutz] abgelehnt. Ein anderer Grund für mich ist die Vorbildfunktion, die wir für die Kids haben, und die oben beschriebenen Erfahrungen (Karl, Nasa), und das daraus resultierende Wissen, daß die Kids hierbei eher negative Erfahrungen machen werden, Erfahrungen, wo ich nicht möchte, daß sie diese machen.

Aus diesen Gründen verspürte ich keine große Lust, noch irgendwelche Informationsbrochüren einzutüten. Zumal wir über die Veranstaltung schon in der DS 42 (?) informiert hatten, hier hatte es schon Diskussionen gegeben, in der ich meinen Standpunkt klargestellt hatte.

Nun war es aber so, daß jemand hier aber den Kram unbedingt drinne haben wollte, und ich mich aus den oben beschriebenen Gründen weigerte (Information doppelt vergeben, „Kimble“ und Dialer). Hier war mensch zu dem Punkt gekommen, daß diese Person den Kram dann selbst eintüten würde.

Leider hatte die Person aber wohl anscheinend nicht den Sinn des Wortes „Nein“ verstanden, oder er glaubte nicht, daß „Nein“ auch Nein heißt. Aufjedenfall rief er, nachdem der Kram in Harburg schon versandfertig war, hier an, und meinte, wir sollten den Kram eintüten. Da wir uns weigerten, telefonierte er durch die Gegend, und fand „Eintüter“.

Aus der ganzen Situation, auch dem Frust, eine versandfertige DS nochmal auseinanderreißen zu müßen, entstand die Stellungnahme.

last but not least:

Das ich eine „alte Geschichte“ so ernst nehme, hat die oben beschriebenen Gründe.

Das ich die Geschichte von Anfang an so ernst nahm weiß Rop, er hatte mit mir ja die Diskussion auf dem letzten Congress. Die Gründe stehen oben, und sind teilweise in der Vergangenheit des CCC's zu finden. Ich würde mich freuen, wenn Rop auch hier mal über Verantwortung nachdenkt, und sich überlegt, was stärker wiegt: die Vorteile oder die Nachteile eines Handelns in dieser Weise. Erfahrungen, wie wir sie gemacht haben möchte ich Rop nicht wünschen.

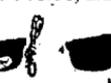
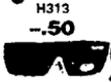
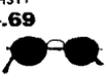
Desweiteren versenden wir auch Exemplare der DS an die verschiedensten Institutionen des Sicherheitsapparates der BRD. Dies aber um hier einen offenen Stil zu fahren, und um zu zeigen, daß wir an irgendwelcher konspirativen Kinderkacke kein Interesse haben.

PS: Das „Kimble“ ein A.... ist, sollte jeder wissen, ob er was mit Ihm zusammen macht, sollte jeder für sich entscheiden. rowue

...SONNENBRILLEN... ...SONNENBRILLEN...

Über 1.000.000 Stück warten auf Sie
in unserem Lager Taiwan.

Super-Mode und Super-Preise, z.B. wie folgt:

			
H313 -50	H314 -46	H311 -69	
			
H312 -69	H292 1.22	H293 1.22	H294 1.22
	Bestellen Sie bitte sofort bei		
H285 1.83	劉氏貿易公司(柏林)		
	Import und Export GmbH		
	1000 Berlin		

Die Invasion der Karten

Mittlerweile kennt sie jeder: die kleinen Karten mit diesem silber-kupfernen Teil drauf - sog. Chipkarten. Zuerst der breiteren Öffentlichkeit nur als Telefonkarten bekannt (und mittlerweile akzeptiert), streben sie nun an, auch in weitere Bereiche unseres Lebens einzudringen. Sicherer als Magnetkarten, die ja noch relativ einfach kopiert werden können und mit einem geringen Aufwand auch neu beschrieben werden können. Für viele ein Segen, für einige ein Fluch, oder zumindest etwas, bei dem die Folgen für die Gesellschaft (Stichwort gläserener Bürger) noch zu bewerten sind.

Worum geht es hier eigentlich

oder ist mein Luftkissenboot voller Aale...

Chipkarten haben auf dieser kleinen Karte meistens (fast immer) einen Microprozessor, und auch mehr oder weniger Speicher integriert. Die Möglichkeiten, die sich dadurch auftun, sind (fast) nur durch die Phantasie derjenigen begrenzt, die sich Gedanken über den Einsatz dieser Geräte machen.

So gehen z.B. Banken mittlerweile dazu über, neben den normalen Magnetkarten auch die Chipkarten zu verwenden, da diese „sicherer“ sind. In Kiel läuft derzeit ein Feldversuch, in dem ein am öffentlichen Personennahverkehr teilnehmender Mensch seine Fahrtkosten auch über Chipkarte zahlen kann. Wenn dies noch als Buchungskarte mit der Telekom-Karte zusammengeführt wird, so ist es hiermit sehr leicht möglich, ein Kommunikationsprofil über eine Person zu erstellen; welche Möglichkeiten der Rasterfahndung (u.U. auch im Zusammenhang mit der Pestleitzahlenumstellung) sich hier ergeben, sollten sich Leute, die hier in Ruhe schlafen möchten, nicht ausmalen.



