Mathematische Grundlagen der Kryptographie

Organisatorisches

Die Veranstaltung sollte über “Aktuelle Trends der Informatik” abgerechnet werden.

Sie besteht aus Vorlesung und Praktikum.

Im Praktikum sollen Algorithmen in python implementiert werden.

Hierzu: Tocas

Die Prüfungsleistung besteht aus:

Im Zweier-Team:

- Implementieren von kleineren Algorithmen
- Ein größeres Projekt: Implementieren und Beschreibung und Dokumentation
- Präsentation (Zu Beginn oder zum Ende der Semesterferien)

Einige Worte zur Kryptographie

Warnhinweis

Die Vorlesung wird deutlich anders werden, als die folgenden Ausführungen.

Was bedeutet “Kryptographie”?

Bis ca. 1970:

Kryptographie = Geheimschrift

(Wortschöpfung aus der Neuzeit)

Seit ca. 1918:

Kryptologie = Kryptographie + Kryptoanalyse

(nicht einheitlich)

Was bedeutet “Kryptographie”?

Heute: Der Begriff hat eine wesentlich weitere Bedeutung.

Ein Definitionsversuch:

> Kryptographie ist die Benutzung und das Studium von Techniken für alle sicherheitsrelevanten Aspekte des Verarbeitens, Übertragens und Benutzens von Informationen in Anwesenheit eines Gegners.

(vergleiche englischsprachige Wikipedia)

Was bedeutet “Kryptographie”?

Ziele heute.

- Vertraulichkeit
- Authentisierung
- Verbindlichkeit
- Integrität

Klassische Ideen

Zwei Personen wollen verschlüsselt Nachrichten austauschen.

1. Ansatz

Veränderung auf Buchstabenebene

- Substitution (ersetze einen Buchstaben durch einen anderen)
- Transposition (verändere die Reihenfolge)

2. Ansatz

Benutzung eines Codebuch

Angriffe mittels statistischer Analyse.

In beiden Fällen:

Es gibt ein Verfahren und einen Schlüssel.

Das Keckhoffs'sche Prinzip

Auguste Kerckhoffs: La cryptographie militaire von 1883:

Das Prinzip kurz und knapp:

> Das Geheimnis darf nur im Schlüssel liegen, und dieser muss noch während der Kommunikation veränderbar sein.

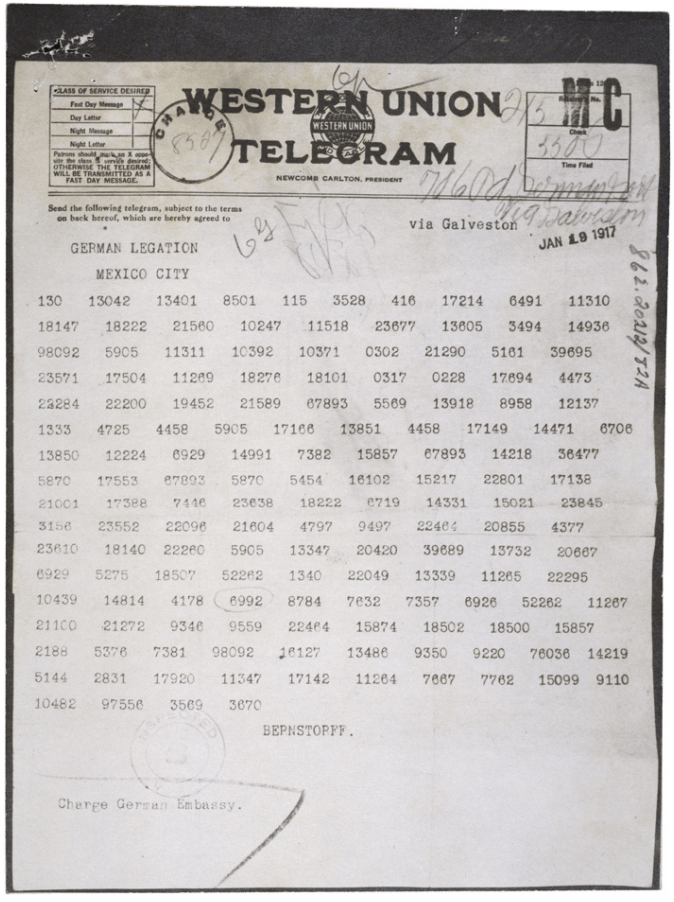
Kleiner historischer Überblick

Drei Perioden:

- Bis 1918: Papier-und-Bleistift-Periode
- 1918 – ca. 1970: Periode der elektrisch-mechanischen Chffriermaschinen
- ab ca. 1970: Das elektronische Zeitalter
  (→ Moderne Kryptographie)

Der Weg zur modernen Kryptographie

Bis 1918: Klassische Ideen mit “Papier und Bleistift”



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

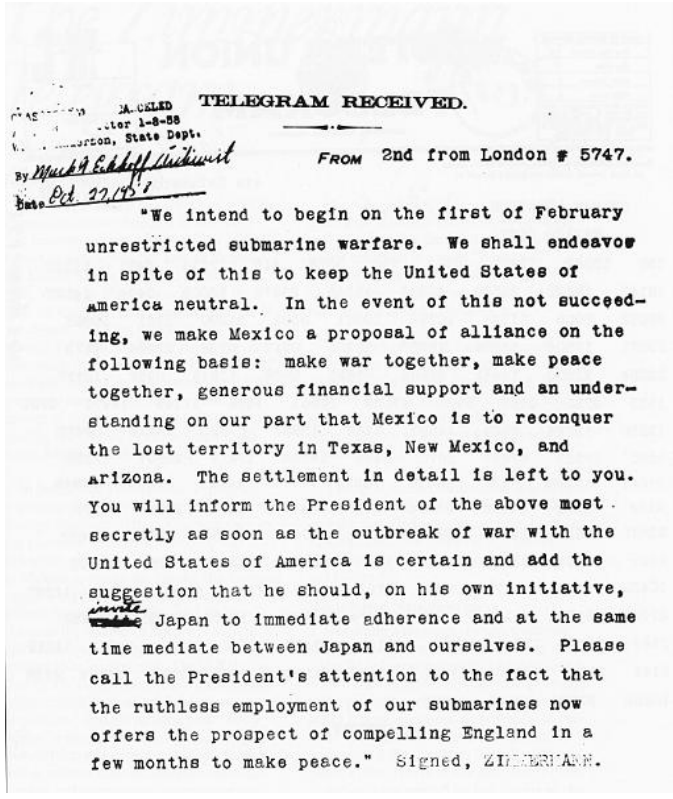
JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.



TELEGRAM RECEIVED.

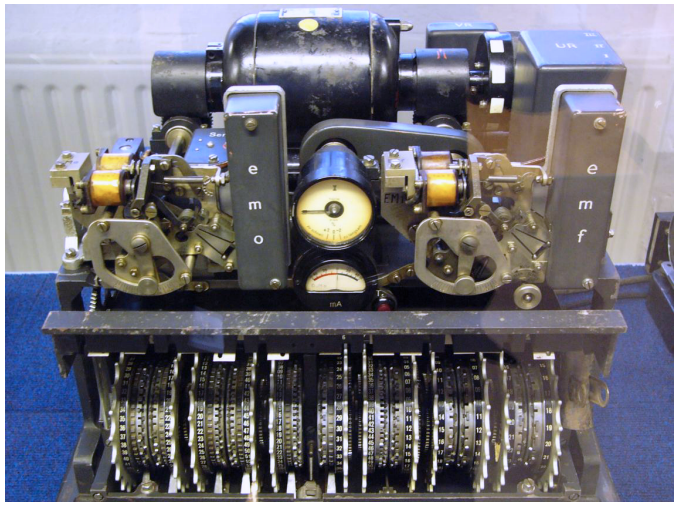
FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Das *Zimmermann-Telegramm* (19.1.1917)

