MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 47/1986

Fachschaftstagung Mathematik des Cusanuswerks 1986

Kryptographie

24.10. bis 28.10.1986

Die Tagung fand unter Leitung von Frau Benita Plassmann (Göttingen), Frau Ursula Rullich (Willich-Anrath) und Herrn Georg Heeg (Dortmund) statt.

Die Fachschaftstagungen sind ein Teil der Bildungsarbeit des Cusanuswerks, Bischöfliche Studienförderung, "bei denen in Zusammenarbeit mit kompetenten Fachleuten Spezialprobleme einer einzelnen Disziplin oder Grenzfragen mehrerer Wissenschaften erörtert werden. ... Sie bieten in besonderer Weise Gelegenheit der Zusammenarbeit von Stipendiaten und Altcusanern", *) da neben Studenten, die vom Cusanuswerk gefördert werden, auch ehemalige Stipendiaten an den Fachschaftstagungen teilnehmen.

Das Thema wurde mit eingeladenen Vorträgen in fünf Schwerpunkten behandelt:

- Einführung in die Kryptographie
- aktuelle mathematische Probleme der Kryptographie
- Geschichte der Kryptographie - insbesondere im Zweiten Weltkrieg
- Anwendung von kryptographischen Methoden im öffentlichen und privaten Bereich heute
- Probleme der ethischen Verantwortung

Es nahmen an der Tagung 9 Studenten und 15 ehemalige Stipendiaten des Cusanuswerks teil.

Die einzigartige Atmosphäre und die hervorragend ausgestattete Bibliothek des mathematischen Zentrums haben sich auf die Qualität unserer Tagung sehr positiv ausgewirkt und ließen bei den Teilnehmern den Wunsch entstehen, die Tagungen der kommenden Jahre wieder in Oberwolfach durchzuführen.

*) Jahresbericht des Cusanuswerks 1985, S. 10

Vortragsauszüge

Th. Beth und A. Beutelspacher: Einführung in die Kryptographie

Eine Nachricht soll von einem Sender zu einem Empfänger übermittelt werden. Diese Übermittlung soll gegen Störung, Verfälschung und Abhören gesichert werden. Sei M eine Menge von Nachrichten, C eine Menge von Chiffretexten, $E: M \to C$ und $D: C \to M$ Abbildungen mit $\forall m \in M: D(E(m)) = m$. Dann heißt (M, C, E, D) Chiffrierung. Ein Entschlüsselungsangriff (Kryptoanalyse) versucht D, bzw. aus gegebenen $E(m)$ m zu erraten. Sei S eine Menge von Schlüsseln und $\Gamma: S \to C^M \times M^C$, so daß $\forall s \in S$ gilt: $(M, C, \Gamma_1(s), \Gamma_2(s))$ ist eine Chiffrierung. Dann heißt $K = (M, C, S, \Gamma)$ Kryptosystem. Im Folgenden sei A ein Alphabet und $M = C = A^*$ die Menge aller endlichen Wörter über A. Eine buchstabenweise Verschlüsselung heißt alphabetisch; ist sie positionsunabhängig, heißt sie monoalphabetisch (Beispiel Caesar), sonst polyalphabetisch (Beispiele Viginère, one timepad (unentschlüsselbar)). Statistische Verfahren über Häufigkeiten von Buchstaben und Buchstabengruppen sind das wesentliche Mittel der Kryptoanalyse.

H. Rohrbach: Verschlüsselung und Entschlüsselung: Eine Systematik der Verfahren zur Zeit des zweiten Weltkriegs

I. Ersetzungsverfahren (alphabetische Chiffrierungen) haben die allgemeine Form $g_i \equiv t(k_i) + s(\vec{k_i}) \bmod n$, wobei g_i: i-ter Geheimtextbuchstabe, k_i: i-ter Klartextbuchstabe, $\vec{k_i} = k_1 \cdots k_i$, $n = |A|$: Länge des Alphabets, $t: A \to A$: eine Permutation und $s: A^* \to A$. Spezialfälle: $s(\vec{k_i}) = s(i)$: Spaltenverfahren, $s(\vec{k_i}) = s$: Tauschverfahren (monoalphabetische Chiffrierung), $t(x) = x$ und $s(\vec{k_i}) = s$: Additionsverfahren (Caesar). **II. Versetzungsverfahren** permutieren den Klartext. Beispiele sind der Würfel und der Doppelwürfel. Bei **III. Codeverfahren** werden in einem Wörterbuch wichtige Worte Buchstabengruppen zugeordnet. **IV. Kombination von Verfahren** wurde eingesetzt durch Überschlüsselung von im Codeverfahren verschlüsselten Texten. Auch das auf Jefferson zurückgehende Streifenverfahren gehört in diese Gruppe. Es wurde im Zweiten Weltkrieg von den USA benützt und von der Rohrbachgruppe geknackt. Bei **V. Kulissenverfahren** werden Buchstaben durch Bitmuster dargestellt (Fernschreiber, Morsealphabet o. ä.). Durch ein Versetzungsverfahren auf der Bitebene entsteht die Buchstabenfolge des Geheimtextes. Zwei **VI. Chiffriermaschinen** wurden eingesetzt: Die deutsche Enigma realisiert ein periodisches Spaltenverfahren und die schwedische Hagelin beruht auf einer Kombination von 26 Tauschverfahren. Für **VII. Fernschreibmaschinen** existierte ein der Hagelin ähnliches Verfahren jedoch auf einem 32-elementigem Alphabet. **VIII. Sprachverschlüsselung** spielte aufgrund der technischen Beschränkungen (analoges Signal) nur eine untergeordnete Rolle mit Störtonüberlagerung, Versetzung nach Zerschneiden von Bändern und Ersetzungsverfahren nach Fourieranalyse.