Nein,
diese
sind nicht
gemeint

Planungen

Ab ca. 1994 (zehn Jahre nach Orwell) soll unter anderem der Krankenschein auf eine Chipkarte umgestellt werden, um auf diese Weise noch einiges mehr an Infos unterzubringen, wodurch der behandelnde Arzt einen wesentlich besseren Überblick über den Patienten bekommt, einen Überblick, den sich ein guter Arzt im Gespräch mit dem Patienten verschafft, und den sich ein „schlechter“ Arzt auch nicht mit der Chip-Karte besorgt. Er sieht eine direkte „Diagnose“ dem Übergreifenden Teil vor. Zum anderen ist es so, daß zur Speicherung der Daten ein Code verwendet wird, welcher vierstellig ist, und damit alle Krankheiten abdecken soll. Inwiefern dieser Code eine differenzierte Diagnose des Krankheitsbildes zuläßt, wird die Zukunft zeigen. Ich glaube es erstmal nicht. Desweiteren sollen aber auch durch diese Codierung u.a. die Leistungssätze der Krankenkassen bestimmt werden. Welche Auswirkungen dies in der Zeit des „Zusammenbruchs“ des Sozialstaates hat, kann mensch sich ja vorstellen: Konnte der Arzt vorher noch entscheiden, ob er anstelle der Antibiotika lieber Naturheilmittel verwenden soll, so wird es in Zukunft wohl eher dahin gehen, daß die Ärzte (auch um „wirtschaftlich“ zu arbeiten) dann eher mal den Knaller nehmen, der zwar auf kurze Sicht besser wirkt, aber auf lange Sicht mehr Nachteile mit sich bringt.



UND
WER
VON

DIESER
NORM
ABWEICHT,

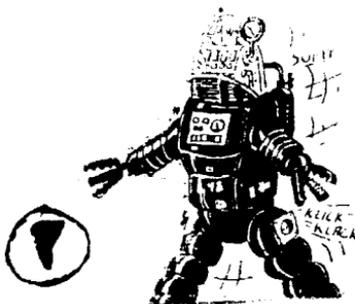
WIRD
ERFASST!

Festung Europa

Zum anderen „lassen sich die Niederlande den Betrug durch Asylbewerber nicht mehr gefallen“ (O-Ton.....) und gehen nun dazu über, jeden Flüchtling einer Erkennungsdienslichen Behandlung zu unterziehen, und diese Daten zum einen in ein Landesweites Informationssystem zu speichern (siehe AFIS in der BRD, hier werden die Fingerabdrücke von Flüchtlingen und „Verbrechern“ gespeichert, um zum einen Doppelidentitäten aufzudecken, aber auch um „Straftaten“ leichter aufzudecken), als auch auf der persönl. Chipkarte elektronisch zu vermerken. Zusammen mit dieser Einführung wurde am Amsterdamer Flughafen „Schiphol“ ein System installiert, wo sich die Fluggäste mittels einer Chipkarte und Ihres Fingerabdrucks an der Passkontrolle „vorbeimogeln“ können. Dies gilt für europäische Mitbürger und soll in dem Bundesland BRD auch bald eingeführt werden.

Was noch????

Konsequent wäre es, auch noch den Personalausweis in Form der Chip-Karte einzuführen: Alle Menschen, die hier leben, gleich nach ihrer Materialisierung einer ED-Behandlung zu unterziehen, diese alle zehn Jahre zu aktualisieren, und evtl. gesammelte Daten sofort zu überprüfen. Ob dies



eine erfolgversprechende Methode ist, die den Aufwand rechtfertigt, und wie sich dies mit einigen Demokratischen Grundregeln verhält, ist fraglich.

rowue

/dev/netland

Mailiste: cypherpunks-request@toad.com
Cypherpunk: caring about privacy on our networks, especially interested in public key cryptography.

CIA World Factbook

Äußerst brauchbare Datensammlung über alle Länder/Regionen der Erde, enthält geographische wie auch soziale und politische Daten.

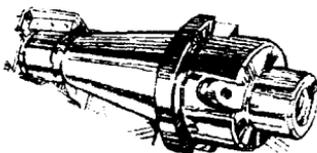
Bequemer Zugang:

\$ telnet info.rutgers.edu : go factbook

Unsere Uni ?

Die Fiji-Islands haben seit kurzem IP-Connectivity (mit eigenem Name-Server). Die Institution nennt sich „University of the South Pacific“, residiert unter kula.usp.ac.fj und hat kürzere IP-Turnaroundzeiten von Hamburg als so manche deutsche Uni.

-bkr



Sorry

Lieber Leserinnen und Leser, liebe tasybestellerInnen,

Etwas kurz nach der DS 36 kam bei uns die „Idee“ auf, einen Taschensynthi zu bauen. Dies sollte ein kleines Gerätchen sein, mit dem die Möglichkeit der netzunabhängigen Tonerzeugung besteht. Jedem sollte eigentlich klar sein, an was wir gedacht hatten.

Leider hatten sich einige Leute etwas zu schnell dazu bereit erklärt, ein Gerätchen zu bauen; leider wurden Zeit und persönliche Motivation, das Gerät zu bauen, überschätzt.

Derzeit ist es Stand der Dinge, daß wir das Projekt eingestellt haben. Insofern möchten uns die Besteller informieren, ob sie das Geld bar, oder als Bestellungen aus dem Bestellfetzen haben möchten.

Wir möchten uns noch einmal entschuldigen und hoffen gelernt zu haben.

chaos-team

RSA

Thema: Datensicherheit, Verschlüsselung mit dem RSA-Code. Theoretisches.

Quelle: Vorlesung über Lineare Algebra, Paderborn.

Das „public key“-System von R. L. Rivest, A. Shamir, L. M. Adleman (1978) (RSA-Code):

Die Benutzer eines öffentlichen Kommunikationssystems wollen verschlüsselte Botschaften austauschen. Es wird ein Alphabet mit N Zeichen benutzt. Die Zeichen werden durchnummeriert. Seien $b(0), b(1), \dots, b(N-1)$ die Buchstaben in diesem Alphabet. Diese Reihenfolge wird beibehalten. Man wählt natürliche Zahlen k und l mit $k < l$, für die N^k (N hoch k) und N^l (N hoch l) ca. 200 Dezimalstellen haben. Das Alphabet, die Reihenfolge der Zeichen, die Zahl N , und die Zahlen k und l werden veröffentlicht.

