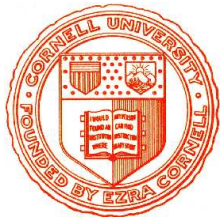
Kryptographie und Komplexität

Wintersemester 2009/10



Christoph Kreitz

kreitz@cs.uni-potsdam.de

http://www.cs.uni-potsdam.de/ti/lehre/09ws-Kryptographie

1. Wozu Kryptographie?
2. Einfache Verschlüsselungsverfahren
3. Anforderungen an moderne Verfahren
4. Organisation der Lehrveranstaltung

Wozu Kryptographie?

Sichere Übertragung vertraulicher Information

- **Nicht jede Information soll öffentlich sein**
  - Zugriff auf Computer, PIN für Bankkonto / Handy, private SMS
    Krankheitsgeschichte, Betriebs- oder militärische Geheimnisse, ...
- **Informationen müssen übertragen werden**
  - Internet, e-mail Kommunikation, Mobilfunk, CD/DVD (Kurier), ...
- **Übertragungskanäle sind oft unsicher**
  - Nachricht könnte von Unbefugten abgehört werden
- **Verschlüsselung macht Information geheim**
  - $\kappa\rho\upsilon\pi\tau o\varsigma$ = geheim $\gamma\rho\alpha\varphi\epsilon\iota\nu$ = schreiben
  - Unbefugte können abgehörte Nachricht nicht lesen
  - Zieladressat kann Originaltext leicht wiederherstellen

Kryptographie ist seit langem bewährt

- **Einfaches aber wirkungsvolles Szenario**
  - Sender und Empfänger einigen sich auf Verfahren und **Schlüssel**
  - Absender chiffriert **Klartext** mit Schlüssel
    und schickt **Schlüsseltext** auf unsicherem Kanal
  - Empfänger verwendet Schlüssel, um Klartext wiederherzustellen
  - Wird der Schlüsseltext von Unbefugten abgefangen, so können
    diese (ohne den Schlüssel) damit wenig anfangen
- **Übermittelte Nachricht ist sicher** . . . solange Schlüssel geheim
  - Zusätzliche Sicherheit durch Geheimhaltung des Verfahrens
    heute kaum noch zu gewährleisten
- **Einfache Verfahren waren lange sicher genug**
  - Ohne maschinelle Unterstützung sind Chiffrierungen kaum zu brechen
  - Die Analyse von chiffrierter Nachrichten konnte Jahre dauern

Der Computer hat alles verändert

Verschiebechiffren

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
X	Y	Z		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- **Eine der ältesten Verschlüsselungstechniken**
  - (Zyklische) Verschiebung der Buchstaben im Alphabet
  - Schon vor über 2000 Jahren von Julius Cäsar eingesetzt
- **Verschlüsselung durch Vorwärtsschieben**
  - Geheimer Schlüssel ist Buchstabe, der das A ersetzt
  - Schlüsseltext wird buchstabenweise erzeugt

    Aus `INFORMATIK BRAUCHT MATHEMATIK` mit Schlüssel `X`

    wird `EJBKNIXPEGWYNXQZDPWIXPDAIXPEG`
- **Entschlüsselung durch Rückwärtsschieben**
  - Adressat muß den Schlüssel (und das Chiffrierverfahren) kennen
  - Klartext wird buchstabenweise wiederhergestellt
- **Zu leicht zu brechen da nur 27 mögliche Schlussel**
  - Ausprobieren aller Schlüssel sogar von Hand durchführbar

Substitutionschiffren

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
X	N	Y	A	H	P	O	G	Z	Q		W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

- **Permutationstabelle für Ersetzung von Buchstaben**
  - Chiffretext entsteht durch Austausch der Buchstaben gemäß Tabelle

    Aus `INFORMATIK BRAUCHT MATHEMATIK`

    wird `ZTPSRBVXZ INRXMYGVIBXVDGHBVZ`
  - Originaltext durch Rückwärtsersetzung ermittelbar
- **Etwas sicherer als die Verschiebungchiffre**
  - Es gibt $n!$ verschiedene Permutationen (10^{28} im Beispiel)
  - Brute-Force Attacke bei mehr als 20 Buchstaben nicht möglich
- **Anfällig für statistische Analysen**
  - Bei langen Texten erlaubt Häufigkeit der Buchstaben Rückschlüsse
  - Im Deutschen ist jeder 7. Buchstabe ein E, jeder zehntausendste ein X

.. und wenn wir ganze Blöcke chiffrieren?