Der Weg zur modernen Kryptographie

Ab 1918: Elektrisch-mechanische Chiffriermaschinen

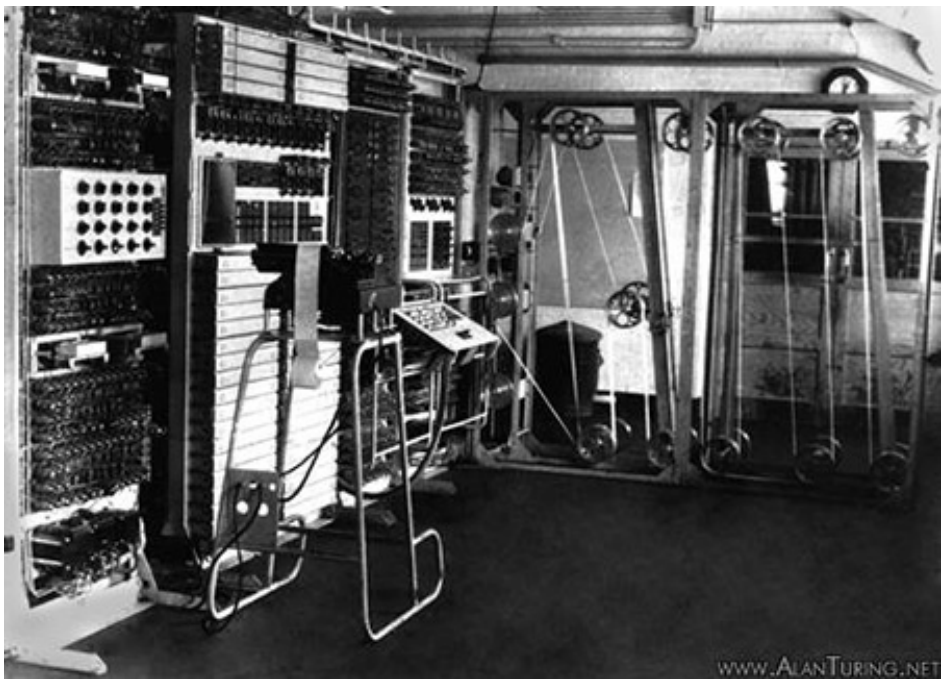


eine *Enigma* und eine *Lorenz-Schlüsselmaschine*

Der Weg zur modernen Kryptographie

Im II. Weltkrieg:

- neue Methoden zur Entziffernung (Gruppentheorie)
- Computer für die Kryptoanalyse



Colossus

Der Weg zur modernen Kryptographie

Ab 1960: Datenverarbeitung kommt auf.