(1) Erzeugung des Codes

Es sei A ein Benutzer dieses Systems. A wählt zwei verschiedene Primzahlen $p(A)$ und $q(A)$ mit jeweils etwa 100 Dezimalstellen, die folgende Bedingung erfüllen:

Es ist $N^k < p(A) * q(A) < N^l$

Dann berechnet A die Zahlen $m(A) = p(A) * q(A)$ und

$\phi(A) = (p(A) - 1) * (q(A) - 1)$

und wählt eine Zahl $e(A)$ zwischen 1 und $\phi(A)-1$, die mit $\phi(A)-1$ keinen gemeinsamen Teiler hat. Anschließend berechnet A die Zahl $d(A)$ für die gilt:

Es gibt eine natürliche Zahl k mit: $d(A) * e(A) = 1 + \phi(A) * k$

(Mathematisch: $d(A) * e(A)$ ist kongruent zu 1 modulo $\phi(A)$)

(Für die Berechnung von $d(A)$ gibt es schnelle Algorithmen. Eingabe dieser Algorithmen ist $e(A)$ und $\phi(A)$. Die Geheimhaltung von $\phi(A)$ ist also dringend erforderlich, um die Sicherheit des Codes zu garantieren.)

Die Zahlen $m(A)$ und $e(A)$ werden veröffentlicht, die Zahlen $p(A)$, $q(A)$, $d(A)$ und $\phi(A)$ müssen geheimgehalten werden. $p(A)$, $q(A)$ und $\phi(A)$ werden nicht mehr benötigt.

(2) Verschlüsselung und Entschlüsselung

Der Benutzer B möchte an A eine verschlüsselte Nachricht schicken. B teilt den Klartext in Blöcke aus k Zeichen und ersetzt jedes Zeichen durch sein „numerisches“ Äquivalent (also jeweils $b(i)$ durch i). So entstehen k -Tupel aus Zahlen in $\{0, 1, \dots, N-1\}$. Es sei $(y(1), \dots, y(k))$ ein solches k -Tupel. B berechnet

$X := y(1) * N^{(k-1)} + y(2) * N^{(k-2)} + \dots + y(k-1) * N + y(k)$

und

$X1 := (X - e(A)) \text{ MOD } m(A)$

Es gilt $0 < X < N^{k-1} < N^{l-1}$. B berechnet die $z(1), \dots, z(l)$ mit

$X1 = z(1) * N^{(l-1)} + z(2) * N^{(l-2)} + \dots + z(l-1) * N + z(l)$.

Das l -Tupel $(z(1), \dots, z(l))$ wird über das öffentliche Kommunikationssystem an A geschickt.

A berechnet daraus wieder $X1 = z(1) * N^{(l-1)} + \dots + z(l)$, und dann

$X2 := (X1 * d(A)) \text{ mod } m(A)$. Es gilt: $X2 = X$.

Aus X berechnet A die Zahlen $y(1), \dots, y(k)$ mit

$X := y(1) * N^{(k-1)} + y(2) * N^{(k-2)} + \dots + y(k-1) * N + y(k)$

und hat damit $(y(1), \dots, y(k))$ zurückgewonnen, und kann die Originalnachricht daraus zusammensetzen.

Anmerkung:

Die Gesamtnachricht setzt sich aus den Kodierungen aller k -Tupel der Originalnachricht zusammen. Die Nachricht verlängert sich beim Kodieren also um das l/k -fache. Zum Kodieren ist die Kenntnis der Zahlen $m(A)$, $e(A)$, k , l , und N sowie die Kodierung der Zeichen im Alphabet notwendig. $m(A)$ und $e(A)$ haben jeweils ca. 200 Stellen und sind somit nur schwer zu merken, oder überall für jeweils alle Benutzer zu speichern.

(3) Identifizierung von Nachrichten

Jeder Teilnehmer erhält eine Signatur $(g(1), \dots, g(k))$ aus Zeichen des Alphabets zugewiesen, die ihn eindeutig identifiziert (z. B. der Username), und die veröffentlicht ist. B möchte mit seiner Botschaft

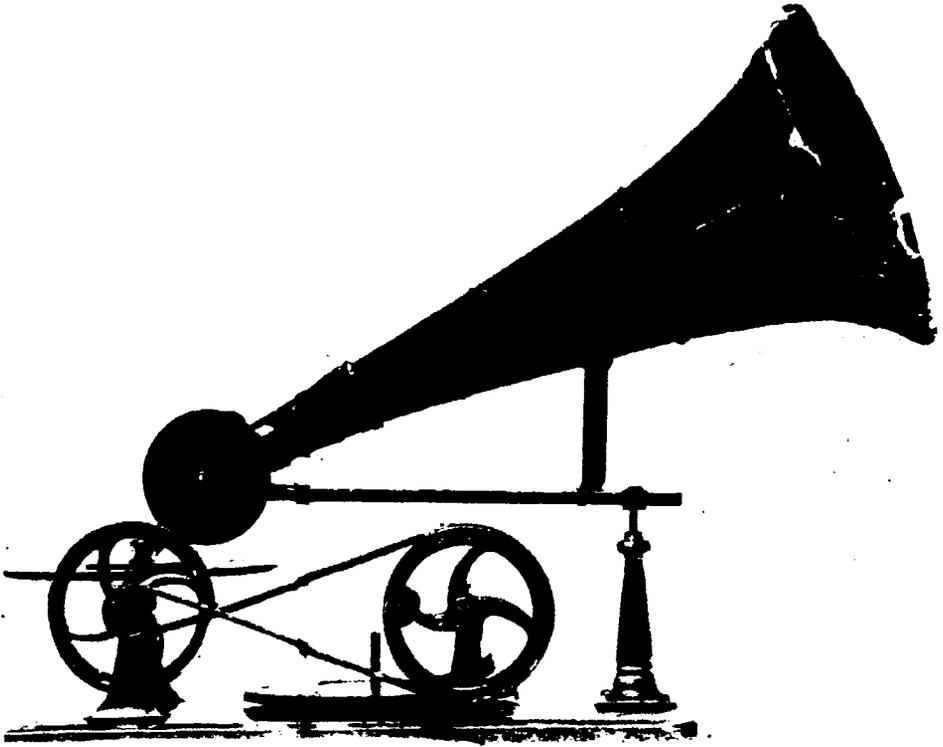
an A einen Beweis dafür mitschicken, daß die Botschaft von ihm kommt. B berechnet mit seiner eigenen Signatur:

$s := g(1) * N^{(k-1)} + g(2) * N^{(k-2)} + \dots + g(k-1) * N + g(k)$ und

$s1 := (s * d(B)) \text{ mod } m(B)$ und ermittelt daraus die $h(1), \dots, h(l)$ mit

$s1 = h(1) * N^{(l-1)} + h(2) * N^{(l-2)} + \dots + h(l-1) * N + h(l)$

und schickt $(h(1), \dots, h(l))$ mit seiner Botschaft an A . A dechiffriert, wie in (2) beschrieben die eingegangenen l -Tupel. Alle ergeben sinnvollen Klartext außer $h(1), \dots, h(l)$. Hiermit berechnet er



wieder

$s_1 := h(1) * N^{(l-1)} + h(2) * N^{(l-2)} + \dots + h(l-1) * N + h(l)$ und $s := (s_1 * e(B)) \bmod m(B)$

A schreibt s als:

$s = g(1) * N^{(k-1)} + g(2) * N^{(k-2)} + \dots + g(k-1) * N + g(k)$

und hat damit $(g(1), \dots, g(k))$ berechnet und vergleicht mit der veröffentlichten Signatur im Telefonbuch.

Anmerkung: Dieses Verfahren klappt nur dann, wenn man die Position der $h(1), \dots, h(l)$ in der verschlüsselten Datei nicht im Voraus ermitteln kann, und wenn B seine Identität bereits anderswo in der verschlüsselten Datei

andeutet. So bietet die hier beschriebene Methode eine Möglichkeit, das Dokument zu „unterschreiben“, so da nicht jeder diese Unterschrift unter ein mit falschem Absender versehenen Brief schreiben kann. Wenn die Zahlen $h(1), \dots, h(l)$ jedoch einem dritten bekannt werden, so ist das Verfahren hinfällig. Außerdem muß B seine Identität anderswo im Dokument angeben, weil sonst der Empfänger alle Möglichkeiten für verschiedene Absender durchgehen muß.

(4) Sicherheit

Die Sicherheit des Systems beruht darauf, daß es (noch) keinen schnellen Algorithmus zur Faktorisierung großer natürlicher Zahlen gibt. Um eine an A gerichtete Nachricht zu entschlüsseln benötigt man $d(A)$ und um $d(A)$ zu berechnen benötigt man die Faktorisierung von $m(A) = p(A) * q(A)$.

(5) Primzahlen

Zur Herstellung von $p(A)$ und $q(A)$ und $e(A)$ hat man einen Generator von Zufallszahlen zu verwenden (und einen schnellen Primzahltest)

(6) Zum modernsten Stand

- G. Brassard, Modern cryptography, 1988 - E. Kranakis, Primality and cryptography - N. Knoblitz, A course in number theory and cryptography
M.Jung

Radiotest

Erstmal einige Begriffe

„Scan“-Funktion: Hier werden in Speicherplätze einprogrammierte Frequenzen abgesehen, ob sich hier ein Träger findet, anschließend wird entweder für eine gewisse Zeit auf dem Kanal (Speicherplatz) verblieben, oder/und solange, bis der Träger verschwindet.

„Search“-Funktion: Hier werden zwei Frequenzen und eine Schrittweite (5 KHz, 12,5 KHz) eingegeben, und zwischen diesen Frequenzen wird nach Trägern gesucht.

Träger: eigentlich erklärt sich das von selbst, ansonsten kann mensch es so verstehen, daß auf der Frequenz was anliegt.

Prioritätenkanal: Die als Prioritätenkanal eingestellte Frequenz wird neben der derzeit eingestellten Funktion auch noch in gewissen Abständen (ca. 10 mal pro Minute) abgesucht, ob sich hier ein Träger findet, wenn einer vorhanden ist, wird je nach „Radio“ entweder solange auf ihr verblieben, bis kein Träger mehr vorhanden ist, oder/und bis eine gewisse Zeitspanne verstrichen ist.

Was will mensch mit dem Teil

Für menschen, die „nur“ mal so unterwegs Radio hören möchten, und wissen, welche Sender sie am liebsten hören, sind Geräte ab etwa 350.- o.k. Diese haben dann zwar keine sog. „Search“-Funktion, mensch kann sich also nur bekannte „Sender“ anhören, aber dies kann ja auch o.k. sein. Wenn mensch nicht so ganz weiß, welche Sender interessant sind, und/oder zu faul ist, sich die Kanal-Raster-Tabellen zu besorgen und die Sender quasi von Hand zu suchen, muß er dann schon mindestens ca. 550.- DM ausgeben, diese Geräte haben dann die sog. „Search“-Funktion. Als „Bonus“ dafür kommt er dann aber auch in den „Genuß“, mehr Sender empfangen zu können (wenn er dies „darf“). Für Leute, die sich lieber mal zuhause hinsetzen möchten, um sich dort in Ruhe dem Radio zu widmen, sind dann „Tischradios“ interessanter. Diese sind in der Handhabung einfacher als die Handradios. Hier gehen die Preise von ca. 450.- bis weit über 1000.-

Wenn mensch nun seinem Computer das „Radio“-steuern überlassen möchte, so muß er mindestens 1200.- anlegen. Im allgemeinen haben die Geräte dann aber den

Nachteil, daß die Steuerung „von Hand“ dann auch nicht so „komfortabel“ ist.

