

Die Datenschleuder



Das wissenschaftliche Fachblatt für kreative Technikknutzung
Ein Organ des Chaos Computer Club

ISSN 0939-1045

Dezember 1995

Nr. 53

DM 3,50

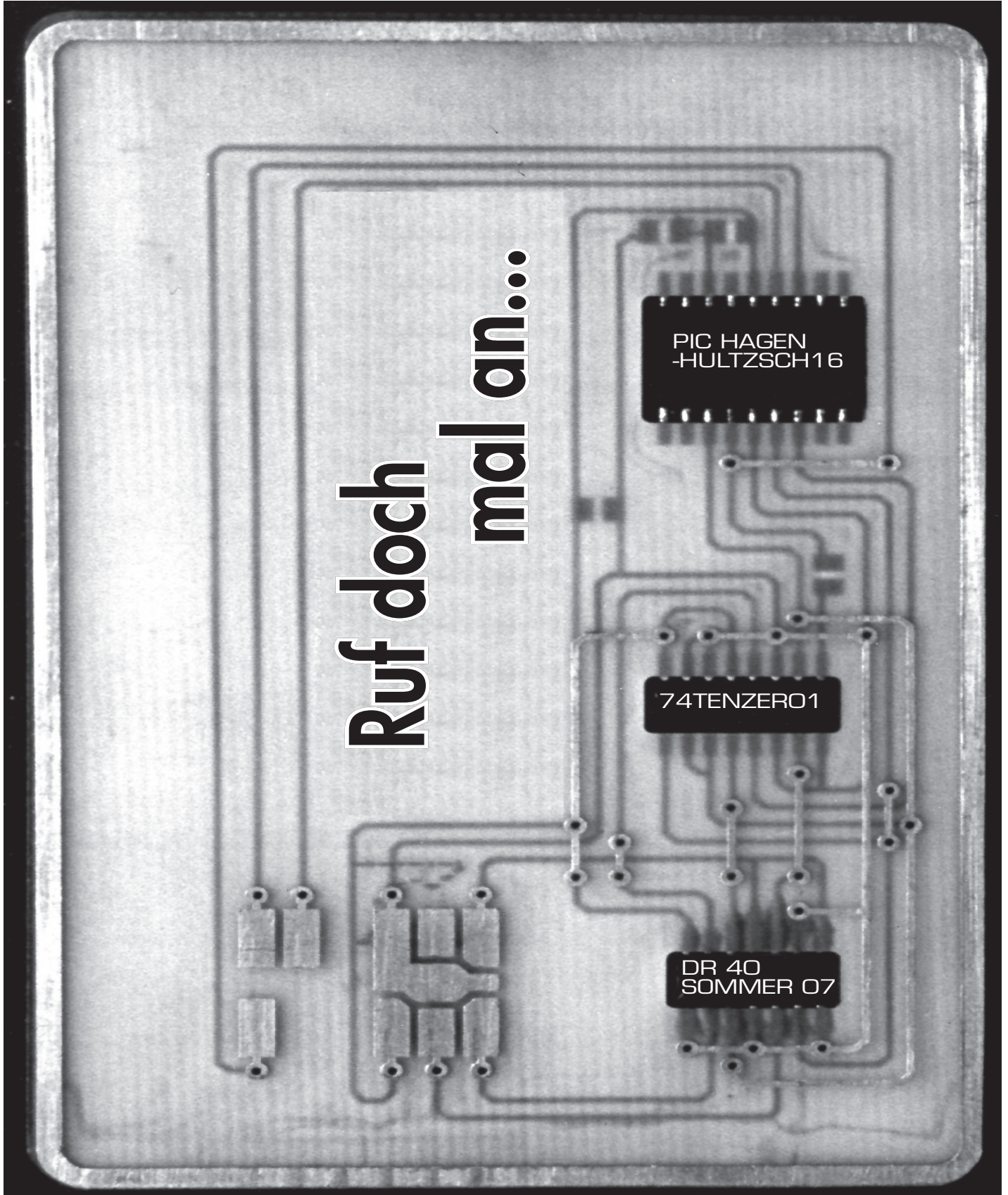
Postvertriebsstück C11301F

Ruf doch
mal an...

PIC HAGEN
-HULTZSCH16

74TENZERO1

DR 40
SOMMER 07



Das Wort zum Sonntag

Diese Datenschleuder wie wohl auch die nächsten Ausgaben kommt aus Berlin, um mal etwas Abwechslung in den drögen Alltag zu bringen.

Die eigentlich geplanten Rubriken Reisen mit der Datenschleuder, Film- und Buchkritik sowie einiges zu Multimedia (Jehova! Jehova!)-Pilotprojekten, Mautstellen auf der Infobahn (Steinigt Ihn! Er hat das Wort gesagt!), Telekom-Standardworten, D-Kanal-Ärger, dem Tarifsandal 96, **a u s f ü h r l i c h e** Telefonkartenbastelanleitung, das Dr. Ron. Sommer-Team berät usw. mußten leider aus Platz- (Geld-) Mangel auf später vertagt werden. Die nächste Datenschleuder wird wohl Ende Januar/Anfang Februar erscheinen, dann mit einer ausführlichen Würdigung des Telekom-Börsencrashes und den vertagten Artikeln.

Der CCC ist nun auch endlich auf dem SuperDatingTurboInfoMoneyHighway vertreten: <http://www.ccc.de/>.



I m p r e s s u m

Die Datenschleuder

Das wissenschaftliche Fachblatt für kreative Techniknutzung.

Nummer 53, Quartal IV, Dezember 1995

Herausgeber: Chaos Computer Club e.V.
Schwenckestr. 85 - D-20255 Hamburg
Tel. 040-4903757 / Fax 040-4917689

ViSdPg: Wau Holland

Druck: St. Pauli Druckerei Hamburg

Redaktion für diese Ausgabe und b.a.w.:
CCC (B) / Redaktion Datenschleuder OST
Neue Schönhauser Str. 20 / D-10178 Berlin

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. Abopreise siehe Rückseite.

Adressänderungen bitte nur schriftlich an die Hamburger Anschrift - Postkarte genügt.

Copyright (C) 1995: Alle Rechte bei den AutorInnen. Kontakt über die Redaktion. Nachdruck für nichtgewerbliche Zwecke mit Quellenangabe erlaubt. Belegexemplar erbeten.

Die teilweise elektronische Vervielfältigung von Datenschleuder-Beiträgen erfolgt nur durch die AutorInnen oder die Redaktion und zwar erst NACHDEM die zahlenden Abonnennten die gedruckte Ausgabe erhalten haben.

Eigentumsvorbehalt: Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme 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.



