Proseminar: Kryptographie

Alessandro Cobbe

Kryptographie

Das Wort *Kryptographie* stammt aus dem Griechischen: *kryptós* bedeutet *verborgen, geheim* und *gráphein* bedeutet *schreiben*. In der Kryptographie geht es darum, verschlüsselte Informationen zu versenden, ohne dass sie von Unberechtigten entschlüsselt werden können. Außerdem soll es möglich sein, die Authentizität der versendeten Nachrichten zu garantieren: Ein Angreifer sollte also auch nicht in der Lage sein, Inhalte von verschlüsselten Texten zu beeinflussen. Obwohl es sich um zwei verschiedene Probleme handelt, werden wir sehen, dass Verfahren zur Verschlüsselung von Texten oft in ähnlicher Form auch zur Sicherstellung der Integrität von Nachrichten benutzt werden können. Das Absichern von Nachrichten gegen technische Übertragungsfehler hingegen ist Aufgabe der Kodierungstheorie.

Bei den ersten historisch bekannten kryptographischen Verfahren handelt es sich um symmetrische Verfahren: Zum Verschlüsseln und Entschlüsseln einer Nachricht benötigt man denselben geheimen Schlüssel, den Sender und Empfänger beide im Vorfeld kennen müssen. Tatsächlich spielt diese Art von Verfahren auch heute noch eine sehr wichtige Rolle, aber mindestens genauso wichtig sind so-genannte Public-Key-Verfahren, in denen ein öffentlicher Schlüssel zum Verschlüsseln benutzt wird und ein dazu passender geheimer Schlüssel zum Entschlüsseln. Die Sicherheit dieser Verfahren basiert darauf, dass keine effizienten Algorithmen zum Lösen bestimmter arithmetischer Probleme bekannt sind, wie das Faktorisieren einer Zahl in Primfaktoren oder die Berechnung diskreter Logarithmen.

Ziel dieses Seminars ist es, einige kryptographische Verfahren zu verstehen, und deren Stärken und Schwächen zu untersuchen, insbesondere was die Sicherheit und die Effizienz der Kommunikation betrifft. Da sich das Seminar ausdrücklich auch an Studierende des zweiten Semesters wendet, werden nur ein paar Vorkenntnisse aus der Linearen Algebra 1 vorausgesetzt. Alle anderen mathematischen Grundlagen, die zum Verständnis der kryptographischen Verfahren notwendig sind, werden nach und nach in einigen Vorträgen besprochen.

Das Proseminar soll wöchentlich donnerstags von 11 bis 13 Uhr stattfinden. Pro Vortrag sind 90 Minuten vorgesehen. Für jeden Vortrag soll es auch eine kurze schriftliche Ausarbeitung geben, die bis etwa drei Wochen nach dem Vortrag abgegeben werden sollte. Der Schwerpunkt für die Note wird allerdings im Vortrag selbst liegen.

Das Proseminar wird am Donnerstag, den 16.02., um 18 Uhr vorgestellt. Die Besprechung wird online stattfinden; der Link dazu ist `https://bbb.unibw.de/ag4-nvv-bwq`, Zugangscode: 824516. Es ist nicht notwendig, externe Software zu installieren; alles läuft über dem Browser.

In den nächsten Seiten folgen die einzelnen Themen. Die Beschreibung ist bewusst knapp gehalten, und ich habe hauptsächlich eine Quelle für den Einstieg angegeben. Es wird aber wichtig sein, auch weitere Literatur zu recherchieren.

Themen

1 Das Vigenère-Verfahren und einige Verallgemeinerungen

Eine der ältesten bekannten Kryptoverfahren ist nach Julius Caesar benannt, und ist ziemlich offensichtlich nicht besonders sicher. Das Vigenère-Verfahren ist auf den ersten Blick besser, aber auch hier sind schon seit langer Zeit Angriffsmöglichkeiten bekannt. In diesem Vortrag soll sich die Betrachtung auch auf weitere Verallgemeinerungen richten, und es soll die Sicherheit dieser Varianten besprochen werden.

Quelle: [Buc15, 3.15-3.20].

2 Sicherheitsmodelle und Blockschiffren

Was bedeutet es eigentlich, dass ein kryptographisches Verfahren sicher ist? Die Antwort auf diese Frage ist nicht ganz so einfach, wie sie scheint, und hängt von den konkreten Anwendungsszenarien ab. Es werden hierzu verschiedene Sicherheitsmodelle eingeführt.

