

Kryptographie - eine mathematische Einführung

Rosa Freund <rosa@pool.math.tu-berlin.de>

03. September 2005

Überblick

- Grundlegende Fragestellungen und Begriffe
- Symmetrische Verschlüsselung: Blockchiffren, Hashfunktionen
- Mathematische Grundlagen: Gruppen, Ringe, Körper, chinesischer Restsatz, kleiner Satz von Fermat.

Grundlegende Fragestellungen

- Eine Nachricht soll nur vom vorgesehenen Empfänger gelesen werden können. Es geht nicht darum, das Lauschen zu verhindern, sondern darum, daß Lauscher die Nachricht nicht entschlüsseln können
- Die Signatur einer Nachricht soll es jedem ermöglichen, die Identität des Absenders zu verifizieren. Gleichzeitig soll es unmöglich sein, eine gefälschte Nachricht mit gültiger Signatur zu erstellen

Allgemeines

Zum verschlüsselten Kommunizieren benötigen die Parteien

- ein Verschlüsselungsverfahren, mit dem ver- und entschlüsselt wird (z.B. PGP, SSL)
- einen Schlüssel, d.h. den Variablen, die das Verfahren benötigt, müssen Werte zugeordnet werden
- z.B. Verschlüsselungsverfahren Cäsarchiffre, Schlüssel ist die Zahl, um die das Alphabet verschoben wird

Effizienz / Komplexität 1

- Ein Verschlüsselungsverfahren heißt effizienter als ein anderes, wenn sein Algorithmus eine niedrigere Komplexität (O-Notation: Maximale Anzahl einzelner Berechnungen) aufweist. Es ist also in der Regel schneller berechenbar.
- Für viele Probleme ist ein Algorithmus mit polynomieller Laufzeit bekannt (z.B. $O(n^2)$). Für andere, einfache Probleme konnten lediglich Algorithmen mit exponentieller Laufzeit gefunden werden (z.B. $O(2^n)$). Allerdings kann bislang nicht bewiesen werden (!), daß für diese Probleme kein polynomieller Algorithmus existiert.
- Es ist also unklar, ob es zwei Klassen von Problemen gibt: polynomiell, und nicht-polynomiell lösbar. Andere Schreibweise: Gilt wirklich $P \neq NP$?

Effizienz / Komplexität 2

- Beispiele: Finde die Primfaktoren einer natürlichen Zahl, Dreifarbenproblem
- Viele Probleme, für die kein polynomieller Algorithmus bekannt ist, sind polynomiell äquivalent. Wird also für nur eins dieser Probleme ein polynomieller Algorithmus gefunden, sind die anderen Probleme auch polynomiell lösbar, und $P = NP$
- Public-Key-Verfahren beruhen meist auf Problemen aus NP . Falls also $P = NP$ gilt, wird ein Großteil der Public-Key-Kryptographie hinfällig.
- Dies ist eher unwahrscheinlich (seit Jahrzehnten wird daran gearbeitet), aber nicht unmöglich.

Symmetrische Verfahren

- Die kommunizierenden Parteien teilen sich einen geheimen Schlüssel (secret key)
- z.B. Blockchiffren, Stromchiffren, Hashfunktionen
- Problem: Schlüsseltausch

Asymmetrische Verfahren 1

- Diffie und Hellman, 1976: *New Directions in Cryptography*
- Es gibt einen öffentlichen sowie einen geheimen Schlüssel (public key, private key), der geheime ist schwer oder garnicht aus dem öffentlichen berechenbar
- Um verschlüsselte Nachrichten erhalten bzw. Nachrichten signieren zu können, generiert A sich einen öffentlichen und einen geheimen Schlüssel
- Wie der Name sagt, muß A ihren geheimen Schlüssel (private key) geheimhalten, den öffentlichen (public key) jedoch veröffentlichen