„Pretty good Piracy“

12. Chaos Communication Congress
- die europäische Hackerparty -

vom 27.-29. Dezember 1995 in Hamburg

im Eidelstedter Bürgerhaus
Alte Elbgastr. 12 / Hamburg-Eidelstedt

Informationen * Diskussionen * Workshops
Chaos-Cafe * Archiv + Fotokopierer * Bild + Funk
Hack-Center * Frauen-Raum * Netzzugangsspielwiesen

	Dauerkarte	Tageskarte
Normal	42.- DM	20.- DM
Schüler / Arbeitslose	36.- DM	12.- DM
Mitglieder d. CCC e.V.	23.- DM	10.- DM
Journalisten	75.- DM	
Gewerbl. Teilnehmer	100.- DM	

Aus organisatorischen Gründen ist eine Voranmeldung durch Überweisung auf das Kto 59 90 90 - 201 bei der Postbank Hamburg (BLZ 200 100 20) für uns hilfreich (nicht zwingend) - bitte Beleg mitbringen.

Vorabinformation gegen 3 * 1.- DM Rueckporto beim CCC in Hamburg
oder über die Usenet-Group de.org.ccc sowie Datex-J *CCC#

Veranstalter:

Chaos Computer Club e.V.
Schwenckestr. 85 D-20255 Hamburg ccc@t42.ppp.de
Tel. 040-4903757 Fax. 040-4917689 http://www.ccc.de/

in Kooperation mit:

Chaos Computer Club Berlin e.V.
Neue Schönhauser Str. 20 D-10178 Berlin cccb1n@artcom.de
Tel. 030-22661155 Fax. 030-22661156 Treff: Di 20 Uhr

FoeBuD e.V.
Marktstr. 18 D-33602 Bielefeld foebud@bionic.zer.de
Tel. 0521-175254 Fax. 0521-61172 Mo-Fr 17-19 Uhr

Sämtliche personalisierte Wesenssammelbezeichnungen verstehen sich als weiblich, männlich und neutral



„Sicherheit“ von EC-Karten

Bereits seit Einführung der EC- oder auch EuroCheque-Karten gibt es das Problem des EC-Kartenmißbrauchs. Anders als bei Kreditkarten, wo bereits die Kenntnis der Kreditkartennummer zusammen mit dem Verfallsdatum genügt um z.B. Versandhausbestellungen zu tätigen, läuft der Mißbrauch hier etwas aufwendiger ab. EC-Karten dienen zum einen dem Nachweis, dass die Unterschrift auf dem EC-Check echt sowie der Benutzer gleich dem Inhaber ist - zum anderen zusammen mit dem 4 stelligen PIN-Code der Möglichkeit, an den europaweit vorhandenen EC-Automaten Geld abzuheben.

Die Höhe des pro Vorgang abhebbaren Betrages hängt dabei ebenso wie andere Eckdaten und PIN-Code von den auf dem Magnetstreifen der Karte gespeicherten Daten ab. Auch wenn das Auslesen der Daten vom Magnetstreifen einer EC-Karte nach Ansicht der Banken ein Ausspähen von Daten nach Paragraph 202a (2. WiKg: Ausspähen von Daten) darstellt, weil die Karte nicht dem Inhaber sondern der jeweiligen Bank gehört (es handelt sich also um bankinterne Informationen) ist sowohl bekannt, welche Daten auf dem Magnetstreifen gespeichert sind - als auch mit welchem Algorithmus der PIN-Code zusammen mit den Daten des Magnetstreifens und weiteren Daten überprüft wird.

Diese Informationen sind im Prinzip öffentlich und z.B. auch durch Einsicht der entsprechenden Patentschriften einsehbar. Allerdings soll es Fälle gegeben haben, in denen aufgrund anderer

Straftatbestände beklagte Hausdurchsuchte des unrechtmässigen Besitzes dieser Unterlagen angeklagt wurden und den „legitimen“ Besitz der Unterlagen darlegen sollten.

Nach Darstellung von Systemersteller und Betreiber ist es mit vertretbarem technischen Aufwand nicht möglich, von den Daten des Magnetstreifens auf den PIN-Code zu kommen.

Aus dieser Behauptung heraus resultieren die Allgemeinen Geschäftsbedingungen für die EC-Karte und das Rechtsverhältnis zwischen KundeIn und Bank. Entscheidender Punkt ist die „Sorgfaltspflicht“ des Kunden für den Umgang mit dem PIN-Code der EC-Karte. Der Kunde ist angehalten, den PIN-Code niemandem mitzuteilen und vor allem ihn niemals zusammen mit der EC-Karte zusammen aufzubewahren. Geht dem Kunden bzw. rechtmässigen Inhaber die EC-Karte nun verloren (bzw. wird sie ihm geklaut) und mit dieser Karte wird Geld abgehoben, muss der Kunde der Bank beweisen, seiner Sorgfaltspflicht nachgekommen zu sein. Konkret muss der Kunde also beweisen, das z.B. in dem ihm geklauten Portemonaie kein Zettel mit dem PIN-Code der Karte war und der PIN-Code auch nicht auf der Karte selbst notiert war.

Auch die sofortige Anzeige des Verlustes durch den Inhaber an Polizei und die Zentralstelle für Kartensperrungen nützt hier wenig: denn auch die Haftung der Bank bzw. des Betreibers greift natürlich nur, wenn der Kunde seiner Sorgfaltspflicht nachgekommen ist.



So liegen der Redaktion Datenschleuder bzw. dem Chaos Computer Club etliche Fälle ratsuchender KundInnen vor, denen die EC-Karte geklaut wurde, unmittelbar danach Geld an verschiedenen Automaten abgehoben wurde und dieses Treiben erst durch Sperrung der Karte beendet wurde.

Der so entstandene Schaden - meist schon einige Tausend Mark - wird von der Bank dem Kunden einfach in Rechnung gestellt: wie sollte den der Täter (Handtaschendieb) an den PIN-Code gelangt sein, wenn nicht durch einen Zettel mit dem PIN-Code in der Tasche bzw. dadurch, dass sie auf der Karte notiert war? Nach Mutmassung der Banken handelt es sich also um einen Fall, in denen der Kunde bzw. die Kundin nicht seiner Sorgfaltspflicht nachgekommen ist.

Besteht das Opfer (KundeIn) nun darauf, dass dieses nicht der Fall war - er bzw. sie also seiner Sorgfaltspflicht nachgekommen sei, stellt die Bank / das Kreditinstitut in der Regel Anzeige gegen den Kunden wegen Falschaussage und Betruges. Der Vorliegende Fall wird dann als „typischer Lügenfall“ bezeichnet, in denen der Kunde lediglich behauptet, dass die Karte entwendet worden sei bzw. seiner Sorgfaltspflicht nachgekommen zu sein um so das entsprechende Geld entsprechend von der Bank zu ergaunern bzw. die Haftung der Bank unrechtmässig in Anspruch nehmen zu wollen.

Vor Gericht sieht sich also der Kunde dann mit der Unmöglichkeit konfrontiert, zu beweisen daß dem entwendeten Portemonaie kein derartiger Zettel beilag bzw. dass er als Kunde schon seiner Sorgfaltspflicht nachgekommen ist -

nur eben der Täter durch die auf Daten auf dem Magnetstreifen auf den PIN-Code gekommen ist.