Als Anwendung soll erklärt werden, wie man Blockchiffren sicher einsetzen kann, und wie nicht. Blockchiffren sind Verschlüsselungsverfahren für Wörter einer festen Länge. Die Frage ist: Wie verschlüsselt man längere Wörter? Die Antwort ist auch hier nicht ganz so einfach, wie man sich vorstellen könnte.

Quelle: [Buc15, Kapitel 4] und [Buc15, 3.7-3.12].

3 Die Enigma-Maschine

Dass die Enigma-Maschine kein sicheres Verschlüsselungsverfahren ist, ist bekannt. Anhand der Sicherheitsmodelle aus Vortrag 2 ist es nicht schwierig, ein grundlegendes Problem der Enigma zu erkennen.

In diesem Vortrag soll etwas tiefer darauf eingegangen werden, wie mit der Enigma-Maschine verschlüsselte Nachrichten im Zweiten Weltkrieg von den Alliierten entschlüsselt werden konnten.

Quelle: [Gre09]

4 DES und AES

Wir kommen hier zu DES, dem ersten modernen Algorithmus, der zum Teil auch heute noch benutzt wird, wenn auch nur in der Variante 3DES. Es handelt sich hier um ein symmetrisches Verfahren, d.h. die Personen, die kommunizieren möchten, müssen schon vor Beginn der Kommunikation einen gemeinsamen geheimen Schlüssel besitzen. Das Verfahren selbst ist relativ kompliziert und besteht aus mehreren Schritten; jeder einzelne Schritt ist eine geschickte Kombination von Bitpermutationen, Additionen modulo 2 und Benutzung von gewissen festgelegten S-Boxen. Das einfache DES gilt inzwischen nicht mehr als sicher, weil die Schlüssellänge zu kurz ist und ein Brute-Force Angriff funktionieren würde; die Variante 3DES (dreifache Anwendung von DES) ist aber immer noch recht verbreitet.

Das modernste symmetrische Verfahren ist der AES-Algorithmus. Dieser soll ebenfalls skizziert werden, wenn auch nicht im Detail.

Quelle: [Buc15, Kapitel 5 und 6].

5 Kongruenzringe und endliche Körper

Wir wollen jetzt die mathematischen Grundlagen einführen, um einige bekannte Public-Key Verschlüsselungsverfahren zu verstehen.

Als erstes beschäftigen wir uns mit dem Ring $\mathbb{Z}/n\mathbb{Z}$ der ganzen Zahlen modulo einer Zahl $n > 1$. Ziel ist es zu verstehen, welche Elemente in $\mathbb{Z}/n\mathbb{Z}$ Einheiten sind, wie man Inverse berechnet, und für welche n der Ring $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist.

Parallel soll auch gezeigt werden, dass man ähnlich vorgehen kann, wenn man $\mathbb{Z}$ durch einen Polynomring $K[x]$ in einer Variablen mit Koeffizienten in einem Körper betrachtet. Auch hier soll untersucht werden, wann man einen Körper erhält.

Quelle: [For15, Kapitel 4, 6].

6 Der chinesische Restsatz und die Sätze von Fermat und Euler

In diesem Vortrag sollen diese wichtigen Sätze vorgestellt und bewiesen werden.

Es soll auch der Square and Multiply Algorithmus erklärt werden, mit dem man effizient Potenzen in einem Ring berechnen kann, sobald man effizient im Ring multiplizieren kann.

Quelle: [For15, Kapitel 6-7].

7 Primzahlen

Hier sollen die Begriffe *Primelement* und *irreduzibles Element* eingeführt werden und deren Zusammenhänge untersucht werden. Dann werden (probabilistische) Primzahltests diskutiert, insbesondere der Fermat-Test und der Miller-Rabin-Test.

In diesem Kontext lohnt es sich, auch einiges über Carmichael-Zahlen zu sagen.

Quelle: [For15, Kapitel 12].

8 RSA

Das RSA-Kryptosystem ist eines der ältesten Public-Key-Verfahren, und es ist immer noch weit verbreitet in den Anwendungen. Das Verschlüsseln funktioniert durch Potenzieren modulo einer Zahl n mit einem öffentlichen Exponenten e; fürs Entschlüsseln braucht man einen anderen geheimen Exponenten d. Um d zu bestimmen, wenn man nur n und e kennt, müsste man die Zahl n faktorisieren, was für sehr große Zahlen mit herkömmlichen Computern nicht machbar ist (mit einem Quantencomputern wäre das anders).