Kleine Übersicht

Handgeräte

PRO-38 (jetzt PRO-41)

Ehemaliges Exportgerät - seit der Änderung (s. DS 41) mit der Möglichkeit versehen, auch das Radioband entsprechend empfangen zu können und seitdem zugelassen (PRO-41). Kleines Gerät, 10 Kanäle, leider keine Search-Funktion. Insofern entweder was für Leute mit 'nem kleinen Geldbeutel und viel Geduld. Aber auch etwas für Leute, die ein anderes Gerät zuhause haben oder aus anderen Gründen die besten Sender kennen und ein Gerät zum „mal kurz mitnehmen“ oder „reinriechen“ suchen. (10 Speicher, 66-88, 136-174, 406-512 MHz, ca. 350.-)

AR-2000 (D)

Schönes Radio, hat in der Auslieferung viele schöne „Extras“ (Ledertasche, schöne Antenne). Leider etwas „fummelig“ zu bedienen. Prioritätenkanal (1000 Speicher, 0,5 - 1300 MHz, ca. 750.-).

Tischgeräte mit Computeranschluß

FRG 9600

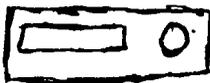
Tischgerät und auch ohne Computeranschluß noch ziemlich leicht zu bedienen. Der Computeranschluß ist leider sowohl auf der Hardware-, als auch auf der Softwareseite so realisiert, daß er nicht ohne Aufwand zu verwenden ist. Vor allem für die Auswertung der Feldstärke ist einiges an Aufwand zu treiben, da diese nur analog zur Verfügung gestellt wird (100 Speicher, viele Betriebsarten, ca. 1200.-). (0,5 - 400 MHz)

AOR 3000

Tischgerät, leider ohne Computeranschluß und fast nicht zu verwenden. Die Tasten sind so klein, daß sie ohne Stift kaum zu bedienen sind, dafür ist das Interface so gut realisiert, daß mensch schon mit einem programmierbaren Terminalprogramm viele Features des Gerätes nutzen kann. (0,1 - 2036 MHz, ca. 400 Speicher, diverse Betriebsarten, ca. 2300.-)

zum Schluß

Wenn mensch das Glück hat in einer größeren Stadt zu wohnen, kann mensch die Dinge über den lokalen „Radio“-Händler beziehen, wenn mensch dieses Glück nicht hat, so sollte er sich auf den Weg in die nächst größere Stadt machen, beim Kaufen über den Versand kann es evtl. zu unangenehmen Überraschungen kommen (vergl. Zykels).



Chaos-Finanzen

Kleiner Einblick in die Kontenstruktur...

Erstmal gibt es bei uns das sog. e.V. Konto, dieses Konto kennt so gut wie jeder, der mal was bei uns bestellt hat, oder der bei uns Mitglied oder Abonnent ist. Von hier aus wird ca. einmal pro Monat Kohle auf das sog. Erfa-Konto Hamburg überwiesen, über welches die Datenschleuder, das Büro in Hamburg, und der Einkauf von Bestellkrams abgewickelt wird. Ansonsten wird vom e.V. Konto noch Geld an ein Konto in Oldenburg überwiesen, zum einem um die redaktionelle Arbeit der Chalisti zu unterstützen, zum anderen um die IN- Gebühren für die Domain .ccc.de des Hamburger Rechners zu zahlen (dies sollte demnächst umgestellt werden, zum einen, da die Chalisti eingestellt werden soll, zum anderen, da die ccchh.ccc.de eine Angelegenheit des Erfa-Kreises Hamburg ist.).

Erfa-Konto Hamburg

Da dieses Konto für die Ausgaben zuständig ist, werden wir uns dieses mal beleuchten: Erstmal kosten uns die Räume im Monat ca. 670.-, hier drin sind enthalten: Miete, Strom, Gas, Wasser. Anschließend kommen pro Monat ca. 490.- an Telefonkosten (Intern, „Hot-Line“, VMB, FAX, Chaos-HH, ccchh), hierbei ist zu bedenken, daß auch die Gebühren für das BTX-Programm in Hamburg anfallen (ca. 130.-/Monat). Das Drucken einer Ausgabe der Datenschleuder kommt zwischen 650.- und 1500.- je nachdem, wo und wie wir Drucken (Xerographie, Offset). Anschließend kommen pro Monat noch ca. 120.- die wir für die Instandhaltung der Räume oder Bestellungen brauchen. Diese Bestellungen sind entweder Info-Material für die Datenschleuder (ca. 20.- pro Monat), oder Material für das Bestellwesen (ca. 100.- - 200.- pro Monat).

ES VI 18

Summasummarum:

Pro Monat brauchen wir derzeit ca. 1500.- um den Laden hier am Leben zu erhalten, wobei die Schwenekestr. selber den größten Teil (ca. 1200.-) verbraucht. In die Erforschung und Entwicklung von Forschungsinstrumenten können wir derzeit nicht allsuviel reinstecken, aber mal sehen, was die Zukunft bringt.....

Der Laden hat als Hauptnutzung die Ansprechstelle für Leute, und das sog. Bestellwesen, anschließend kommen das Archiv und die Datenschleuder (app. Archiv: wer hat Lust, mal mitzuhelfen, den Kram mal vernünftig zum Laufen zu bringen? Vorraussetzung: Gesundes Ego, Streßbereitschaft und Lust am Chaos).

