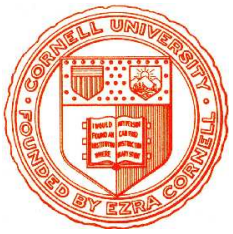
Kryptographie und Komplexität

Wintersemester 2007/08



Christoph Kreitz

kreitz@cs.uni-potsdam.de

http://www.cs.uni-potsdam.de/ti/lehre/07-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 $\gamma\rho\alpha\phi\epsilon\iota\nu$ = 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
  - Absender schickt **Schlüsseltext** auf unsicherem Kanal
  - Wird der Schlüsseltext von Unbefugten abgefangen, so können diese (ohne den Schlüssel) damit wenig anfangen
  - Empfänger verwendet Schlüssel, um Klartext wiederherzustellen
- **Übermittelte Nachricht ist sicher**

  . . . solange der Schlüssel geheim bleibt
  - Zusätzliche Sicherheit durch Geheimhaltung des Verfahrens ist heutzutage aber 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
  - Wurde vor über 2000 Jahren schon 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`
  - Verschlüsselter Text kann über unsichere Kanäle verschickt werden
- **Entschlüsselung durch Rückwärtsschieben**
  - Adressat muß den Schlüssel (und das Chiffrierverfahren) kennen
  - Klartext wird buchstabenweise wiederhergestellt

Verschiebechiffren sind zu einfach

- **Brute-force Attacke: Ausprobieren aller Schlüssel**
  - Aus `EJBKNIXPEGWYNXQZDPWIXPDAIXPEG` wird schrittweise
    `FKCLOJYQFHXZOYR EQXJYQEBJYQFH` (Schlüssel ' ')
    `GLDMPKZRGIY PZSAFRYKZRFCKZRGI` (Schlüssel 'Z')
    `HMENQL SHJZAQ TBGSZL SGDL SHJ` (Schlüssel 'Y')
    `INFORMATIK BRAUCHT MATHEMATIK` (Schlüssel 'X')
  - Klartext ist meist der einzige sprachlich akzeptable Text
- **Verschiebechiffren sind von Hand zu brechen**
  - Es gibt nur so viele Schlüssel wie Symbole im Alphabet (27 im Beispiel)
  - Oft kann ein Schlüssel bereits nach wenigen Buchstaben akzeptiert oder verworfen werden
  - Beispiel: dechiffrieren Sie `XYKTLWAENYLLYETBLMTN`
    Lösung: `DER SCHLUESSEL IST U` (Schlüssel 'U')

Mit dem Computer geht es noch einfacher

Brute-Force Attacke auf Verschiebechiffren

- **Computer generiert alle 27 Möglichkeiten**

```
EJBKNIXPEGWYNXQZDPWIXPDAIXPEG  Schlüssel  'A'
DIAJMHWODFVXMWPYCOVHWOC HWODF  Schlüssel  'B'
CH ILGVNCEUWLVOXBNUGVNBZGVNCE  Schlüssel  'C'
BGZHKFUMBDTVKUNWAMTFUMAYFUMBD  Schlüssel  'D'
AFYGJETLACSUJTMV LSETL XETLAC  Schlüssel  'E'
 EXFIDSK BRTISLUZKRDSKZWDSK B  Schlüssel  'F'
ZDWEHCRJZAQSHRKTYJQCRJYVCRJZA  Schlüssel  'G'
YCVDGBQIY PRGQJSXIPBQIXUBQIY   Schlüssel  'H'
XBUCFAPHXZOQFPIRWHOAPHWTAPHXZ  Schlüssel  'I'
WATBE OGWYNPEOHQVGN OGVS OGWY  Schlüssel  'J'
V SADZNFVXMODNGPUFMZNFURZNFVX  Schlüssel  'K'
UZR CYMEUWLNCMFOTELYMETQYMEUW  Schlüssel  'L'
TYQZBXLDTVKMBLENSDKXLDSPXLDTV  Schlüssel  'M'
SXPYAWKCSUJLAKDMRCJWKCROWKCSU  Schlüssel  'N'
RWOX VJBRTIK JCLQBIVJBQNVJBRT  Schlüssel  'O'
QVNWZUIAQSHJZIBKPAHUIAPMUIAQS  Schlüssel  'P'
PUMVYTH PRGIYHAJO GTH OLTH PR  Schlüssel  'Q'
OTLUXSGZOQFHXG INZFSGZNKSGZOQ  Schlüssel  'R'
NSKTWRFYNPEGWFZHMYERFYMJRFYNP  Schlüssel  'S'
MRJSVQEXMODFVEYGLXDQEXLIQEXMO  Schlüssel  'T'
LQIRUPDWLNCEUDXFKWCPDWKHPDWLN  Schlüssel  'U'
KPHQTOCVKMBDTCWEJVBOCVJGOCVKM  Schlüssel  'V'
JOGPSNBUJLACSBVDIUANBUIFNBUJL  Schlüssel  'W'
INFORMATIK BRAUCHT MATHEMATIK  Schlüssel  'X'
HMENQL SHJZAQ TBGSZL SGDL SHJ  Schlüssel  'Y'
GLDMPKZRGIY PZSAFRYKZRFCKZRGI  Schlüssel  'Z'
FKCLOJYQFHXZOYR EQXJYQEBJYQFH  Schlüssel  ' '
```