H. Rohrbach: Eulers Logogryph

In einem Brief an Goldbach 1714 findet sich ein verschlüsselter Text mit den Angaben: Der Klartext sei lateinisch und die Dechiffrierabbildung monoalphabetisch. Eine Buchstabenhäufigkeitsanalyse ergibt, daß Homophone vorkommen müssen, da im Chiffretext 27, in lateinischen Texten jedoch nur 22 Buchstaben benutzt werden. Die Betrachtung von sich wiederholenden Buchstabengruppen ermöglicht Vermutungen über Homophone. Durch Identifizierung von fünf Buchstabenpaaren lassen sich e und i entschlüsseln. Eine Bigrammanalyse ergibt, daß qu als Einzelbuchstabe verschlüsselt ist, und ermöglicht weitere Identifizierungen. Eine Floskel des Textendes (Zitatstelle) ermöglicht es, die restlichen Buchstaben zu erraten. Der überlieferte Text enthält Fehler.

F.-P. Heider: Komplexitätsbetrachtungen für Kryptosysteme

Gesucht werden Chiffrierungen (M, C, E, D), bei denen es praktisch undurchführbar ist, aus M, C und E D zu berechnen, so daß E veröffentlicht werden kann (public key). Ausgehend vom Satz von Fermat-Euler: $\forall a, n \in \mathbb{N}$: $ggT(a,n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \ mod \ n$, und der speziellen Situation $n = p \cdot q$ mit $p, q \sim 10^{100}$ Primzahlen ist $\phi(n) = (p-1) \cdot (q-1)$. Wähle e, v mit $ggT(e, \phi(n)) = 1$ und $v \cdot e \equiv 1 \ mod \ \phi(n)$. Das Paar (n, v) heißt öffentlicher, e heißt geheimer Schlüssel. Die Verschlüsselung $E(m) \equiv m^v \ mod \ n$ läßt sich mit $D(E(m)) \equiv E(m)^e \ mod \ n \equiv m^{v \cdot e} \ mod \ n \equiv m \ mod \ n$ entschlüsseln (RSA-Verfahren). Die Verschlüsselung und die Entschlüsselung benötigen $O(log \ n)$ Schritte. Geeignete Primzahlen p, q zu finden ist mit Hilfe des Miller-Rabin Tests in polynominaler Zeit möglich. Für die Faktorisierung von n, die für den Entschlüsselungsangriff notwendig erscheint, sind jedoch keine schnellen Algorithmen bekannt. Wählt man jedoch v gleich für mehrere Teilnehmer, so sind Entschlüsselungen über andere Wege möglich.

Th. Beth: Verschlüsselung von gesprochener Sprache bei der Polizei in London

Das Sprachsignal wird in zeitliche Blöcke zerhackt, auf die ein Versetzungsverfahren angewandt wird. Aus Speicherungsgründen wird das Signal dazu in einem Deltaverfahren digitalisiert. Die Permutationen werden über Pseudozufallszahlen bestimmt; denn die Permutation muß ständig wechseln, da Experimente erwiesen haben, daß sich sonst das menschliche Ohr einhört und nach kurzer Zeit die verschlüsselte Sprache versteht. An diesem Beispiel wird das Problem der beschränkten Ressourcen seitens der berufenen und unberufenen Entschlüsseler deutlich. Über aufwendige Frequenzanalyse kann es z. B. gelingen, die richtige Reihenfolge ohne Kenntnis der Permutation zu bestimmen. Speziell im Polizeieinsatz wird jedoch unterstellt, daß der Lauscher nicht über genügend Ressourcen verfügt, um schnell genug zu entschlüsseln.

A. Beutelspacher: Verschlüsselungsprobleme beim Zahlungsverkehr mit der Chipkarte

Zur Zeit wird bei der Fa. Siemens ein Feldversuch vorbereitet, Scheckkarten mit Magnetstreifen durch Chipkarten zu ersetzen. Das wesentliche Problem ist dabei die Authentifizierung. Hierbei stehen nicht die Algorithmen, sondern die Protokolle (d. h. das Wie und Wann des Datenaustausches) im Vordergrund, für die es noch keine Theorie gibt.