Dies mal so als Vermittlung des Eindrucks, der sich hier beim Durchsehen der Konten so ergibt.

rowue



Kurzmeldungen

Uhr-heben

Auf der Jahrestagung der Deutschen Gesellschaft für Recht und Informatik in Fulda fand eine Podiumsdiskussion zu der Frage statt, ob die Strafbewährung für Softwarepiraterie abgeschafft werden solle. Die Quintessenz der diskutierenden Podiumsteilnehmer RA M. Barsch (Karlsruhe), RA Heymann (Frankfurt), StA Franzheim (Köln), Prof. Dr. Ulrich Sieber (Würzburg), Dr. Eichler (IBM Stuttgart) ging in die Richtung, dass die Bestrafung der Kids mit geklauten Spielen unsinnig sei und man für die Konzentration für den professionellen Handel eine Änderung der Vorschriften benötige. Der auf dieser Veranstaltung anwesende und hierauf angesprochene Herr Gravenreuth verwies auf "Einladungen der Szene und dort geführten teils heftige Auseinandersetzungen" wie die Chaos Communication Congresses, die Kieler Netzstage u.ae. Abgesehen davon, dass wir ihm somit noch lange nicht die Absolution für sein Handeln geben, wird der "heftig kritisierte" und mittlerweile bereits "mit Morddrohungen" behaftete Anwalt am 3.10.93 in Bielefeld im Bunker Ulmenwall im Rahmen einer Veranstaltung des FoeBud e.V. (Adresse siehe Adressenteil) einen Rechtfertigungsversuch wagen. Die Veranstalter haben angekündigt, fuer diesen bedrohten Teil der Bevölkerung Polizeischutz zu beantragen. Dass ihm abhanden gekommene Schild seiner Anwaltskanzlei in München geht derzeit als Wanderpokal durch die Szene, prämiert werden die effektivsten Aktivitäten gegen die Umtriebe des Herrn G. (Asterix/Andy)

Uhr-piepsen

Auf der IFA waren die Cityruf-Uhren der Fa. Swatch zu bestaunen (schon das an die Hand legen war wg. der dicken Ketten schwierig). Zunaechst soll es nur ein Nur-Ton (ca. 150 DM) und ein Numerik-Modell (ca. 250.- DM) im Exklusiv-Vertrieb der Tele-Kommerzialisten geben. Ein bisschen klobig sind sie noch, herzuheben ist die praktische Batterie-Tausch Möglichkeit, die allerdings auch alle 4 Wochen in

Anspruch genommen werden muss. Akkus gibt es in dieser Grösse angeblich noch nicht, so dass es wohl nur eine Frage

der Zeit ist, bis die Telekommunikationsindustrie die Autoindustrie nicht nur in Punkten Umsatz, sondern auch in Punkto Umweltbelastung erreicht hat. Aber die Dinger stinken wenigstens im Betrieb nicht.

D-Netz Leistungsmerkmale

Nachdem die Firma SEL bereits auf der CeBIT '93 ein 2400 Baud Modem in der Grösse eines mittleren Toasters für den Betrieb an D-NETZ Telefonen und rund 20.000 DM vorgestellt hatte, soll es ab Anfang nächsten Jahres dann tatsächlich Mobil-Faxe und ähnliches für GSM-Geräte geben. Wie Blueboxer und andere schon festgestellt haben dürften, geht bei der D/A-Wandlung und Digital-Komprimierung eher mehr als die Hälfte verloren, so dass man für derartige Aktivitäten (gemeint ist hier allerdings auch Fax / DFUE) vorerst nur die analoge Variante empfehlen kann. Ab Januar will der Rüstungskonzern ISDN-Leistungsmerkmale anbieten (OAD-Übermittlung abgehend und ankommend, Anklopfen, Makeln, 3er Konferenz), die Tele-Kommerzialisten ebenfalls im Frühjahr. Die Geräte-Preise werden im Weihnachtsmarkt (dank hoher Service-Provider Provisionen) wohl noch einmal deutlich fallen. Andy



Unser Globalgalaktisches Wörterbuch

yacker - Yuppie-Hacker glaubt, daß mensch zum Hacken mindestens 'nen 586'er, fünf Manta-Modems und mindestens 128 MB Hauptspeicher braucht.

OCR - Optical Character Recognition. Schlagwort von Menschen, die immer noch glauben, daß Computer die Arbeit effizienter machen. Möglichkeit Bücher zu lesen.

Unix - siehe NetHack.

Nethack - DuD-Adventure, spartanische Grafik, dafür mehr ins Spiel selbst gelegt. Achtung: Suchtgefahr!!!

VS - Volksturm, Verein zur Abfechtung der aufrechten Gesinnung.

Kaffee - dunkles flüssiges Betriebsmittel der leichteren Art

HD - siehe Hard Disk

Hard Disk - Harte Scheibe. Gekapseltes Medium. Gerät, mit dem durch das Speichern von Daten Rechner tiefergelegt werden. Ähnlich Autos: je größer und schneller, desto tiefer.

C5 - Internationales Vermittlungssystem. Arbeit über Töne. siehe auch Blueboxen.

Blueboxen - Möglichkeit, umsonst zu telefonieren. Arbeitet unter der Verwendung von Vermittlungssystemen und TallFree Nummern. Beim Telefonieren, kommt mensch in rauschähnliche Zustände und hört den Anderen zeitversetzt.

Cityruf - Pagerdienst der Telekomiker. Möglichkeit vielen Leuten zu erzählen welche Probleme mensch hat.

Pagerdienst - Möglichkeit einem anderen menschen eine Nachricht auf den Pager zu übermitteln, und ihn damit zu informieren. Siehe Cityruf.

POCSAC - Taschensack (siehe Cityruf-docu). Standard für Pagerdienste.