- **Wörterbuch hilft bei Bestimmung der Lösung**

.. und wenn wir ganze Blöcke chiffrieren?

- **Verschiebe Blöcke von m Buchstaben gleichzeitig**
  - Schlüssel verschiebt Elemente eines Buchstabenblocks unterschiedlich

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

    wird `IMPSOM CMH AAERCGCDJASRIJASSOX`

    (Letzter Fünferblock wurde durch Leerzeichen vervollständigt)
  - Originaltext durch Rückwärtsschieben der Blöcke ermittelbar
- **Es gibt viel mehr Schlüssel**
  - Bei n Symbolen und Blockgröße m insgesamt n^m Schlüssel

    ($27^5 = 14.348.907$ im Beispiel)
  - Brute-Force Attacken mit dem Computer werden ab Blockgröße 8 und Verwendung von 62 alphanumerischen Symbolen undurchführbar
- **Trotzdem nicht sicher**
  - Blockgröße kann bei lange Chiffretexten bestimmt werden
  - Wörterbuchattacken überprüfen einfache Schlüssel (≤ 500.000 Tests)
  - Statistische Analysen ermöglichen Ermittlung von Schlüsselteilen

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

- **Buchstaben werden permutiert**
  - Chiffretext entsteht durch entsprechende Ersetzung der Buchstaben

    Aus `INFORMATIK BRAUCHT MATHEMATIK`

    wird `ZTPSRBVXZ INRXMYGVIBXVDGHBVZ`
  - Originaltext durch inverse Permutation 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
- **Ebenfalls anfällig für statistische Analysen**
  - Bei langen Texten erlaubt Buchstabenhäufigkeit Rückschlüsse
  - Deutsch: E$\hat{=}$14.7%, N$\hat{=}$8.8%, R$\hat{=}$6.8%, ... Q$\hat{=}$0.014%, X$\hat{=}$0.013%

Permutationschiffre

- **Vertausche Elemente eines Buchstabenblocks**
  - Schlüssel ist Permutation π der Zahlen $1..m$ (Liste $[\pi(1), ..., \pi(m)]$)
  - Verschlüsselung teilt Text in m-Blöcke auf 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 wurde durch Leerzeichen vervollständigt)

- **Sicher nur 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 (Linear-)kombinationen aller Elemente des Klartextblocks
  - Kann immer noch durch Invertierung von Matrizen gebrochen werden
- **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

Es gibt zwei Arten kryptographischer Verfahren

- **Private-Key Kryptographie** (symmetrisch)
  - Sender und Empfänger benutzen den gleichen geheimen Schlüssel
  - Arbeitsweise und Sicherheit basiert auf "Kompliziertheit" des Verfahrens
    - Mehrfachverschlüsselung von Textblöcken mit Substitution/Permutation
    - Schnelle Ausführung, da Hardwareunterstützung möglich
    - Große statistische Streuung macht sicher gegen bekannte Angriffsarten
  - Bekannteste Vertreter: DES und AES (z.B. in WLAN Routern)
  - Problem: Schlüssel muß vorher auf sichere Art ausgetauscht werden
- **Public-Key Kryptographie** (asymmetrisch)
  - Ver- und Entschlüsselung benutzen verschiedene (inverse) Schlüssel
  - Empfänger legt einen Schlüssel zur Verschlüsselung offen
    Privater Schlüssel kann aus dem öffentlichen nicht berechnet werden
  - Ermöglicht spontane sichere Verbindungen mit jedem Netzteilnehmer

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 Public-Key Verfahren**
  - Benannt nach seinen Erfindern Rivest, Shamir und Adleman (1977)
  - Behandelt Bitblöcke einer Nachricht als (sehr große) Zahlen
- **Benutzt bekannte Gesetze der Modulararithmetik**
  - Sind p, q Primzahlen und $x<n:=p*q$, dann gilt $\boldsymbol{(x^e)^d \bmod n = x}$ für jedes Paar von Zahlen e und d mit $d*e \bmod (p-1)(q-1) = 1$
    (folgt aus einem Satz von Euler-Fermat)
  - Um d aus e und n zu berechnen, muß man n in p und q zerlegen können
    Faktorisierung sehr großer Zahlen ist nicht in akzeptabler Zeit möglich
- **Verschlüsselungsverfahren**
  - Verschlüsselung wird Potenzieren mit e modulo n: $\boldsymbol{e_K(x)} = x^e \bmod n$
  - Entschlüsselung wird Potenzieren mit d modulo n: $\boldsymbol{d_K(y)} = y^d \bmod n$
  - Dabei $n = p*q$ für große Primzahlen p, q und $d*e \; mod \; (p-1)(q-1) = 1$
  - Gesamtschlüssel ist $K := (n, p, q, d, e)$, wobei nur e, n öffentlich

Das RSA Verfahren am Beispiel

- **Einfaches Zahlenbeispiel**
  - Wähle $p = 11$ und $q = 23$, also $n = 253$
  - Wähle $e = 3$. Dann muß $d = 147$ sein $(3 * 147 \bmod 220 = 1)$
  - Verschlüsselung der Zahlen 4 5 6 7 8 9 mit e ergibt 64 125 216 90 6 223
  - Entschlüsselung benötigt Computerprogramm für Modulararithmetik
- **Ein computergeneriertes Beispiel mit 256 Bit**
  - Generiere $p =$ 200090614988854752464080544630480762821
    und $q =$ 185943990722218737951811440044937739573
    und $e =$ 91225117934565043354694670473901491802882927843894977203888465620701016614749
  - Ausgangstext " INFORMATIK BRAUCHT MATHEMATIK "
  - Umwandlung des gesamten Textes in eine 256-bit Zahl (77 Stellen) 14603531222158190878074976722480774803100880121174407015018204085926251667488
  - Verschlüsselung mit der Zahl e ergibt 582951775580622158001308682120043451387474318773483567458266088260993963468 9
  - Chiffrierter Text wird als Bitkette (nicht als Dezimalzahl) übertragen

Das RSA Verfahren - wichtige Fragen

- **Wie bestimmt man (effizient) einen Schlüssel?**
  - Erzeuge zwei zufällige Primzahlen p, q mit 512 bit
  - Erzeuge ein zufälliges e mit $\mathrm{ggT}(e, (p-1)(q-1)) = 1$
  - Berechne d als das modulare Inverse von e (modulo $(p-1)(q-1)$)
  - Lege $n := p * q$ und e offen, halte d, p und q geheim
- **Wie schnell kann ver-/entschlüsselt werden?**
  - Wiederholtes Quadrieren und Multiplizieren (jeweils modulo n)
  - z.B. $x^{13} = x * x^{12} = x * (x^6)^2 = x * ((x^3)^2)^2 = x * ((x * x^2)^2)^2$
- **Wie sicher ist das Verfahren?**
  - Um privaten Schlüssel zu bestimmen, muß man n faktorisieren können
  - Faktorisierung braucht exponentiell viele Schritte in Anzahl der Bits
    z.B. braucht ein PC für 1024 Bit mehr als 100.000.000 Jahre
  - Verfahren kann selbst gegen den besten Faktorisierungsalgorithmus und massive Parallelverarbeitung sicher gemacht werden

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- und Entschlüsselung, Schlüsselerzeugung, Komplexität von Attacken
- **Kryptoverfahren auf Basis diskreter Logarithmen**
  - El Gamal Verfahren, Schlüsselerzeugung, Attacken
  - Chiffrierung mit Elliptische Kurven
- **Jenseits von Vertraulichkeit**
  - 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 (Mi 11:00–12:30 + Fr. 9:20–10:45)
    - Präsentation der zentralen Konzepte / Ideen
    - Keine Vorlesung am (31.10.,) 7.11., 9.11., 19.12., 21.12 und 9.1.2008
  - Sprechstunde (Mi 9:30–10:30 . . . , 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 (mündlich oder schriftlich, je nach Teilnehmerzahl)