Das der Kunde zumindest ersteres nicht kann ist wohl klar. Auch der Beweis, dass sich der PIN-Code mit den Kartendaten ermitteln lässt gelang bisher nicht. Fast nicht.

Nach einem Bericht von ARD-Ratgeber Technik, ausgestrahlt am 29.10.1995 hat der Darmstädter Professor Manfred Pausch bereits 1988 in einem Gutachten nahegelegt, dass der PIN-Code „unter bestimmten Vorraussetzungen aus den Daten errechnet werden kann, die auf der EC-Karte gespeichert sind.“ (dpa)

Zumindest in einem Verfahren 1988, in dem Pausch als Gutachter auftrat, wurde die Dresdner Bank verurteilt einer Frau 900 DM zu erstatten, die nach dem Diebstahl ihrer EC-Karte von ihrem Konto abgehoben worden waren (AZ 36 C 4386/87). Dieses Urteil ist allerdings ganz sicher eine Ausnahme zur sonstigen Rechtsprechung. Es gibt mehrere „Standartgutachten“ der Ersteller / Betreiber des Systems, deren Kernaussage die Nichterrechenbarkeit des PIN-Codes aufgrund der mathematischen Komplexität ist (siehe Anhang).

Die in ARD-Ratgeber dargestellte Technik, in denen Pausch einige Daten des Magnetstreifen der Karten auf der X-Achse und die dazugehörigen PIN-Codes auf der Y-Achse eines Koordinationsystems zeigt um auf den Zusammenhang aufmerksam zu machen ist uns - zumindest nach Betrachtung des ARD-Beitrages - nicht klar.



Derweil versuchen wir gerade den besagten Professor Pausch, sein Gutachten und das 1988 erwirkte Urteil zu besorgen - hierzu in der nächsten Datenschleuder mehr.

Neben den technischen Unzulänglichkeiten des Systems (dazu später mehr) gibt es aber noch ein viel gravierenderes logisches Problem, das jedem Grund genug sein sollte, ein EC-Karten Kundenverhältnis zu meiden.

In einem Beitrag von RTL-Extra vom 16.10.1995 wurde die Möglichkeit aufgezeigt, mit einer Mini-Kamera den Kunden dabei zu beobachten, wie er seinen PIN-Code eingibt.

So ist es nicht nur möglich und denkbar, unmittelbar an einem EC-Automaten eine entsprechende Minikamera inkl. Sender etwa in der Gesamtgröße ein 10er Packs 3 1/2 Zoll Disketten anzubringen um dann in einem wenig entfernten PKW den PIN-Code auf einem Videoband aufzuzeichnen und in Zusammenarbeit mit einem Handtaschenräuber mit der EC-Karte schnellstmöglich Geld abzuzocken.

Der PIN-Code wird ja neuerdings nicht nur an EC-Automaten selbst, sondern auch an sogenannten POS-Terminals (Point of Sale) eingegeben - z.B. in Tankstellen, Warenhäusern und anderen Verkaufsstellen. Es soll Fälle gegeben haben, wo bestochene Tankstellenwärter schlicht die Raumüberwachungskamera des Verkaufsraums etwas besser ausgerichtet haben, so dass der sowieso vorhandene Videorekorder die Eingabe des PIN-Codes genau beobachtete. Oder eben eine zweite Kamera entsprechend installiert wurde.

Die Kombination Tankstelle / Taschenräuber ist natürlich unsinnig - wie übrigens auch die Annahme der Täter müsse überhaupt in den Besitz der Karte gelangen. Um den vollständigen auf dem Magnetstreifen der Karte gespeicherten Datensatz zu bekommen genügt es ja, diese kurz in einen zweiten unter dem Tresen befindlichen Magnetkartenleser durchzuziehen „zu Sicherheitszwecken“ (so das Beispiel im RTL-Beitrag) bzw. einfach den Datensatz zwischen POS-Terminal und Kasse mitzuprotokollieren (unauffälliger ist das...).

Für den so erlangten Datensatz samt PIN-Code gibt es zwei Verwendungsmöglichkeiten. Zum einen lässt er sich mit dem entsprechenden Know-How auf eine andere EC-Karte kopieren und an deutschen Automaten zum Abheben von Geld benutzen - das in einem deutschen Automaten vorhandene MM-Modul prüft zwar das optische <?> MM-Merkmal auf der Karte, lässt sich aber mit entsprechendem Know-How (Kombination zu Daten auf dem Streifen) auch dazu überreden, eine andere EC-Karte als echt zu bezeichnen. Die andere Möglichkeit ist, dass die Daten schlicht auf eine weisse Blanko-Karte kopiert werden (EDV-Grosshandel, Stück ca. 30 Pfennig) und an einem ausländischen (im RTL-Beitrag an einem holländischen) Automaten eingesetzt werden, der besagtes MM-Modul zur Echtheitsprüfung nicht hat.

Das Problem bei der Möglichkeit, den PIN-Code auszuspähen - ob die Karte dann entwendet wird oder nicht - ist, dass sie sowohl in den Geschäftsbedingungen als auch in der



Rechtssprechung *nicht vorgesehen ist*. Das heisst - der Kunde kann seiner Sorgfaltspflicht noch so gründlich nachkommen - beweisen kann er es im Zweifelsfall nicht.

Somit - müsste man annehmen - hat dieses Kundenverhältnis einen gewissen sittenwidrigen Charakter. Die Rechtsprechung ist bislang eine andere.

Interessant wäre es darüberhinaus natürlich zu erfahren, wie sich die Entwicklung des EC-Karten-Missbrauchs finanziell niedergeschlagen hat. Für 1994 ist von einem Wert von 100 Millionen Mark für EC-Karten die Rede. Die eigentlich interessante Frage ist natürlich, wie die X/Y-Kurve Zeitraum und Missbrauchshöhe aussieht; gibt es irgendwann einen steilen Anstieg? Und was ist zu diesem Zeitpunkt passiert? Haben sich organisierte Kriminelle massenhaft mit SMD-Kameras ans Werk gemacht? Oder ist es doch jemandem gelungen den PIN-Code mathematisch...?

Zugegebenerweise zählt dieser Artikel die Sicherheitslücken nur unvollständig auf. Auch lässt sich die Sachlage noch etwas gründlicher beleuchten. Um für das grundsätzliche Verbraucherschutzrechtliche Problem eine Lösung anzubieten, arbeiten wir derzeit an einem Gutachten, das Betroffenen bei Gericht entsprechend Unterstützung bieten soll. Mitarbeit und Know-How Zutragung erwünscht.

Mehr zu den technischen Verfahren und zum Modell von Prof. Pausch in der nächsten Datenschleuder.

Andy Müller-Maguhn

Ein paar Quellenverweise zum Thema:

- „PINs und POSsen“ Papier- und bargeldlose Zahlweise per Automat von Armin Gebbert in iX 10/1991

- „Grobe Fahrlässigkeit des Aufbewahrens der

Scheckkarte zusammen mit persönlicher Geheimzahl“ - Sonderbedingungen für den ec-Service Nrn 5.1, 5.2, 9.2 Urteil v. 10.1.1992 - 9U959/91

aus: NJW 1992, Heft 16, Seite 1051/1052 mit Verweis auf BGH, NJW 1992, 445.

