

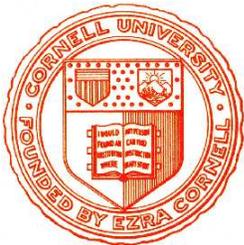
Kryptographie und Komplexität

Wintersemester 2014/15

Christoph Kreitz

kreitz@cs.uni-potsdam.de

<http://cs.uni-potsdam.de/krypto-ws1415>



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

WORUM GEHT ES?

- **Information ist die Grundlage unseres Alltags**
 - Eine Gesellschaft ohne ständigen Zugriff auf Informationen ist nicht mehr denkbar
 - EC karte, Kreditkarte, Online Banking, Online Store, Ebay, ...
 - E-mail, Smartphones, Facebook, Instagram, ...
 - Öffentliche Verwaltung, Gesundheitsakten, Leistungsübersicht, ...
 - Die Nachfrage nach neuen Formen von Informationsaustausch wächst
 - Cloud Computing, Online Voting, ...
 - Electronic Cash, elektronische Gesundheitskarte
 - Car2Car Kommunikation, automatische Flugverkehrskontrolle, ...
- **Informationen müssen gelagert werden**
 - Papierakten und -zettel, SIM Karte, Festplatte, Cloud, ...
- **Informationen müssen übertragen werden**
 - Internet, e-mail Kommunikation, Mobilfunk, CD/DVD (Kurier), ...

In einer idealen Welt wäre das alles ganz einfach

WOZU BRAUCHT MAN KRYPTOGRAPHIE?

Vertrauliche Informationen müssen geschützt werden

- **Nicht jede Art von Information soll öffentlich sein**
 - Zugriffsdaten für Computer, PIN für Bankkonto oder Handy, ...
 - Private emails oder SMS, persönliche Krankheitsgeschichte, ...
 - Betriebs- oder militärische Geheimnisse, ...
- **Es gibt ständig Mißbrauch von Daten / Kommunikation**
 - Kreditkartenbetrug, EC Diebstahl, Wirtschaftsspionage, ...
 - Offenlegen persönlicher Informationen, peinlicher Facebookbilder, ...
 - Überwachung von Telephonverbindungen, Bewegungsprofile, ...
 - Zerstörung von Daten durch Computerviren, Terrorismus, ...
 - Unerwünschte Fernsteuerung von Autos, Flugzeugen, ...
- **Die Welt ist nicht so sicher, wie es scheint**
 - Forscherteam übernimmt Kontrolle einer Militärdrone (Juni 2012)
 - **CarShark** kontrolliert Auto-CanBus, Bremsen, Tachometer, Lenkung ... über GPS (2010)
 - **Heartbleed-Bug** macht alle “sicheren” Internet-Verbindungen anfällig für Angriffe (2014)

KRYPTOGRAPHIE KANN INFORMATIONEN SCHÜTZEN

κρυπτος = geheim *γραφειν* = schreiben

- **Verschlüsselung macht Informationen unkenntlich**
 - Unbefugte Personen können verschlüsselte Daten nicht lesen
 - Berechtigte können versteckte Information leicht wiederherstellen
 - Ermöglicht sichere Lagerung und Übertragung von Informationen
- **Kommunikationsszenario ist einfach aber wirkungsvoll**
 - Sender und Empfänger einigen sich auf Verfahren und **Schlüssel**
 - Absender chiffriert **Klartext** mit Schlüssel und schickt **Schlüsseltext** auf ungeschütztem Kanal
 - Empfänger verwendet **Schlüssel**, um Klartext zu rekonstruieren
- **Kryptographie ist seit langem bewährt**
 - Verschlüsselte Informationen sind sicher:
 - Ohne den Schlüssel können Unbefugte den Klartext nicht rekonstruieren
 - **Nur der Schlüssel muß geheim bleiben**
 - Geheimhaltung des **Verfahrens** liefert keine zusätzliche Sicherheit mehr

EINFACHE VERFAHREN WAREN LANGE SICHER GENUG

- **Verschiebechiffren** (Julius Cäsar, 60 v Chr.)
 - Zyklische Verschiebung der Buchstaben im Alphabet
 - **Angriff:** Ausprobieren aller Möglichkeiten
- **Affine Chiffre** (ca. 1500)
 - Multiplikation der Buchstabenposition und anschließendes Verschieben
 - Ausprobieren aller Möglichkeiten ist möglich aber sehr aufwendig
 - **Angriff:** Häufigkeitsanalyse und Lösen linearer Gleichungssysteme
- **Allgemeine Substitutionschiffre**
 - Austausch von Buchstaben mithilfe einer Ersetzungstabelle
 - Ausprobieren aller Möglichkeiten undurchführbar
 - **Angriff:** statistische Analysen (sehr aufwendig)
- **Verschiebe Textblöcke mit Schlüsselwort** (Vigenere ca. 1550)
 - Leichtere Ver-/Entschlüsselung als Substitutionschiffre
 - **Angriff:** Kasiski Test (1863!) und Häufigkeitsanalysen