Asymmetrische Verfahren 2

- Beim Verschlüsseln nutzt B den öffentlichen Schlüssel von A, um eine Nachricht an A zu verschlüsseln. A entschlüsselt die Nachricht mit ihrem geheimen Schlüssel
- Beim Signieren signiert A die Nachricht mit ihrem geheimen Schlüssel. B benutzt As öffentlichen Schlüssel, um die Signatur zu verifizieren

Asymmetrische Verfahren 3

- Sicherheit beruht meist auf algorithmischen Problemen mit hoher (bzw. ungeklärter) Komplexität
- Mathematisch geht insbesondere algebraische Zahlentheorie ein (z.B. diskreter Logarithmus, elliptische Kurven)
- Häufig zum Austausch von Schlüsseln für symmetrische Verfahren genutzt (z.B. SSL), da weniger effizient als symmetrische Verfahren

Vertrauen

- Wenn ich eine Person persönlich kenne, und sie mir ihren öffentlichen Schlüssel selbst übergibt, kann ich ihr vertrauen.
- Problem: Wie kann ich öffentlichen Schlüsseln von Personen vertrauen, die mir nicht persönlich bekannt sind, oder von denen ich die öffentlichen Schlüssel per Mail oder via einem Keyserver erhalte?
- Lösung: Web of Trust und Keysigning.

Kerckhoff-Prinzip

- Auguste Kerckhoff, 1883: *La Cryptographie militaire*
- Sicherheit eines kryptographischen Systems sollte nur auf der Geheimhaltung des Schlüssels beruhen, nicht jedoch auf Geheimhaltung des Verfahrens selbst
- Vorteile: die Qualität des Verfahrens kann intensiver untersucht werden

Blockchiffren

- symmetrisch
- Jede Nachricht wird in gleichlange Blöcke aufgeteilt, die Blöcke werden separat und unterschiedlich verschlüsselt. Der letzte Block wird ggf. mit Bits gepadded
- z.B. DES (1977), AES / Rijndael (2001)

Hashfunktionen 1

- Berechnet für Inputs beliebiger Länge Hashwerte von vorgegebener (meist kurzer) Länge
- Geringe Änderung des Inputs führt zu stark geändertem Hashwert
- Weitere Merkmale: Kollisionsarmut (aber: Geburtstagsparadoxon), nicht umkehrbar, eindeutig

Hashfunktionen 2

- Beispiele: MD5 (seit 2004 bekannt, daß Kollisionsangriffe möglich), SHA-1 (seit Anfang 2005 bekannt, daß Preimageattacken möglich, praktisch noch nicht von Bedeutung), SHA-2 (bislang als sicher eingestuft)
- Anwendungen z.B.: Unix-Paßworte (aber: Dictionary-Attacke), Prüfsummen.

Physikalische Aspekte

- **Quantenkryptographie.** Idee: Ein Nachrichtenstrom verändert sich, wenn er beobachtet wird (\rightarrow Unschärferelation)
- **Quantencomputer.** Die Sicherheit der momentan gängigen Verfahren beruht auf schwierigen Algorithmen (d.h. nicht in polynomieller Laufzeit lösbar), und der Annahme $P \neq NP$. Mit Quantencomputern sind exponentielle Laufzeiten kein Problem mehr. Es wird bereits jetzt an sogenannter „quantum-hard cryptography“ gearbeitet.

Also:

- **Fazit:** Symmetrische Verschlüsselungsverfahren sind viel effizienter (also schneller) als asymmetrische. Problem bei symmetrischen Verfahren: Schlüsseltausch.
- Asymmetrische Verfahren beruhen darauf, daß $P = NP$ unbewiesen ist. Quantencomputer und -kryptographie sind von der Anwendung noch Jahre bzw. Jahrzehnte entfernt.
- **Jetzt:** Mathematische Grundlagen für RSA.