F.-P. Heider: Konstruktion sicherer Systeme

Die ISO (International Standard Organization) hat für die Struktur von Kommunikationssystemen ein 7-Schichten-Modell entwickelt: 1. Bittransport, 2. Sicherung, 3. Vermittlung, 4. Transport, 5. Kommunikation, 6. Darstellung, 7. Anwendung. Sicherheitsüberlegungen spielen auf allen Ebenen eine Rolle. Es wurde eine Theorie für sichere Systeme vorgestellt, bei der die Sicherheitsstufen einen Verband bilden. Eine Komponente heißt darin sicher, wenn in ihr Informationen nicht von höheren auf niedrigere Sicherheitsstufen weitergegeben werden können. Informationswege, auf denen Informationen in umgekehrter Richtung fließen können, heißen Guards. Bei der Analyse realer Systeme bilden sogenannte verdeckte Kanäle, auf denen unbeabsichtigt und unbemerkt Informationen fließen, ein großes Problem. Möglichkeiten der Realisierung sicherer Systeme auch im militärischen Bereich wurden als im Moment unwahrscheinlich angegeben.

G. Kongehl: Ethik der Datenverarbeitung

Nach Definition der Begriffe Ethik, Wert und Tugend wurde intensiv die Spemannsche These diskutiert, daß aus humanistischen Überlegungen eine für alle Menschen gültige Rangfolge der Werte gefunden werden kann. Ethische Probleme der Speicherung von Persönlichkeitsdaten liegen im medizinischen, psychologischen Bereich und in der Arbeitssituation. Neben dem unberufenen Zugriff liegen Probleme in der Verknüpfung und Weiterverarbeitung zu anderen Zweckbestimmungen als ursprünglich vorgesehen. Dies kann zu Fehlinformationen und Fehlinterpretationen z. B. bei der Persönlichkeitsbestimmung führen. Eine ähnliche Wirkung kann auch durch Einschränkung der Modellbildungen auf programmierbare Modelle entstehen. Neben der Zunahme der Informationsmenge bewirkt insbesondere der schnelle Zugriff einen erheblichen Machtzuwachs.

Beiträge zu diesem Bericht leisteten Frau Benita Plassmann (Göttingen), Frau Ursula Rullich (Willich-Anrath) und Herr Andreas Könen (Köln). Berichterstatter war Herr Georg Heeg (Dortmund).

Berichterstatter: G. Heeg

Tagungsteilnehmer

Rochus B a u e r
Im Wolfswinkel 13
7800 F r e i b u r g / Br.

Matthias B ü c k e r
Heckenweg 5
7505 E t t l i n g e n 6

Prof. Dr. Thomas B e t h
Hohentwielweg 8
7517 W a l d b r o n n 1

Joachim G e i g e r
Ehingerstr. 19
7900 U l m

Prof. Dr. Albrecht Beutelspacher
Schwalbenstr. 78
8012 O t t o b r u n n

Peter H a n n i g
Rußheimer Str. 2
7500 Karlsruhe-Neureut

Alexander B o c k m a y r
Ebertstr. 49
7500 K a r l s r u h e 1

Georg H e e g
Stortsweg 8
4600 D o r t m u n d 50

Volker B r e c h
Georg-Büchner-Str. 2
6236 E s c h b o r n 2

Dr. Franz-Peter H e i d e r
Martin-Luther-Str. 7
5030 H ü r t h

Christoph B r z o s k a
Habrechtstr. 80
1000 B e r l i n 44

Jürgen J ä g e r
Rotheweg 88
4790 P a d e r b o r n

Klaus K ä m m e r l e

R.-Schirrmann-Str. 14
App. 701

6500 M a i n z

Andreas K ö n e n

Bachemerstr. 51

5000 K ö l n 41

Dr. Gerhard K o n g e h l

Eichenweg 31

7915 E l c h i n g e n 2

Werner K r a n d i c k

Bürgerwehrstr. 30

7800 F r e i b u r g / Br.

Ina L e i ß

Im Kläuerchen 6

6504 O p p e n h e i m

Peter-Michael M i n n e m a

Masbergweg 8

4000 D ü s s e l d o r f 30

Benita P l a s s m a n n

Edith-Stein-Haus
Stauffenbergring 8

3400 G ö t t i n g e n

Prof. Dr. Helmut R i e d e r

Tegernseeweg 21

8580 B a y r e u t h

Thomas R o d a c h

Friedensstr. 14

7500 K a r l s r u h e 1

Prof. Dr. Hans R o h r b a c h

In der Fischzucht 5

8743 Bischofsheim/Rhön

Ursula R u l l i c h

Am Krickerhof 32

4156 W i l l i c h 2
-Anrath

Albert S c h m i d t

Wiesenstr. 86/1

7830 E m m e n d i n g e n

Helmut S c h m i t t
Fr.-L.-Jahn-Str. 7
6370 O b e r u r s e l 5

Michael S c h n o r b a c h
Bahnhofstr. 88
6078 N e u - I s e n b u r g

Theodor S t a r k
Hans-Seibold-Str. 9
8950 K a u f b e u r e n

Hans-Georg U l r i c h
Liebigstr. 21
8025 U n t e r h a c h i n g

Lothar U l s c h m i d
Narzissenstr. 21
8000 M ü n c h e n 21