Usenet - Möglichkeit, mehr Informationen zu bekommen, als ein Mensch an einem Tag lesen kann.



BSI - Bravo Sierra India, oder auch Bundesbehörde für Sicherheit in der Informationstechnik. Ehemaliger MAD-Laden, legt Sicherheitsebenen und Sicherheitskriterien fest. Hat auch einiges mit Ver- und Entschlüsselung zu tun.

MAD - Verrückt. Militanter Abschirm Dienst. Institution zum Schutze der Streitkräfte.

Scanner - Abtaster zum Lesen von Seiten, oder zum Anhören von hochfrequenten Signalen (Aufgebohrtes Radio).

Information - Fakten, mit denen mein Denken in eine bestimmte Form gebracht werden soll.

foia - Freedom of information act. Gerüchteweise in den USA existierendes Gesetz, welches einem den Zugriff auf alle über ihn gespeicherte Informationen verschafft. Es sei denn, sie sind vom Gesetz ausgenommen.

Seil - Gerät zum Hochziehen.

Politik - Versuch, daß Überleben, sowie das friedliche Zusammenleben aller Ektoplasmen diese Universums in Gegenwart und Zukunft zu gewährleisten. Beim Mißlingen spricht mensch von Basisferne oder Wahlmüdigkeit

Flickschusterei - Gegenteil von Politik, wird aber häufig als diese verkauft.

**CHAOS-MITGLIEDS-
ABBOFETZEN****Chaos Computer Club**Schwenckestraße 85
D-20225 Hamburg
Telefon +49-(0)40-4903757
Telefax +49-(0)40-4917689Postgiro Hamburg
(BLZ 200 100 20)
Konto 599 090 - 201

Name: _____

Adresse: _____

Mitgliedschaft im CCC e.V. Schließt Datenschleuder-Abo mit ein.

<i>eww</i>	20,00 DM	Einmalige Verwaltungsgebühr bei Eintritt
<i>ewnm</i>	120,00 DM	Normalmitgliedschaft (Jahresbeitrag)
<i>ewsoz</i>	60,00 DM	Mitgliedschaft für Studenten, Schüler, Arbeitslose (Jahresbeitrag)

Reine Datenschleuder Abos Ein Abo gilt für 8 Ausgaben.

<i>nabo</i>	60,00 DM	Normalabo der Datenschleuder
<i>sabo</i>	30,00 DM	Abo der Datenschleuder für Studenten, Schüler, Arbeitslose

post ??,?? DM Porto/Verp./Spende/TrinkgeldSumme: DM _____, _____ bar V-Scheck Überweisung

Rechtsgültige Unterschrift _____

Chaos: E

BE

ERL

ADRESSEN**CHAOS-HH - CCC Hamburg**

Treffen jeden Dienstag ab 20 Uhr, Ort ist an der Aussenür ausgeschildert. Mailbox CHAOS-HH unter +49-40-4911085 Voice +49-40-4903757 Voice MBX +49-40-497273 Fax +49-40-4917689 Briefpost: CCC-HH, Schwenckestraße 85, D-W-2000 HAMBURG 20

CHAOS-B - CCC Berlin

Treffen jeden Dienstag ab 20 Uhr bei gutem Wetter: Am See im Park in der Brunnenstr. gegenüber der Polizeiwache (U-Bahn Linie 8: Rosenthaler Platz). bei schlechtem Wetter: Zettel an der Tür vom Cafe Art Acker, Ackerstr. 18, D-O-1040 Berlin. Briefpost: CCC-B c/o Müller, Postfach 840, 10048 Berlin. An der sonstigen Erreichbarkeit wird derzeit noch gearbeitet (DAL bzw. Prio. f. EAS/BAS gesucht).

Redaktion Chalisti/CCC Nordwest

c/o Frank Simon Strackerjanstr. 53, D-W-2900 Oldenburg Tel.: +49-441-76206 chalisti@sol.zer, chalisti@sol.north.de

CHAOS-HL - CCC Lübeck

Treffen am ersten und dritten Freitag im Monat, 19 Uhr in der Röhre (gerade von der Mengstraße ab).

Briefpost: CCC-HL, c/o Benno Fischer, Bughagenstr. 7, 2400 Lübeck 1 Voice: +49-451-34799 Mbx: MAFIA InfoSys +49-451-31642 300-38.400 Bps

CHAOS-RH - CCC RecklinghausenTreffen alle zwei Wochen oder so.
Voice: +49-2364-16349
Fax: +49-2361-652744
Mailbox: LITB +49-2363-66378 und LIVE-TIMES +49-2361-373214

Hack-Tic

Postbus 22953
 NL-1100 DI Amsterdam
 Voice: +31-20-6001480
 Fax: +31-20-6900968

2600 Magazine

Overseas \$30 individual, \$65 corporate.
 Back issues available for 1984-88 at \$25 per
 Year, \$30 per year overseas. Adress all Sub-
 scription correspondence to: 2600 Subscrip-
 tion Dept., P.O. Box 752, Middle Island, NY
 11953-0099.

Office Line: +1-516-751-2600
 Fax-Line: +1-516-751-2608
 Voice-Mail-System: +1-516-751-6634

2600 Meeting in Germany

Jeden ersten Freitag im Monat um 18:00
 Uhr im Münchener Hauptbahnhof in der er-
 sten Etage bei Würger King und den Tele-
 fonsellen.

Erreichbar als 2600@sectec.hanse.de, Voice-
 Mailbox +1-904-366-4431, auf den Tref-
 fen im Hauptbahnhof ueber die anrufbaren
 Zellen +49-89-591-835 und +49-89-558-541
 (bis 545, hier handvermittelt über Opera-
 tor).



CHAOS-RN CCC Rhein Neckar

Treffen jeden Dienstag 20 Uhr im „Vater
 Rhein“ in HD.