- „Gutachten zur Sicherheit von ec-Karten mit Magnetstreifen“ v. Siegfried Herda, Februar 1994, Gesellschaft fuer Mathematik und Datenverarbeitung mbH (GMD), Rheinstr. 75, D-64295 Darmstadt im Auftrag des Landgerichts Köln

- „Geldausgabeautomaten: Der Coup von Köln“ in KES (Zeitschrift für Kommunikations- und EDV-Sicherheit), Jahrgang 2, Heft 1/86 vom 26.1.1986.

- „Bankautomatenraub“ Buch von Wolfgang Ziegler, T. Watter Verlag Regensburg

- „Magnetkartensysteme“ Buch von Michael Gleissner, T. Watter Verlag Regensburg

- „Kartentricks“ - Kreditkarten-Betrug per Computer in: Computer-Live 6/90

- „Magnetkarten“ Normen, Aufbau, Ge- und Missbrauch Von Christian Kiefer in: Elektor 4/93

Die Echtheit der Karte wird vom Terminal (GAA) mittels RSA-Algorithmus nach der Formel

$S(j) = i \exp e \text{ mod } n$

(n = Schlüssel aus 2 Primzahlen)

($i = 2 \times j$)

(j = Verkettung von

Kontonr. (44 BIT)

+ Kartennr. (76 BIT)

+ Gebrauchscode (08 BIT)

+ Gültigkeitsdatum und Ende (32 BIT)

überprüft. Das Terminal liest:

Kontonr. 44 BIT

+ Kartennr. 76 BIT

+ Authentizitätswert (=Offset) und prüft nach

Funktion $P(V) = V \exp 3 \text{ mod } n$ die Karte auf

Echtheit (= PIN Eingabe o.k.?) Sodann wird

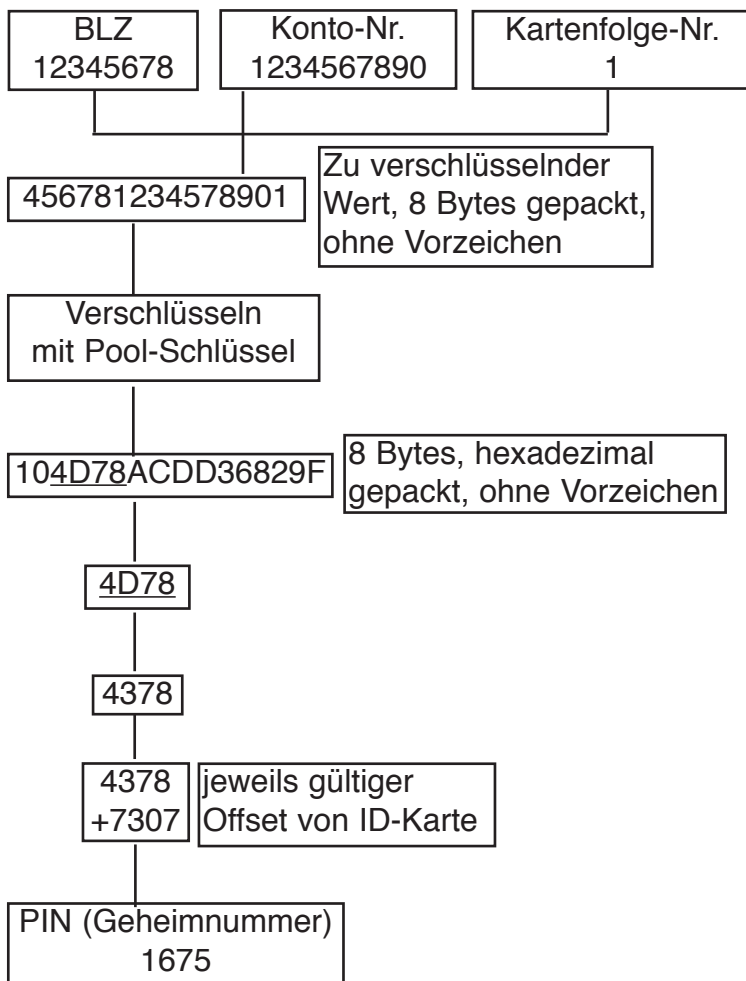
noch die Prüfziffer der PAN berechnet:

Jede 2. Ziffer (von vorne) wird mit 2 multipliziert

alles wird addiert, Rest bis zum nächsten

Zehner = Prüfziffer





Belegung der Spur 3 einer Euroscheckkarte / Bankkundenkarte

B Startzeichen

00 0 Format-Code 01 = internationale Karte
 01 1 00 = nationale Karte
 02 5 Branchen-Schlüssel 59 = EC-Karte
 03 9
 04 Bankleitzahl Clearing Gebiet
 05 Clearing Ort
 06 „
 07 Netzbetreiber
 08 Landeszentralbank
 09 „
 10 Filialnummer
 11 „
 12 D Separator Feldtrenner
 13 Kontonummer
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23 Pruefziffer PAN Pruefziffer fuer BLZ und Kto-Nr.
 24 D Separator
 25 2 Laender-Schlüssel 280 = Deutschland
 26 8
 27 0
 28 9 Waehrungs-Schlüssel 954 = DM
 29 5
 30 4
 31 0 Waehrungs-Exponent Faktor fuer Waehrungsangaben
 32 Limit pro Zyklus maximaler Veruegungsbetrag

33 innerhalb eines festgelegten
 34 Zeitraumes
 35
 36 Restbetrag pro Zyklus noch veruegbarer Restbetrag
 37
 38
 39
 40 Zyklusbeginn Einerstelle des aktuellen Jahres
 41 Tage seit dem 1.1 des Jahres
 42 „
 43 „
 44 Zykluslaenge Angabe in Tagen
 45
 46 3 Fehlbedienungszähler wird mit jeder Fehlbedienung ver-
 mindert
 47 0 Algorithmus-Schlüssel 01 = DES-Schlüssel 48 1
 49 Offset 1 zur Berechnung der PIN
 50
 51
 52
 53 0 Freizuegigkeit 0 = EC 6 = Bank-Card 2 = S-Card
 54 2 Kontoart
 55 0 Benutzereinschraenkung
 56 0 siehe 54
 57 0 siehe 55
 58 0 siehe 54
 59 0 siehe 55
 60 Verfallsdatum Jahr
 61 „
 62 Tag
 63 „
 64 Kartenfolgenummer
 65 Kartensicherungscode als EAN-Code
 66 MM-Verfahren
 67
 68
 69
 70
 71
 72
 73
 74 D Separator
 75 D Separator
 76 1 Nachrichtbeginn
 77 D Separator
 78 Veruegungsdatum
 79
 80
 81
 82 86-PVV (Offset 2)
 83
 84
 85
 86 Offset 3
 87
 88
 89
 90 EC-Sprach-Code
 91 frei fuer Institut
 92
 93
 94 Restbetrag/Tag Restbetrag am Tag
 95 ONL. x 10 bei Online-Verbindung zum
 96 Autorisierungszentrum
 97 Restbetrag/Tag Restbetrag am Tag
 98 OFF. x 10 ohne Online-Verbindung zum
 99 Autorisierungszentrum
 100 Veruegungsdatum Jahr
 101 Institut „
 102 Tag
 103 „
 104 FF EOT
 105 / LRC