- **Verschiebe Blöcke von m Buchstaben gleichzeitig**
  - Schlüsselwort schiebt Elemente eines Buchstabenblocks unterschiedlich

    Aus `INFORMATIK BRAUCHT MATHEMATIK` mit Schlüssel '`A KEY`'

    wird `IMPSOM CMH AAERCGCDJASRIJASSOX`

    (Letzter Fünferblock durch Leerzeichen vervollständigt)
  - Originaltext durch Rückwärtsschieben der Blöcke ermittelbar
- **Es gibt viel mehr Schlüssel**
  - Bei n Symbolen und Blockgröße m insgesamt n^m Schlüssel (28^5 im Beispiel)
  - Ab Blockgröße 8und Verwendung von 62 alphanumerischen Symbolen sind Brute-Force Attacken selbst mit Computern undurchführbar
- **Trotzdem nicht sicher**
  - Blockgröße kann bei lange Chiffretexten bestimmt werden
  - Wörterbuchattacken überprüfen einfache Schlüssel ($\leq$ 500.000 Tests)
  - Statistische Analysen ermöglichen Ermittlung von Schlüsselteilen

Permutationschiffre

- **Vertausche Elemente innerhalb eines Buchstabenblocks**
  - Schlüssel ist Permutation π der Zahlen $1..m$ (Liste $[\pi(1), ..., \pi(m)]$)
  - Verschlüsselung teilt Text in m-Blöcke und vertauscht entsprechend
  - Entschlüsselung ist wie Verschlüsselung mit inverser Permutation

    Aus `INFORMATIK BRAUCHT MATHEMATIK` mit $\pi = [2\ 4\ 5\ 3\ 1]$
    wird `NORFIAIKTMBAUR H MTCTEMHATK IA`
    (Letzter Fünferblock durch Leerzeichen vervollständigt)

- **Sicher bei sehr großen Blöcken**
  - Es gibt $m!$ verschiedene Permutationen

    Ab Blocklänge 15 sicher gegen Brute-Force Attacke mit PC's
  - Häufigkeitsanalysen nutzen wenig
  - Aber, wenn mehr als m Klar-/Schlüsseltextpaare bekannt sind, kann

    Schlüssel durch Invertierung von $m \times m$-Matrizen berechnet werden

... und wenn die Chiffrierung noch komplexer wird?

- **Gleichzeitige Verschiebung und Permutation**
  - Verschlüsselung von Buchstabenblöcken
  - Jedes Element des Schlüsseltextblocks ergibt sich durch Linearkombinationen aller Elemente des Klartextblocks
  - Immer noch durch Invertierung von Matrizen zu brechen
- **One-Time Pad**
  - Schlüssel genauso groß wie Nachricht, einmalige Verwendung
  - Absolut sicher .... aber wie soll der Schlüssel übermittelt werden?
- **Strom-Chiffre**
  - Systematische Erzeugung von Pseudo One-Time Pads
  - Erzeuge beliebig lange Schlüssel aus Anfangsschlüssel + Nachricht
  - Mit mathematischen Methoden zu brechen, wenn Verfahren zur Schlüsselerzeugung bekannt geworden ist

Einfache Verfahren sind heute nicht mehr sicher

Kryptographische Systeme - was brauchen wir?

- **Sicherheit**
  - Nachricht soll von Unbefugten nicht dechiffriert werden können auch wenn das Chiffrierverfahren bekannt ist
  - Absolute Sicherheit ist (fast) nicht erreichbar

    Es reicht, daß der Code nicht in akzeptabler Zeit zu brechen ist
  - Praktische Sicherheit: gegen alle heute bekannten Arten von Attacken
  - Beweisbare Sicherheit: aus theoretischen Gründen niemals zu knacken
- **Flexibilität**
  - Verschlüsselung ist nicht nur etwas für Militär und Geheimdienste
  - Jeder muß mit jedem spontan sichere Verbindungen aufbauen können
- **Effiziente Ausführung**
  - Ver-/Entschlüsselung muß auch bei großen Datenmengen schnell sein
  - Verfahren muß auch auf Chipkarten o.ä. implementiert werden können

Ohne gute Theorie läuft nichts mehr

- **Sicherheit braucht gute Mathematik**
  - Statistik und Lineare Algebra überwinden einfache Chiffrierverfahren
    auch dann, wenn die Codierung relativ trickreich ist
    Mathematische Analysen offenbaren versteckte Regelmäßigkeiten
  - Zahlentheorie und Komplexitätstheorie ermöglichen neue Verfahren
    die nachweislich nicht in akzeptabler Zeit zu brechen sind
- **Flexibilität braucht gute Mathematik**
  - Zahlen- und Gruppentheorie ermöglichen asymmetrische Chiffrierung
    - Ver- und Entschlüsselung kann verschiedene Schlüssel benutzen
    - Ein Schlüssel kann gefahrlos veröffentlicht werden
- **Effizienz braucht gute Theorie**
  - Verschlüsselungsverfahren können durch Umstellungen auf der Basis
    mathematischer Gesetze erheblich beschleunigt werden
  - Sichere Schlüssel für viele Teilnehmer können schnell erzeugt werden