Einwegfunktionen

- Viele mathematische Funktionen sind leicht umkehrbar: $f : x \mapsto (x + 5)/17$,
 $f^{-1} : x \mapsto 17x - 5$
- Für die Kryptographie sind mathematische Funktionen interessant, die nur umkehrbar sind, wenn eine Zusatzinformation bekannt ist (one-way function with trapdoor)
- z.B.: Faktorisierung zweier großer Primzahlen: $f : \mathbb{P} \times \mathbb{P} \rightarrow \mathbb{Z}, (p, q) \mapsto pq$

Mathematische Strukturen 1

- Gruppen, Ringe, Körper sind mathematische Strukturen. Sie bestehen aus einer Menge von Elementen, sowie Verknüpfungen der Elemente. Jeder Körper ist auch ein Ring, und jeder Ring eine Gruppe. Eine Gruppe besitzt nur eine Verknüpfung (in der Regel als $+$ geschrieben), Ringe und Körper besitzen zwei Verknüpfungen (in der Regel als $+$ und \cdot geschrieben).
- Gruppe: zum Beispiel $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) , (Punktgruppe einer elliptischen Kurve, Punktaddition)
- Ring: zum Beispiel $(\mathbb{Z}, +, \cdot)$. Die erste Verknüpfung ist umkehrbar ($7 - 5 \in \mathbb{Z}$), die zweite nicht ($7/5 \notin \mathbb{Z}$). Weiteres Bsp. ist der Polynomring $(K[x], +, \cdot)$

Mathematische Strukturen 2

- Körper: zum Beispiel $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{F}_q, +, \cdot)$
- Wir gehen in diesem Vortrag immer von kommutativen Verknüpfungen aus. Das heißt, es gilt stets: $a \circ b = b \circ a$, wobei \circ eine beliebige Verknüpfung ist.
- Exakte Definitionen: Siehe Arbeitszettel.
Mehr Informationen in beliebigen Algebrabüchern, z.B. Meyberg, Algebra 1.

Endliche Körper

- Endliche Körper mit q Elementen: $\mathbb{F}_q = \{0, 1, \dots, q - 1\}$, wobei gilt, daß q prim oder Primzahlpotenz ist. \mathbb{F}_q wird auch $\mathbb{Z}/q\mathbb{Z}$ geschrieben.
- Gerechnet wird modulo q , wie bei einer Uhr (modulo 12).
- Schreibweise: z.B. in \mathbb{F}_5 : $3 \cdot 4 = 12 \equiv 2 \pmod{5}$. Sprich: „kongruent zwei modulo fünf“.

Chinesischer Restsatz

- Es gilt: $\mathbb{F}_p \times \mathbb{F}_q \cong \mathbb{F}_{p \cdot q}$ (oft so geschrieben: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/p \cdot q\mathbb{Z}$), sprich: „kreuz“, „isomorph“
- Anders formuliert: Seien $p, q \in \mathbb{Z}$ teilerfremd (Primzahlen erfüllen dies in jedem Fall). Seien $a, b \in \mathbb{Z}$ beliebig. Dann gibt es ein eindeutig bestimmtes $N \in \mathbb{F}_{pq}$ mit $N \equiv a \pmod{p}$ und $N \equiv b \pmod{q}$.
- Intuitiv: Seien $p = 3, q = 5$. Suche: $N \in \mathbb{F}_{15}$ mit $N \equiv 2 \pmod{3}$ und $N \equiv 1 \pmod{5}$. Lösung: $N \equiv 1 \pmod{5}$ gilt für $N = 1, 6, 11$. Aber nur für $N = 11$ gilt zusätzlich $N \equiv 2 \pmod{3}$.

Kleiner Satz von Fermat

- Es gilt: $x^{p-1} = 1$ für $x \in \mathbb{F}_p$
- Intuitiv: z.B. für $p = 3$: $2^2 = 4 \equiv 1 \pmod{3}$

Also:

- Grundlegende Konzepte, die für RSA und ElGamal benötigt werden, habt ihr nun kennengelernt.
- Morgen: Anwendung der mathematischen Grundlagen bei RSA und ElGamal.
- Jetzt: Aufgaben!