Kurzmeldungen

Stimmerkennung bei Calling-Cards

Die US-amerikanische Telefongesellschaft Preferred Telecom Inc. setzt erstmals Spracherkennungssysteme zur Anruferverifikation ein. Die Stimme des Anrufers wird von einem Spracherkennungssystem der Firma VCS (Dallas) analysiert und mit den für seine Calling Card gespeicherten Stimm-Merkmalen verglichen. Die Kartenummer und die anzuwählende Nummer wird bei diesem System nicht getippt, sondern gesprochen. Abzuwarten bleibt, wie sich das System bei einer Erkältung des Anrufers verhält. Zudem ist natürlich kein Schutz gegen illegale Aufzeichnungen gegeben. Sollte sich das System bewähren, ist eine schnelle Verbreitung sowohl im Calling-Card-Bereich als auch z.B. zur Anwahl und Nutzeridentifizierung bei Mobiltelefonen zu erwarten.

Miniruf/Quix

Seit kurzem ist einer der Telekom-Konkurrenten bei Paging am Markt aktiv. Die Miniruf GmbH (Sitz Hannover, 40% Vebacom, 40% RWE, 20% Telecom Danmark) betreibt auf 448,475 MHz 1200/2400 bit/s einen POCSAG-Dienst. Der Service ist in der Grundversion SCALL-ähnlich (anonym, Numerik, keine Grundgebühr, Anrufer zahlt) und in der erweiterten Version Cityruf-ähnlich (personengebunden, auch alphanumerik, Grundgebühr, geringere Anrufpreise, bundesweite Rufzone möglich). Die Rufzonen entsprechen den Vorwahlzonen. Ähnlich

den aus den USA bekannten Paging-Systemen ist bei Quix auch eine persönliche Begrüßung des Anrufers und die Einrichtung einer Voicemailbox möglich. Interessanterweise ist eine Empfängerklasse erhältlich, die ohne weitere Kosten mit den aktuellen dpaprio-1 Schlagzeilen versorgt wird. Die Verteilung der Rufe von der zentralen Annahme in Hannover (0165x) zu den Aussendestationen wird über Satellit (Teleport Europe / RWE) vorgenommen, die Reaktionszeit bis zum Eintreffen des Rufes liegt bei ca. 2 Sekunden (!). Das Gesamtsystem ist von Ericsson, die Zentrale ist mit einer Ericsson AXE-Vermittlung an das Telefonnetz angebunden. Die Datenverarbeitung läuft auf einem SUN-Netz unter Oracle. Die Sprachverarbeitung stammt von Group 2000 (Niederlande). Die Empfänger sind von Motorola und Philips.

(unter Verwendung von TeleTalk 9/1995)

Zweitanschluß mit Erstkündigung

Eine interessante Variante der Gebührenbegrenzung, die zum Jahresende leider ausläuft, ist ein Zweitanschluß, bei dem die erste Rufnummer aus irgendwelchen Gründen gekündigt wurde (Zahlungsunwilligkeit o.ä.). Die Zweitnummer läuft dann nicht selten einfach weiter und kostet netto 10,60 im Monat, was als Grundgebühr ganz erträglich ist.

Studentenschiesser böse auf



Blueboxer

Unklar (crd) - Das längst von vielen totgeglaubte / totgeredete Blueboxing hat zumindest in Verkehrsrichtung von Deutschland via 0130 nach China zwecks Manipulation der dortigen Einrichtungen in einem nicht unbe-trächtlichen Zeitraum mal wieder Ausmaße angenommen, die für die dortigen Stellen nicht akzeptabel sind.

Die durch die Telekom zwecks Verhinderung der Simulation von C5-Signaltönen von der British Telecom eingekauften Filter erwiesen sich offenbar einmal mehr als unzuverlässig, so daß das Problem nur mit entsprechendem Personalaufwand erschlagbar schien. Näheres hierzu demnächst bei den entsprechenden Landeskriminalämtern.

Engländer geben nicht auf

London (crd) - Nach dem nicht wirklich als geglückt zu bezeichnenden diesjäh-rigen Versuch, in London eine Hacker-Konferenz zu machen (siehe Bericht in der letzten Datenschleuder) versucht's nun nochmal wer anders. Ausser, daß sie im April 1996 stattfinden soll, steht allerdings noch nicht viel fest. Infos in alt.ph.uk bzw. alt.hackers bzw. bei Alex McLean: alex@forestbk.demon.c o . u k

Informationsgesellschaft -

Medien - Demokratie

Marburg (crd) - Oben genanntes ist der Titel einer Veranstaltung des Bundes demokratischer WissenschaftlerInnen (BdWi), die vom 19.-21. Januar 1996 in der Universität Hamburg stattfinden wird. Die Themenpalette versucht

offenbar, möglichst alle Aspekte zukünf-tigen Lebens abzudecken, die Träger repräsentieren ebenso ein breites Spektrum. Nähere Informationen gibt es beim BdWi, Postfach 543, D-35037 Marburg, Tel 06421-21395, Fax 06421-24654 bzw. bei Rainer Rilling: rillingr@mail.uni-marburg.de

Chipkarten immer noch nicht abgeschafft

Berlin (crd) - Obwohl die angebliche Sicherheit von Chipkarten durch die Simulation derselben (siehe Titelbild dieser Datenschleuder) hinreichend ad absurdum geführt worden sein sollte, wird sie immer noch als DAS sichere Medium schlechthin für zukünftige elektronische Geldbörsen, Krankenkassenkarten etc. angesehen. So widmet sich die „Multicard '96“ auch dem Thema „Chipkarte im Alltag - Anwendungskonzepte und Verbraucherschutz“ (vom 10.-12. Januar 1996 im Berliner Grand Hotel Esplanade). Eintrittspreis 2550 DM, Einschränk-ungen im Realitätsgehalt lediglich durch Befürwortung dieses Unsinn bedingt, Abendempfänge mit Buffet und Cocktails inklusive. Informationen: inTIME Berlin, Seesener Str. 53, D-10711 Berlin, Tel 030-8929763 Fax 030-8932848.