Nur gute Mathematiker konnten Chiffrierungen brechen

- **Verschiebung und Permutation in Textblöcken**

- Verschlüsselung ist Linearkombinationen der Elemente im Klartextblock
Immun gegen statistische Analysen und Brute-Force Attacks
- **Angriff:** Abfangen von Klar-/Schlüsseltextpaaren + Matrixinvertierung

- **Strom-Chiffren**

- Erzeuge beliebig lange Schlüssel aus Anfangsschlüssel + Nachricht
- Nur zu brechen, wenn Verfahren zur Schlüsselerzeugung bekannt

- **One-Time Pad**

- Schlüssel genauso groß wie Nachricht, einmalige Verwendung
- **Nicht zu brechen(!)** ... aber wie soll der Schlüssel übermittelt werden?

- **Sicher bis zum Ende des zweiten Weltkriegs**

- Effiziente Chiffrierung mithilfe von Verschlüsselungsmaschinen
- Analyse einzelner(!) chiffrierter Texte dauerte oft Jahre

- **Der Computer hat alles verändert**

- Maschinen, die Milliarden von Tests in wenigen Sekunden ausführen, können jede “mechanische” Chiffrierung in kurzer Zeit brechen

Was sind die Ziele?

- **Sicherheit**

- Schlüsseltext soll nicht von Unbefugten dechiffriert werden können auch wenn das Chiffrierverfahren bekannt ist
- **Absolute Sicherheit** ist aber fast nicht erreichbar
- Es reicht, daß die Chiffrierung nicht in akzeptabler Zeit zu brechen ist
Praktisch reicht Sicherheit gegen alle bekannten Arten von Attacken

- **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

SICHERHEIT HAT VERSCHIEDENE ASPEKTE

- **Vertraulichkeit**
 - Unbefugte können keinen Zugriff auf Informationen bekommen
 - Erreichbar durch **Verschlüsselung von Daten**
- **Integrität**
 - Fälschung oder Manipulation von Informationen ist nicht möglich
 - **Sichere Hashfunktionen** ermöglichen Überprüfung von Veränderungen
- **Authentizität**
 - Eine Nachricht stammt garantiert vom angegebenen Sender
 - Möglich durch Verwendung von **Paßwörtern und Identitätszertifikaten**
- **Verbindlichkeit**
 - Absender kann Urheberschaft nicht nachträglich leugnen
 - **Digitale Signaturen** binden Nachricht an ihren Absender

Kryptographie kann Vertrauen schaffen

- **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
(RSA: Potenzieren mit großen Zahlen modulo n , El Gamal, elliptische Kurven)

- **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

Ältestes öffentliches Verfahren (Rivest, Shamir & Adleman, 1977)

● Mathematisch einfaches Verschlüsselungsverfahren

- Behandelt Bitblöcke einer Nachricht als (sehr große) Zahlen
- Verschlüsselung durch Potenzieren mit e modulo n : $e_K(x) = x^e \bmod n$
- Entschlüsselung durch Potenzieren mit d modulo n : $d_K(y) = y^d \bmod n$
- Dabei $n = p * q$ für große Primzahlen p, q
und $d * e \bmod (p-1)(q-1) = 1$
- 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 $(x^e)^d \bmod n = x$ (Satz von Euler-Fermat)
- Effizienz: Ver-/Entschlüsselung verwendet binäres Horner Schema
Iteriertes Quadrieren und Multiplizieren modulo n
- Sicherheit: Faktorisierung von Zahlen ist exponentiell in Anzahl der Bits

THEMEN DIESER VERANSTALTUNG

- **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 Elliptischen Kurven
- **Jenseits von Vertraulichkeit** (Nur kurze Übersicht)
 - Protokolle für Hash, Signatur, Secret Sharing, Authentifikation
 - Public-Key Infrastrukturen und Anwendungen

Schwerpunkt: Krypto-Algorithmen und ihre Komplexität

Implementierungsaspekte spielen nur eine untergeordnete Rolle

Relevante Mathematik wird jeweils bei Bedarf vorgestellt

- **Folien der Vorlesung**
 - Im voraus auf dem Webserver erhältlich
- **Beispielprogramme für Demos und eigene Experimente**
 - Verwenden Programmiersprache OCaml (meist im Interpreter-Modus)
 - Werden gelegentlich auf dem Webserver aktualisiert
- **Wichtige Lehrbücher** (Themenauswahl/Reihenfolge etwas anders als in Vorlesung)
 - Douglas R. Stinson *Cryptography: Theory and Practice*
 - Johannes Buchmann, *Einführung in die Kryptographie*
 - Jörg Rothe, *Complexity Theory and Cryptology*
- **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** (Mi 10:15–11:45 (1.02), Do 10:15–11:45 (1.02))
 - Präsentation der zentralen Konzepte / Ideen
 - **Keine Vorlesung am 17./18.12.2014 und 7.1.2014**
 - **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
- **Erfolgskriterium: Abschlußklausur am 12. Februar 2015**
 - Mündliche Prüfung als Alternative (nur bei geringer Teilnehmerzahl)