Beispiel: Public-Key Kryptographie mit RSA

- **Ältestes und wichtigstes öffentliches Verfahren**
  - Benannt nach seinen Erfindern Rivest, Shamir und Adleman (1977)
  - Behandelt Bitblöcke einer Nachricht als (sehr große) Zahlen
- **Verschlüsselungsverfahren**
  - Verschlüsselung durch Potenzieren mit e modulo n: $\boldsymbol{e_K(x)} = x^e \bmod n$
  - Entschlüsselung durch Potenzieren mit d modulo n: $\boldsymbol{d_K(y)} = y^d \bmod n$
  - Dabei $n = p * q$ für große Primzahlen p, q (mindestens 1024 bit) und $d * e \; mod \; (p-1)(q-1) = 1$
  - Öffentlich bekannt sind $n := p * q$ und e, d, p und q bleiben geheim
- **Hohe Qualität wegen gutem theoretischen Fundament**
  - Korrektheit: Für $x<n=p*q$ gilt $\boldsymbol{(x^e)^d \bmod n = x}$ (Satz von Euler-Fermat)
  - Effizienz: Ver-/Entschlüsselung verwendet binäres Hornerschema
    Iteriertes Quadrieren und Multiplizieren modulo n
  - Sicherheit: Faktorisierung von Zahlen ist exponentiell in Anzahl der Bits

Kryptographie leistet mehr als Vertraulichkeit

- **Vertraulichkeit**
  - Unbefugte können Nachricht nicht lesen
  - Erreichbar durch Verschlüsselung der Nachricht
- **Integrität**
  - Fälschung/Manipulation der Nachricht ist nicht möglich
  - Sichere Hashfunktionen ermöglichen Überprüfung von Veränderungen
- **Authentizität**
  - Garantie, daß Nachricht wirklich vom angegebenen Sender stammt
  - Möglich durch Verwendung von Paßwörtern und Identitätszertifikaten
- **Verbindlichkeit**
  - Absender kann Urheberschaft nicht nachträglich leugnen
  - Digitale Signaturen binden Nachricht an ihren Absender

Themen dieser Veranstaltung

Kryptographische Algorithmen und ihre Komplexität

- **Kryptoanalyse einfacher Verschlüsselungssysteme**
  – Mathematische Methoden zum Brechen von Chiffrierverfahren
- **SPN Chiffren** (Nur kurze Übersicht)
  – Substitutions-Permutations Netzwerke, DES, AES
- **Public Key Kryptographie mit RSA**
  – Ver- /Entschlüsselung, Schlüsselerzeugung, Komplexität von Attacken
- **Kryptoverfahren auf Basis diskreter Logarithmen**
  – El Gamal Verfahren, Schlüsselerzeugung, Attacken
  – Chiffrierung mit Elliptische Kurven
- **Jenseits von Vertraulichkeit** (Nur kurze Übersicht)
  – Protokolle für Hash, Signatur, Secret Sharing, Authentifikation
  – Public-Key Infrastrukturen und Anwendungen

Relevante Mathematik wird bei Bedarf vorgestellt

Lehrmaterialien

- **Folien der Veranstaltung**
  - (evtl. kurz) vor der Vorlesung auf dem Webserver erhältlich
- **Wichtige Lehrbücher**
  - Douglas R. Stinson *Cryptography: Theory and Practice*
  - Johannes Buchmann, *Einführung in die Kryptographie*
  - Jörg Rothe, *Complexity Theory and Cryptology*

  Themenauswahl und Reihenfolge der Vorlesung ist anders
- **Hilfreiche Zusatzliteratur**
  - F.L Bauer, *Decrypted Secrets*
  - Richard Mollin, *An introduction to cryptography*,
  - O. Goldreich, *Foundations of Cryptography (2 volumes)*
  - A. Beutelspacher, H. Neumann, T. Schwarzpaul, *Kryptografie in Theorie und Praxis*
  - A. Beutelspacher, *Kryptologie*
  - M. Stamp, R. Low, *Applied Cryptanalysis: Breaking Ciphers in the real world*

Organisatorisches

- **Zuordnung: theoretische/angewandte Informatik**
- **Veranstaltungen**
  - Vorlesung (Di 10:15–11:45 + Fr. 12:15–13:45)
    - Präsentation der zentralen Konzepte / Ideen
    - Keine Vorlesung am 18.12.2009 und 5.1.2010
  - Sprechstunde (Fr 10:30–11:30 . . . , und immer wenn die Türe offen ist)
    - Fachberatung / Klärung von Schwierigkeiten mit der Thematik
  - Übungsaufgaben (gelegentlich)
    - Anregung und Herausforderungen zum Selbsttraining
- **Empfohlene Vorkenntnisse:**
  - Gutes Verständnis von Mathematik / theoretischer Informatik
- **Erfolgskriterien**
  - Abschlußprüfung schriftlich (mündlich bei geringer Teilnehmerzahl)