Anis-Bug dann doch mal abge-schaltet

Berlin (crd) - Nachdem wir bereits auf dem Chaos Communication Congress 1994 den Leiter des Privatkundenvertriebs Klaus Busch auf den ANIS-Bug aufmerksam gemacht hatten, hat die Telekom es nach einem dreiviertel Jahr tatsächlich hingekriegt,





einen ziemlich groben Fehler zu beheben. „ANIS“ (Analoge Teilnehmer an ISDN-fähigen Vermittlungsstellen) sollte es Telefonteilnehmern, die an einer modernen digitalen Vermittlungsstelle angeschlossen sind ermöglichen, ISDN-Leistungsmerkmale zu nutzen, wie das Makeln zwischen zwei gleichzeitig geführten Gesprächen und das „Anklopfen“ bei einem Teilnehmer, wenn er bereits ein Gespräch führt. Wenn beim Makeln zwischen zwei Teilnehmern in einer bestimmten Reihenfolge die Gesprächspartner auflegten, konnte man auf einmal ein Gespräch zwischen anderen Teilnehmern belauschen, die hiervon nichts bemerkten. Nach acht Monaten und einigen Presseerwähnungen wurde dann eine neue DIV-Software auf die fehlerbehafteten Ortsvermittlungsstellen von Siemens aufgespielt - interessanterweise wurde die Software zunächst auf der DIV eingespielt, auf der dieser BUG von einem CCC-Mitglied entdeckt wurde. Bis zum nächsten Fehler dann..

Pornotorische Correctness mit Corel Draw

Amerikanischer Puritanismus findet sich in Lizenzvereinbarungen mit USA-Software. So heißt es in der deutschen Version von Corel Draw 4.0 unter Punkt C in den 'Lizenzvereinbarungen' wörtlich: „Sie dürfen nicht: anstößige, obszöne oder moralisch verwerfliche Arbeiten anfertigen, bei denen Sie die zu diesem Programm gehörenden digitalen Bilder verwenden.“ Irgendwer sagte einmal: „Was darf Satire? Alles!“ In diesem Sinne sucht der CCC Bildsatiren, die die zu Corel Draw 4

gehörigen digitalen Bilder originell und kunstvoll verfremden. Nur so kann einem Anbieter, der sich den USA-Fundamentalisten der WASP-Ideologie unterwirft, verdeutlicht werden, daß die EMRK (Europäische Menschenrechtskonvention) stärker ist als WASP-Vorschriften. Übrigens hat der Kreuzfundi Leo Kirch in seinem Sender Pro7 am 31.10.1995 einen Beitrag zur „Bravo“ bringen lassen. Darin ging es um ein drohendes Verbot der Jugendzeitschrift wegen Verbeitung pornografischen Gedankengutes an Jugendliche. Das ist keine Satire, sondern Ernst. Eine Nummer wurde bereits verboten, weil ein Mädchen mit den Worten: „...wir haben auch andere Stellungen ausprobiert, so die 69...“ zitiert wurde. Nach Auffassung des Zensors ist das bäh. (c) 95 by Wau Holland - Text ab 20.12.1995 frei nach GNU GPL

Ladenhüter Lemming '95

(/emp)

Pastellblaues Blei ziert Regale und Paletten bei den Kistenschiebern aus der Bitbedarfsartikelbranche. Händler, die Windows '95 für 153 DM bei Palettenabnahme einkauften, warteten trotz Frühöffnung vergeblich auf kaufwütige Lemminge. Das winzigweiche Marketing in Deutschland brachte keine Gratis-BILD-Zeitung am Erstverkaufstag mit einem Ganzfoto des Gurus Gates und eingebautem singenden Gummibärchen analog zum Musikchip der Glückwunschtelegramme. Große Palettenhüter stoppten das START!-Programm und verkauften das Pastellblei für 149 DM, vier Mark unter Einkauf, getreu dem Motto:



„Mindesthaltbarkeitsdatum 31.12.95“
 „Jetzt bin ich froh, daß ich nicht mehr bestellt habe, sonst könnte ich aus Liquiditätsgründen meinen Laden dicht machen,“ zitiert die nicht für Endverbraucher gedachte Zeitschrift „Computer Business 39/95“ einen Händler. Ein anderer verkauft Windows '95 nur, damit seine Kunden nicht woanders hinrennen müssen. Weiter sagt er: „Viele Anwender handeln nach dem Motto: ‘Never touch a running machine’. [...] Meine Kundschaft setzt sich vor allem aus einem gesetzteren Publikum zusammen, also keine Kids und Computerfreaks, und von denen stellt einfach keiner um. Das wollen sich die Leute einfach nicht antun.“ Ein Fachhändler: „Das Programm ist ein Speicherfresser ohne Ende und nudelt ständig auf der Festplatte rum. Weder ich noch meine Kunden sind begeistert. [...] Ein Großteil meiner Kunden hat Probleme mit der Installation. Manche haben Windows'95 sogar schon wieder von der Platte entfernt. [...] denke [...] ernsthaft darüber nach, ob ich mich nicht wieder stärker auf OS/2 konzentrieren soll.“ Ein Indianer übersetzt Windows: „Weißer Mann, sitzend vor Sanduhr.“
 (c) 95 by Wau Holland
 Text ab 20.12.1995 frei nach GNU GPL

Bit-Burger TELEKOTZ

Die amtliche Behörde der Postbeörde TELEKOM hat ein neues Vorbild gefunden bei der Hamburger-Reklame von Ronald Mac Donald. „Egal, wo in der Welt Sie McDonald's antreffen.“ zitiert die Wirtschaftswoche 43/95 TELEKOM-Vorstand CF Meißner, „Sie wissen immer, wie das Restaurant

gemanagt wird, wie der Hamburger schmeckt und Sie kennen sogar den Preis.“ Weiter wird Meißner zitiert mit: „Wir wollen das McDonald's der Telekommunikation werden.“ Ein extrafeuchter Traum, denn schon ab 1.1.96 wird viel Online-Usern ihr telekommischer „Bit-Burger“ nicht im Hals stecken bleiben, sondern sie gehen woanders hin... Das ,t,e,l,e,k,o,m,a, hat in Kenntnis des CCC-Vorschlags „Nulltarif von Null bis vier“ eine so absurde Kostensteigerung für Onliner dahergelugnet. Nun werden auch Bötsch-Notbremsversuche bei ausgebauter ABS das Hinschleudern der Infobahnfahrer zur Datennetz-Konkurrenz kaum noch verhindern.
 (c) 95 by Wau Holland
 Text ab 20.12.1995 frei nach GNU GPL

Telekom Kunden mit mehr Rechten

Der Regulierungsrat beim BMPT hat am 23.10.95 bessere Kundenschutzregelungen für Telekom-Kunden beschlossen. Kernpunkte sind ein u.a. Zurückbehaltungsrecht bei Unklarheiten mit der Telefonrechnung, das Recht auf eine Durchschnittszahlung bei überhöhten unklaren Rechnungen und Regelungen für den Zugang zu Mietleitungen für den Aufbau eigener Netze. Des weiteren gab Bötsch bekannt, das die T an einer Tariflösung für Online-Nutzer arbeitet, was wohl auf das Family- and Friends Konzept hinauslaufen wird.