Wegbeschreibung von der Stadthalle: „Gehe
 über die Fußgängerampel, Gehe nicht über
 LOS. Durchquere den Mimipark. Gehe halb
 links. Jetzt stehst Du davor. Begib Dich
 in den linken Flügel der Gaststätte. Hin-
 ten rechts siehst Du einen Haufen Leute mit
 Schlepptops, Funkgeräten und ähnlichem
 Kram. Das sind wir. Trau Dich zu fragen,
 wir beißen nicht.“

Mailbox CHAOS RN unter +49-6221-
 904727

Briefpost: CCC-RN, Postfach 104027,
 6900 Heidelberg

Die Datenschleuder

CHAOS-RM - CCC Rhein-Main

Treffen finden statt oder auch nicht
 Voice: +49-6103-4100
 Mailbox:BITMAIL vielleicht unter +49-
 6103-45287

Briefpost: CCC-RM, c/o Engelter,
 Postfach 1201, 6073 Egelsbach

SUECRATES

Stuttgarter Computerrunde mit Zeitschrift

D'Hacksete

Garantiert keine Satzungsdebatten - Mit-
 glied im Bundesverband gegen Vereins-
 meierei e.V. Kontakt: T.Schuster, Im Feuer-
 hapt 19, 7024 Filderstadt 3 E-Mail: nor-
 man@delos.stgt.sub.org

FoeBuD-BI

Verein zur Förderung des öffentlichen be-
 wegten und unbewegten Datenverkehrs e.V.,

Bielefeld Treffen jeden Dienstag, 19:30 Uhr
 im Café

„Spinnererei“, Heeperstraße 64, D-W-4800
 Bielefeld 1, voice +49-521-62339

Monatliche „Public Domain“-Veranstaltung
 zu Themen aus Randbereichen der Com-
 puterkultur jew. am 1. Sonntag im Monat
 (außer Januar, Juli und August) ab 15 Uhr,
 im Bunker Ulmenwall, Kreuzstraße 0, 4800
 Bielefeld 1. Termine siehe BIONIC.

Voice: +49-521-175254 Fax: +49-521-61172
 Mailbox BIONIC unter +49-521-68000

Briefpost: FoeBuD c/o Art d' Ameuble-
 ment, Marktstraße 18, 4800 Bielefeld 1
 e-mail: ZENTRALE@BIONIC.ZER / zen-
 trale@bionic.zer.de

CCC-Ulm

Treffen jeden Mittwoch, 19 Uhr im Café
 „Einstein“, Uni-ULM

Kontakt: Framstag, framstag@rz.uni-ulm.de
 (Uli

Horlacher, Landfriedbühl 5, 7900 Ulm) und
 Deep Thought

(brenner@tat.physik.uni-tübingen.de
 (Martin Brenner) oder CCC-ULM, ccc-
 ulm@sol.zer und ccc-ulm@sol.north.de
 ohne Gewähr

**CHAOS-
BESTELLFETZEN**
Chaos Computer Club
Schwenckestraße 85
D-20225 Hamburg
Telefon +49-(0)40-4903757
Telefax +49-(0)40-4917689
Postgiro Hamburg
(BLZ 200 100 20)
Konto 599 090 - 201

Postvertriebsstück, Gebühr bezahlt - C 11301 F

Name: _____

Adresse: _____

Chaos-Literatur (auch im Buchhandel erhältlich)

_____ *hab1* 33,33 DM Die Hackerbibel, Teil 1 (260 Seiten A4)

_____ *vergriffen hab2* 33,33 DM Die Hackerbibel, Teil 2 (260 Seiten A4)

Chaos-Literatur (im Buchhandel eher nicht erhältlich)

_____ *stud* 7,50 DM Studie für die Grünen

_____ *metst* 16,00 DM Elektronische Informationssysteme für den Umweltschutz

_____ *vergriffen dok1* 5,00 DM Doku zum Tode von Hagbard (Karl Koch)

Infopakete / Software & Co. z.Zt. nur 5 1/4" Disketten möglich

_____ *ped* 25,00 DM PC-DES für MS-DOS: Private Verschlüsselung

_____ *psynth* 20,00 DM PC Soundprogramm für blane Töne

_____ *pcosac* 10,00 DM Pocsac - Decoder - nur für Schulung

Backer PVC wassergeschützt / gestanzt, wenn nicht anders angegeben

_____ *3ks* 3,33 DM 3 Stück „Kabelsalat ist gesund“ mit Chaos-Knoten

_____ *ah* 3,33 DM Bogen mit 64 Stück „Achtung Abhörgefahr“, Papier, zum Selbstausschneiden, postgelb

_____ *ooo* 5,00 DM 18x „Außer Betrieb“, 8x „Out of Order“, 1x „Guasto“

_____ *post* 5,00 DM Bogen mit Post-Totenkopf-Klebern verschiedener Größe

_____ *glob* 5,00 DM Bogen mit 10 Stck „Globales Dorf, Rechtsfreier Raum“

_____ *zula* 5,00 DM Zulassungsscheine („ZZF-Prüfnummer“)

_____ *cia* 5,00 DM Bogen mit 68 Stück „Chaos im Äther“, Papier, zum Selbstausschneiden, rot

Ganz Wichtiges Gedenkt bitte unserer immensen Portokosten! Rückporto **mindestens erbeten!**

_____ *post* ??,?? DM Porto/Verp./Spende/Trinkgeld

Summe: DM _____, _____ bar V-Scheck Überweisung

Rechtsgültige Unterschrift _____

Chaos: Eingang _____

Betrag erhalten _____

Erliegt _____



10. Chaos Communication Congress 1993

1984 - 10 Jahre später

27. - 29.12.1993