Für das Besprechen der Sicherheit soll auf die in Vortrag 2 besprochenen Sicherheitsmodelle Bezug genommen werden. Dabei werden einige Feinheiten auffallen, die für eine praktische Umsetzung zu beachten sind.

Quelle: [For15, Kapitel 15].

9 Faktorisierungsalgorithmen

Für das RSA-Verfahren benutzt man in der Regel Zahlen n, die ein Produkt von zwei Primfaktoren p und q sind. Typische Größenordnungen für n sind 2048 oder 4096 Bits, also $n \approx 2^{2048}$ oder $n \approx 2^{4096}$. Es ist also klar, dass man nicht alle Primteiler bis $\sqrt{n}$ einfach ausprobieren kann, auch nicht mit einem Computer. Dieser Algorithmus hat eine exponentielle Laufzeit in der Bitlänge. Die Frage ist: Geht es effizienter? Idealerweise würde man sich eine polynomiale Laufzeit wünschen. Tatsächlich gibt es Algorithmen, die besser sind als der oben beschriebene naive Ansatz, aber es sind keine Algorithmen bekannt, die in Polynomialzeit ein Ergebnis liefern (außer in Spezialfällen, die man in der Kryptographie bewusst vermeiden muss). In diesem Vortrag sollen einige dieser Ansätze erklärt werden.

Quelle: [For15, Kapitel 14], [Buc15, Kapitel 9].

10 Diffie-Hellman und ElGamal

Das Diffie-Hellman Verfahren ist eigentlich kein Kryptosystem, da man es nicht direkt benutzen kann, um Nachrichten zu übermitteln, sondern ein Verfahren, um ein gemeinsames Geheimnis zwischen zwei Personen zu erzeugen, woraus man einen Schlüssel für ein symmetrisches Kryptosystem herleiten kann, wie z.B. 3DES oder AES. Die Idee ist, ein öffentlich bekanntes Element γ aus einer Gruppe G mit gewissen geheimen Exponenten zu potenzieren und die Ergebnisse an den jeweils anderen zu schicken. Für den Vortrag konzentrieren wir uns auf die multiplikative Gruppe von $\mathbb{Z}/p\mathbb{Z}$, wobei p eine große Primzahl ist. Das ElGamal System ist eine Variante des Diffie-Hellman Verfahrens, womit man auch direkt eine Nachricht versenden kann.

Quelle: [Buc15, Kapitel 8.6-8.7].

11 Diskreter Logarithmus

Die Sicherheit der Verfahren von Diffie-Hellman und ElGamal beruht auf der Schwierigkeit der Berechnung diskreter Logarithmen. Das heißt: Man kennt Elemente α, γ aus einer Gruppe G (z.B. $\mathbb{Z}/p\mathbb{Z}^\times$, wie oben) und sucht $x \in \mathbb{N}$, so dass $\alpha = \gamma^x$. Wie bei der Faktorisierung, hat auch hier der naive Algorithmus eine exponentielle Laufzeit und ist somit in der Praxis unbrauchbar. Ähnlich wie bei der Faktorisierung gibt es auch hier viele interessante Ansätze, aber es ist kein Algorithmus mit polynomialer Laufzeit bekannt.

Quelle: [Buc15, Kapitel 10].

12 Digitale Signaturen

Genauso wichtig wie die Geheimhaltung von Nachrichten ist die Überprüfung deren Authentizität. Dazu gibt es digitale Signaturen, die zum großen Teil auf denselben Ideen beruhen, wie entsprechende Public-Key Kryptosysteme.

Quelle: [Buc15, Kapitel 12].

13 Das Goldwasser-Micali Kryptosystem

Das Goldwasser-Micali Kryptosystem basiert auf der Idee, dass es keine effizienten Algorithmen gibt, um zu entscheiden, ob eine Zahl ein Quadrat modulo n ist oder nicht, ohne die Zahl n zu faktorisieren.

Quelle: [KL21, 11.1].

Literatur

[Buc15] Johannes Buchmann. *Einführung in die Kryptographie.* Berlin: Springer, 6. Auflage, 2015.

[For15] Otto Forster. *Algorithmische Zahlentheorie.* Springer-Verlag, 2. Auflage, 2015.

[Gre09] Cornelius Greither. *Mathematik und Geheimhaltung.* mathe-lmu.de, Heft 19, Januar 2009. `https://www.math.lmu.de/~fmwus/download/ausgabe19.pdf`

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL, 2021. Third edition.