Titelbild

Bonn (crd) - Nachdem lange Zeit von der Telekom keine Aussage zur Problematik der gefälschten Telefon-Chip-Karten zu bekommen war, liegt nunmehr eine vor. Unter der Überschrift „Hunderprozentige Sicherheit gibt es nicht“ kommt die Telekom der CCC-Argumentation nach zehn Jahren anmählich entgegen. Wenn die Telekom in dieser Geschwindigkeit weiterlernt, wird Sie etwa im Jahre 2005 einsehen, dass Sicherheit nicht nur unvollkommen auftritt, sondern eine vollständige Illusion ist. Fragwürdig bleibt eine andere Aussage des Verantwortlichen Technik-Netze Vorstandsmitglied Gerd Tenzer: das „sofort alle Karten mit verdächtigen Seriennummern gesperrt [wurden]“ können wir zumindest nicht bestätigen. Ansonsten verlässt sich die Telekom auf die Sicherheit des Eurochips: „Es handelt sich dabei um einen Chip, der mit einem kryptologischen Verschlüsselungsverfahren arbeitet. Sie sind nach heutigen Erkenntnisstand nicht zu entschlüsseln.“ Kommentar eines breit grinsenden Hackers: „Naja, nach dem Erkenntnisstand eines Herrn Tenzer bestimmt nicht.“

Shit happens: Nach Redaktionsschluss erreichte uns noch folgende Nachricht:

„Generalsekretär“ des CCC Frankreich war seit 1983 Spitzel des DST

Jean-Bernard Condat, der Gründer des CCCF wurde offenabr 1983 vo der DST (Direction de la Surveillance du Territoire, etwa dem FBI vergleichbar)

angeworben. Die DST organisierte und bezahlte seine Teilnahme an diversen Hackerveranstaltungen im Ausland und entschied 1989 das Condat nun für größere Aufgaben eingesetzt werden solle. Der CCCF wurde auf Anweisung der DST von Condat gegründet, sein Image in der Öffentlichkeit gezielt erarbeitet um Condat zum Anziehungspunkt für die französische Hackerszene zu machen. Diverse Aktivitäten des CCCF wurden von der DST finanziert. Condat half tatkräftig bei den Ermittlungen zu den Hackings bei den Firmen Thomson und Pechiney im Jahre 1991. Bei Fernsehshows ließ er sich die Antworten auf Fragen von seinem Führungsoffizier ins Headset diktieren. Condat gab zu 52 Monate direkt für die DST gearbeitet zu haben und in dieser Zeit mehr als 1000 Berichte abgeliefert zu haben. Er behauptet 1991 mit der DST gebrochen zu haben und demnächst seine Version der Geschichte veröffentlichen zu wollen. Condat arbeitet momentan als Sysop für das France-Forum bei `C o m p u s e r v e .` Quelle: Intelligence Newsletter, 12.10.1995, Bezug auf „Guerre dans le Cyberspace, Internet et les Services Secrets“, Jean Gisel, Editions La Decouverte (ISBN 2-7071-2502-4) Fast unbemerkt von der Öffentlichkeit



RSA nicht mehr sicher?

ist ein gewaltiger Durchbruch auf dem Gebiet der Faktorisierung gelungen. Erstmals wurde ein Verfahren entwickelt, mit dem eine Zahl mit nur polynomiellem Aufwand in ihre Primfaktoren zerlegt werden kann. Die Grundidee ist dabei die Verwendung von Computern, deren Gatter auf Atomgröße reduziert werden. Dieses als „Quantum Computing“ bezeichnete Verfahren benutzt die Wellenfunktion des Computers (der aus einem „Haufen Atome“ besteht) zur Berechnung und macht dabei von der Tatsache Gebrauch, daß, solange man den Prozeß nicht beobachtet, alle Quantenzustände gleichzeitig ablaufen und damit die Berechnung für alle Quantenzustände gleichzeitig durchgeführt wird. Dadurch wird eine Parallelität erreicht, die exponentiell mit der Anzahl der beteiligten Teilchen wächst. Sämtliche NP-Probleme lassen sich damit mit einer polynominellen Anzahl von Teilchen in polynomineller Zeit lösen.

Ein Verfahren zur Faktorisierung von großen Zahlen mit Hilfe von Quantum Computing wurde von P.W. Shor entwickelt (<http://vesta.physics.ucla.edu/~smolin>). Da alle derzeit als sicher geltenden Public-Key-Verfahren auf der Komplexität des Faktorisierungsproblems bzw. auf dem äquivalenten Problem des diskreten Logarithmus basieren, muß man sich die Frage stellen, wie lange man noch Public-Key-Kryptographie als sicher betrachten kann. Doch vorerst besteht kein Grund zur Sorge: technisch ist das Verfahren von Shor auf absehbare Zeit nicht beherrschbar. Trotzdem sollte man sich jedoch bereits jetzt über Kryptographie mit Hilfe von Quanteneffekten Gedanken machen. Quelle: Science, Vol. 270, October 13, 1995, pp. 255-261, „Quantum Computation“, David P. DiVincenzo

Geschichten von den Nachbarn

Es begab sich zu einer Zeit, daß das große Land Hcierknarf seinem pubertierenden Häuptling Carihc gestattete, auf den Fernen Inseln mit großen Bomben zu spielen, weil er Probleme mit den allgemeinen Annahmen über die Dimensionen seines Phallus hatte. Alle anderen Länder, deren Häuptlinge schon eingesehen hatten, daß sich solche Probleme nicht wirklich mit Keulenschwingen, Brüllen und Umherstampfen lösen lassen, waren zwar besorgt ob der Jähzornigkeit und des Starsinns ihres Häuptlingsbruders, runzelten aber nur die Stirn und murr-

ten leise. Die Untertanen des Großen Häuptlings Carihc waren in der Mehrzahl nicht gewillt, ihren Führer auf die Schädlichkeit seines Tuns hinzuweisen. So beschlossen die Völker in der Nähe der Fernen Inseln, ein großes Geschrei zu entfachen und mit ihren Kanus zu den Fernen Inseln zu rudern, um den Häuptling Carihc an seinem schändlichen Tun zu hindern. Die Besten Helden aus den Nachbarvölkern Hcierknarfs beschlossen, den fernen Brüdern zur Hilfe zu eilen und auch mit ihren Kanus zu den Fernen Inseln zu fahren. Auch gedachten die Helden der



Rauchwölkchentelegrafie im Kalten Land am kleinen Stinkeflüßchen, als Mahnung für die Menschen in Hcierknarf ihre Brüder in aller Welt aufzurufen, viele kleine Rauchwolken zu der Hütte des Häuptlings Carihc zu senden, auf daß er nicht mehr atmen könne vor lauter Qualm und ablasse von seinem schändlichen Tun. Sie redeten mit den Herolden, auf daß ihr Aufruf verkündet werde allem Volke. Die Herolde gingen hin und trugen den Aufruf unter die Menschen. Nun waren aber die Menschen träge und faul. Sie wollten nicht vor ihre Hütte gehen, ein Feuer entzünden und die Rauchwolkendecke schwingen, auf das die Rauchwölkchen zur Hütte des Häuptlings Carihc schwebten. Die Helden der Rauchwölkchentelegrafie sahen dies und waren sehr besorgt. Sie setzten sich in einer Hütte zusammen und palaverten lange und intensiv. Nach vielen Stunden und vielen wohlriechenden Wölkchen die aus der Hütte entwichen waren, hatten sie eine Lösung gefunden: Die automatische Rauchwölkchen-zum-Häuptling-Carihc-Versende-Maschine (tm). Flugs gingen sie hin und bauten die Maschine in großer Zahl um sie kostenlos unter allem Volke zu verbreiten. Nun waren aber die Menschen in ihrer Mehrzahl sogar zu faul, sich die kleine automatische Rauchwölkchen-zum-Häuptling-Carihc-Versende-Maschine (tm) vor die Hütte zu stellen. Die Helden der Rauchwölkchentelegrafie waren darüber sehr betrübt und liessen nach in ihrem Schwunge. Sie wandten sich anderen Dingen zu und der Häuptling Carihc spielte immer noch mit seinen

B o m b e n .