1973 – 1977: Wettbewerb zum “Digital Encryption Standard (DES)” von NIST

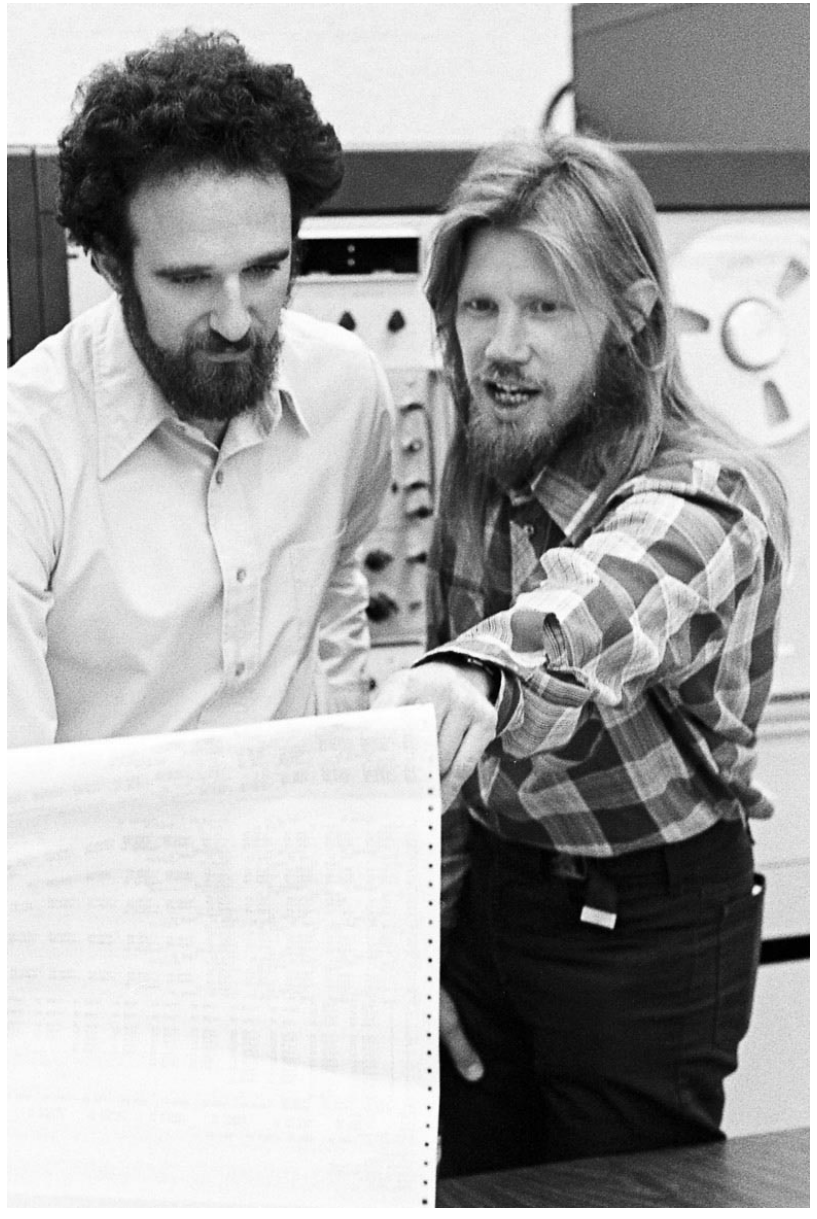
1976: Whitfield Diffie und Martin Hellman, New directions in cryptography

Der Weg zur Modernen Kryptographie

Umbrüche und Paradigmenwechsel um 1980

- Technischer Umbruch: hin zu Computern
- Neue, weitere Zielsetzungen
- Neue Arten von Verfahren (insb. Kryptographie mit öffentlichen Schlüsseln)
- Neue Methoden: Komplexitätstheorie und Zahlentheorie
- Offene Forschung statt geheimer militärischer Forschung
- Verwissenschaftlichung der Kryptographie

Das Diffie-Hellman Protokoll



Modulorechnen

Es sei p eine Primzahl.

Wir haben die Menge der Restklassen

$$\mathbf{Z}/p\mathbf{Z} \ .$$

Beispiel.

$$\mathbf{Z}/11\mathbf{Z} = \{[0]_{11}, [1]_{11}, \ldots, [10]_{11}\}$$

$$[11]_{11} = [0]_{11} \ , [24]_{11} = [13]_{11} = [2]_{11} = [-9]_{11}$$

$$[5]_{11} + [6]_{11} = [11]_{11} = [0]_{11}$$

$$[3]_{11} \cdot [4]_{11} = [12]_{11} = [1]_{11}$$

$\mathbf{Z}/p\mathbf{Z}$ ist ein Körper mit Null-Element $[0]_p$ und Einselement $[1]_p$.
Bezeichnung: $\mathbf{F}_p$. Die multiplikative Gruppe ist

$$\mathbf{F}_p^* = \mathbf{F}_p \backslash \{[0]_p\} = \mathbf{F}_p \backslash \{0\} \ .$$

Die Ordnung

Für $a \in \mathbf{F}_p^*$ betrachten wir

$$\langle a \rangle := \{a^0 = 1\,,\, a^1 = a\,,\, a^2\,,\, \ldots\,,\, a^i\,,\, \ldots\}\,.$$

Die Anzahl $\#\langle a \rangle = \{a^i \mid i \in \mathbf{N}_0\}$ heißt die Ordnung von a, $\mathrm{ord}(a)$.

Es ist $\langle a \rangle = \{a^0 = 1\,,\, a^1 = a\,,\, a^2\,,\, \ldots\,,\, a^{\mathrm{ord}(a)-1}\}$,

$$a^{\mathrm{ord}(a)} = a^0 = 1\,.$$

Beispiel. Es ist

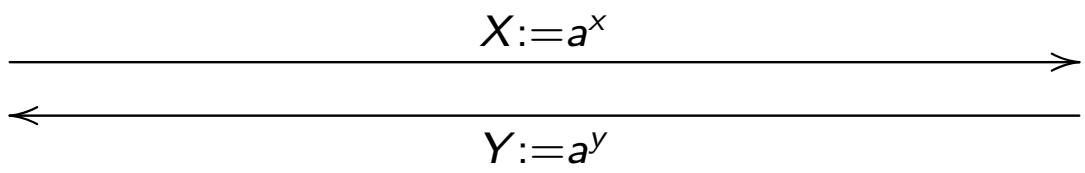
$$[4]_{11}^2 = [5]_{11}\,,\; [4]_{11}^3 = [9]_{11}\,,\; [4]_{11}^4 = [3]_{11}\,,\; [4]_{11}^5 = [1]_{11} = 1$$

und somit $\mathrm{ord}([4]_{11}) = 5$.

Das Diffie-Hellman Protokoll

Alice und Bob einigen sich (in der Öffentlichkeit) auf eine große Primzahl p und ein Element $a \in \mathbf{F}_p^*$.

Alice	**Bob**
Wählt $x < \mathrm{ord}(a)$.	Wählt $y < \mathrm{ord}(a)$.

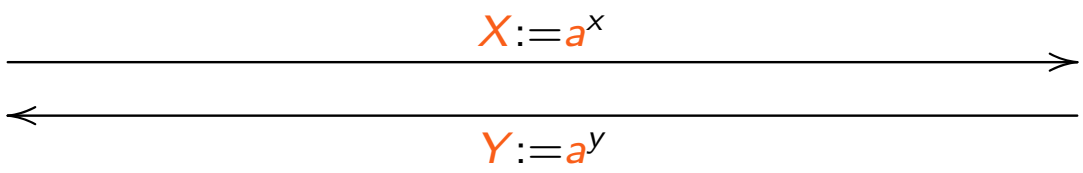


$$\boxed{Y^x = a^{xy} = X^y}$$

Das Diffie-Hellman Protokoll

Alice und Bob einigen sich (in der Öffentlichkeit) auf eine große Primzahl p und ein Element $a \in \mathbf{F}_p^*$.

Alice	**Bob**
Wählt $x < \mathrm{ord}(a)$.	Wählt $y < \mathrm{ord}(a)$.



$$\boxed{Y^x = a^{xy} = X^y}$$

Zur Sicherheit

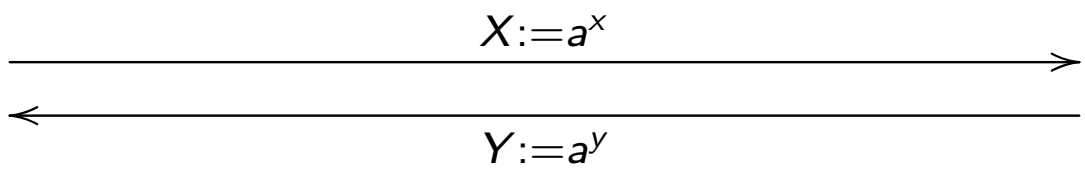
Zur Sicherheit des Protokolls:

- Für die Sicherheit des Protokolls ist das Diffie-Hellman Problems relevant:
  Gegeben $p; a, X = a^x, Y = a^y$, berechne a^{xy}.
- Hierfür ist insbesondere die Schwierigkeit des klassischen diskreten Logarithmusproblems relevant:
  Gegeben $p; a, X = a^x$, berechne x.
- Wir haben eine Reduktion vom DHP auf das DLP
  (DHP $\leq$ DLP)

Das Diffie-Hellman Protokoll

Alice und Bob einigen sich (in der Öffentlichkeit) auf eine große Primzahl p und ein Element $a \in \mathbf{F}_p^*$.

Alice	**Bob**
Wählt $x < \mathrm{ord}(a)$.	Wählt $y < \mathrm{ord}(a)$.



$$\boxed{Y^x = a^{xy} = X^y}$$

Zur Sicherheit II

Zur Sicherheit des Protokolls:

- Besser: Das Protokoll ist für Parameter p, a genau dann sicher gegenüber Lauschern, wenn das entsprechende Diffie-Hellman Problem nicht gelöst werden kann:
  Gegeben $X = a^x, Y = a^y$, berechne a^{xy}.
- Aber: Wer sagt, dass man "sicher" nicht auch anders definieren kann? Vielleicht gibt es andere sinnvollle Definitionen.
- Dazu: Das Protkoll wird zur gemeinsamen Schlüsselerzeugung eingesetzt. Man will: Das Ergebnis soll (de facto) ununterscheidbar von einem echt zufälligen Element in $\{0, 1, \ldots, \mathrm{ord}(a) - 1\}$ sein.
- Dies führt zu einem anderen algorithmischen Problem, dem Diffie-Hellmann-Entscheidungsproblem:
  Gegeben $X = a^x, Y = a^y$, unterscheide a^{xy} von einem uniform zufälligen Element in $\{0, 1, \ldots, \mathrm{ord}(a) - 1\}$.

Zur Sicherheit III

Zur Sicherheit des Protokolls:

- Diffie-Hellman-Entscheidungsproblem (DDHP) (zu Parametern p und a):
  Gegeben $X = a^x$, $Y = a^y$, unterscheide a^{xy} von einem uniform zufälligen Element in $\{0, 1, \ldots, \mathrm{ord}(a) - 1\}$.
- Rechnerisches Diffie-Hellman-Problem (DHP) (zu p und a):
  Gegeben $X = a^x$, $Y = a^y$, berechne a^{xy}.
- Klassisches diskretes Logarithmusproblem (DLP) (zu p und a):
  Gegeben $X = a^x$, berechne x.
- Wir haben Reduktionen

$$\mathrm{DDHP} \leq \mathrm{DHP} \leq \mathrm{DLP}$$

Zur Sicherheit IV

- Das Protokoll ist vollkommen unsicher gegenüber aktiven Angreifern.
- Authentisierung fehlt!
- Für ein Protokoll mit Authentisierung will man zweigen: Jeder effiziente Angriff aus einer großen Angriffsklasse führt zu einem effizienten Algorithmus für das DH-Entscheidungsproblem (oder besser: für das recherische DH-Problem oder sogar für das DLP) (reduktives Sicherheitsresultat).

Zur Sicherheit kryptographischer Verfahren

Zur Sicherheit kryptographischer Verfahren

Eine Aussage der Form "Das Verfahren ist sicher" ist nur sinnvoll bezüglich eines klar definierten Angriffsszenarios.

Fragen, die man immer im Kopf haben sollte:

- Sicher gegenüber welcher Art von Angreifern?
  Oder: In welchem Kontext wird der Angriff betrachtet?

  Mögliche Arten von Angriffen bei Verschlüsselungssystemen sind z.B.:
  Lauscher, chosen palintext attack (gewählter-Klartext-Antriff), chosen ciphertext attack (gewählter-Chiffriertext-Angriff)

  Klare, umfassende Definitionen sind wichtig!

Zur Sicherheit kryptographischer Verfahren

- Angreifer mit welchen Ressourcen werden betrachtet?
  Unterscheidung zwischen
  - asyptotischen, qualitativen Betrachtungen zu Verfahren (Komplexitätstheorie)
    und
  - konkreten Betrachtungen für konkrete Parameter

    (z.B.: Angreifer kann eine Zahl $n = pq$ mit p, q je 500 bit nicht faktorisieren.)

Zur Sicherheit kryptographischer Verfahren

- Welche Annahmen werden getroffen?

  Was man gerne hätte:

  Wenn ein bestimmtes "schönes" Problem schwer ist, ist das Verfahren sicher in dem vorgegebenen Angriffsszenario.

  Z.B.:

  > Wenn das DLP nicht qualitativ effizient gelöst werden kann, ist das Verfahren qualitativ sicher bezüglich dieses Angriffsszenarios.

  Deutlich schwerer zu begründen sind solche Aussagen:

  Wenn das DLP für ein p mit x bit schwer ist, ist das Verfahren sicher bezüglich dieser und jener Angriffe.

Zur Sicherheit kryptographischer Verfahren

Alle Sicherheitsresultate ("Sicherheitsbeweise") zur Kryptographie mit öffentlichen Schlüsseln sind wenn-dann-Aussagen.

Selbst wenn scheinbar ein "Sicherheitsbeweis" vorliegt, kann ein Verfahren angreifbar sein

wegen:

- Angriffen außerhalb des Szenarios
  (insb. solche mit "Abstrahlung")
- Fehlern im "Beweis"
- Programmierfehlern
- Falscher Verwendung rein asyptotischer Resultate
- Das "unterliegende Problem" ist schwächer als angenommen.
  (Insbesondere könnte es ein merkwürdiges ad hoc Problem sein.)

Diese Vorlesung

Was wir machen und was nicht

Diese Vorlesung

Es geht im Folgenden weitgehend um grundlegende zahlentheoretische Methoden und Probleme für kryptographische Verfahren mit öffentlichen Schlüsseln:

- Zahlentheoretische Grundlagen, einfache Algorithmen
- Schwere, sicherheitsrelevante algorithmische Probleme:
  - das diskrete Logarithmenproblem
  - das Faktorisierungsproblem
- Algorithmen zum Lösen dieser Probleme

Dies ist ein Aspekt der Konstruktion in der Praxis sicherer Systeme.

Was wir durchnehmen werden

1. Grundlagen
2. Euklidische Ringe
3. Primzahltests
4. Endliche Körper
5. Faktorisierung
6. Berechnung diskreter Logarithmen
7. Elliptische Kurven

Literatur

C.D. Kryptologie – Methoden, Anwendungen und Herausforderungen

C.D. Skript zur Vorlesung Linearen Algebra für Mathematiker, insb. Kapitel 1 und Abschnitt 4.1

Neal Koblitz. A course in number theory and cryptography

Johannes Buchmann. Einführung in die Kryptographie

Eric Bach, Jeffrey Shallit. Algorithmic number theory

Steven Galbraith. Handbook of public key cryptography

Mögliche Projekte

1. Dicht besetzte Matrizen, Polynomfaktorisierung (wird benötigt in P8)
2. Dünn besetzte Matrizen, der Berlekamp-Massey- und der Wiedemann-Algorithmus (sollte benutzt werden in P6,P7,P8, P10)
3. Dünn besetzte Matrizen und der Lanczos-Algorithmus (sollte benutzt werden in P6,P7,P8, P10)
4. Generische Methoden für das Faktorisieren und das DLP
5. Elliptische Kurven und Faktorisierung mit Elliptischen Kurven
6. Faktorisieren mit Faktorbasis und Sieb
7. Faktorisieren mit Faktorbasis und Kettenbruchzerlegung
8. Diskrete Logarithmen in kleiner Charakteristik
9. Elliptische Kurven und Reduktion vom ECDLP zum DLP
10. Hyperelliptische Kurven und das diskrete Logarithmus Problem hierfür