Adressen

CHAOS-HH – CCC Hamburg

Treff jeden Dienstag ab 20 Uhr in den Clubräumen bzw. Restaurant gegenüber. Adresse siehe Impressum.

CHAOS-B - CCC Berlin

Treffen jeden Dienstag ab 20 Uhr jetzt in der Neuen Schönhauser Str. 20, D-10178 Berlin-Mitte (S-/Tram-Hackescher Markt) ganz oben. Kontakt: cccb1n@artcom.de

CHAOS-HL - CCC Lübeck

Treff am ersten und dritten Freitag im Monat, 19 Uhr in der Röhre (gerade Querstraße, geht von der Mengstraße ab). Briefpost: CCC-HL, c/o Benno Fischer, Bugenhagenstr. 7, D-23568 Lübeck, Voice +49 (451) 34799, Mailbox Mafia +49 (451) 31642.

CHAOS-SüdThür

Treffen demnächst in Illmenau. Briefpost CCC-SüdThür Arnstädterstr. 26/7, 98693 Martinroda, Voice +49 (3677) 790556, Fax +49 (3677) 790558

CHAOS-Ulm - Treffen jeden Mittwoch, 19 Uhr im Café „Einstein“

SUECRATES - Stuttgarter Computerrunde mit Zeitschrift d'Hacketse. Kontakt: T.Schuster, Im Feuerhaupt 19, D-70794 Filderstadt, e-mail: norman@delos.stgt.sub.org

2600 Magazine - Amerikanische Hackerzeitschrift

Overseas \$30 individual, \$65 corporate. Back issues available for 1984-88 at \$25 per year, \$30 per year overseas. Adress all subscription correspondence to: 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0099. Office Line: +1 (516) 751-2600, Fax +1 (516) 751-2608

Foebud-BI - Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V., Bielefeld Treffen jeden Dienstag, 19:30 Uhr im Cafe „Spinnerei“, Heeperstrasse 64, dort voice: +49 (521) 62339 Monatl. „Public Domain“-Veranstaltung; Themen und Termine siehe Mailbox BIONIC. Voice: +49 (521) 175254, Fax +49 (521) 61172, Mailbox BIONIC +49 (521) 68000. FoeBuD, Marktstraße 18, D-33602 Bielefeld, e-mail: zentrale@bionic.zer.de

CHAOS-L: Chaos Computer Club Leipzig

noch nicht offiziell – aber irgendwie doch in Gründung. Mails an ccc@t42.ppp.de werden weitergeleitet. Näheres auf dem Kongress?



Chaos Computer Club e.V.	Vorname _____	B E
Schwenckestr. 85	Name _____	S T
D-20255 Hamburg	Strasse _____	E L
Telefon + 49-40-4903757	PLZ, Ort _____	L F
Telefax + 49-40-4917689	Telefon _____	E T
		Z E
		N -

FÜLL AUS, IF Überweisung THEN fax:=vaild
Version 27B/6-1 ELSE einschicken + V-Scheck or money

Mitgliedschaft im Chaos Computer Club e.V. - Abo in Mitgliedschaft inklusive

___	___	1,- DM Satzung des Chaos Computer Club e.V.
___	___	20,- DM Einmalige Verwaltungsgebühr bei Eintritt
___	___	120,- DM Normal-Jahresbeitrag. Dauerauftragalternative: 10,- pro Monat
___	___	60,- DM Sozial-Jahresbeitrag. Dauerauftragalternative: 5,- pro Monat

Datenschleuder Abonnement für 8 Ausgaben, erscheint vierteljährlich

___	___	60,- DM Abonnement, Normalpreis
___	___	30,- DM Abonnement, Sozialpreis

Bücher bzw. diverse Druckschriften

vergr.	33,33 DM	Die Hackerbibel, Teil 1 (260 Seiten A4), Erstellung 1981-1985
vergr.	33,33 DM	Die Hackerbibel, Teil 2 (260 Seiten A4), Erstellung 1985 - zur Zeit vergriffen
___	___	7,50 DM CCC-Studie für die Grünen über politische Computereinsatz
___	___	16,00 DM Elektronische Informationssystem für den Umweltschutz
___	___	5,00 DM Dokumentation zum Tod von „KGB“-Hacker Karl Koch
___	___	20,00 DM Zerberus-Mailbox-BenutzerInnen-Handbuch
___	___	50,00 DM „Lock Picking“ Dokumentation über das Öffnen von Schlössern
___	___	15,00 DM Dokumentation zum Chaos Communication Congress '93

Werkzeug zur Wahrnehmung informationeller Selbstbestimmung

___	___	25,00 DM Sammlung von Verschlüsselungsprogrammen, neues PGP + Handbuch
-----	-----	--

Aufkleber, spritzwassergeschützt, wunderschön und überhaupt

___	___	3,33 DM 3 Aufkleber Chaos-Knoten + „Kabelsalat ist gesund“
vergr.	5,00 DM	15 Aufkleber „Achtung Abhörgefahr“ - auch für Mobiltelefone
vergr.	5,00 DM	Bogen mit Postknochen-Aufklebern verschiedener Größe
vergr.	5,00 DM	Bogen mit 10 Aufklebern „globales Dorf - rechtsfreier Raum“
vergr.	5,00 DM	Bogen mit 15 A023/042Z Zulassungszeichen
___	___	5,00 DM Bogen mit 64 Aufklebern „Chaos im Äther - ich höre zu“

__X	___	5,00 DM Portopauschale
->	___	Der Sozialtarif gilt für Schüler und minderbetuchte Studenten etc.
->	___	Da unser Versandpersonal ehrenamtlich tätig ist, bitten wir um Verständnis für Lieferzeiten bis zu max. 6 Wochen

_____ DM Gesamtbetrag (bitte die Portopauschale, und bei Mitgliedschaft die Verwaltungspauschale NICHT vergessen)

___	___	Bargeld anbei	___	___	V-Scheck	___	___	Überweisung auf Konto 599090-201
								Postbank Hamburg (BLZ 200 100 20)
								erfolgt am: _____.

Eingang

Betrag erhalten

Erledigt:

