



PROF. DR. DR. STEFAN SCHÄFFLER
DIPL.-MATH. ARIANE SUTOR



Institut für Mathematik und
Datenverarbeitung
Fakultät für Elektrotechnik
und Informationstechnik
85577 Neubiberg
Tel.: 089/6004 2633
Fax: 089/6004 2615
stefan.schaeffler@unibw-muenchen.de

Kryptographie

Winter 2002

Inhaltsverzeichnis

1	Ziele und historische Entwicklung	3
1.1	Nachricht und Information	3
1.1.1	Transposition und Substitution	4
1.1.2	Kryptoanalyse monoalphabetischer Chiffren	7
1.2	Perfekte Sicherheit	10
1.2.1	Kryptosysteme	10
1.2.2	Perfekte Sicherheit	10
2	Mathematische Grundlagen	14
2.1	Gruppen, erzeugende Elemente	14
2.2	Rechnen in Restklassengruppen	16
2.3	Der größte gemeinsame Teiler	17
2.4	Primzahlen	18
2.5	Körper	18
3	Public-Key-Kryptographie	19
3.1	Trapdoor-Einwegfunktionen	19
3.2	Das RSA-Verfahren	20
3.3	Der diskrete Logarithmus	21
3.4	Das Verschlüsselungsverfahren von El Gamal	21
3.5	Elliptische Kurven	22
4	Zero-Knowledge-Verfahren	25
4.1	Authentikationssysteme	25
4.2	Der Fiat-Shamir-Algorithmus	26

Kapitel 1

Ziele und historische Entwicklung

1.1 Nachricht und Information

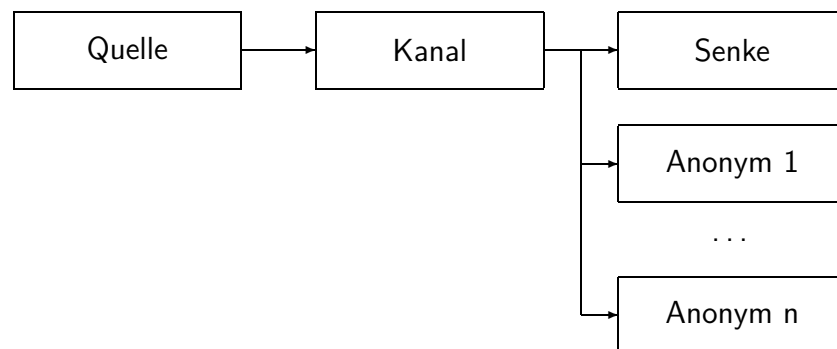
Um die Ziele der Kryptographie darstellen zu können, betrachten wir zunächst ein einfaches Nachrichtenübertragungssystem:



Dabei sollen die Quelle und die Senke über den gleichen Zeichenvorrat $\mathcal{A}$ verfügen (etwa das Alphabet $\{A, B, C, D, \dots\}$). Ziel ist es nun, eine Folge von Einzelzeichen aus $\mathcal{A}$ über den Kanal von der Quelle zur Senke zu übertragen. Eine im allgemeinen endliche Folge von Zeichen aus $\mathcal{A}$ wird als Nachricht bezeichnet. Eine Nachricht entsteht somit immer in der Quelle und hat das Ziel, der Senke etwas mitzuteilen. Daher besteht eine Nachricht aus einer Darstellungs- und einer Bedeutungskomponente. Die Bedeutungskomponente repräsentiert den Inhalt der Nachricht, während die Darstellungskomponente die Darstellung der Nachricht durch eine endliche Folge von Zeichen repräsentiert.

Von der Nachricht genau zu unterscheiden ist der Begriff der Information. Information entsteht immer in der Senke und zwar genau dann, wenn der Inhalt der Nachricht der Senke nicht vollständig bekannt war. In der Informationstheorie lassen sich die entsprechenden Begriffe mit wahrscheinlichkeitstheoretischen Hilfsmitteln exakt definieren.

Die Kryptographie beschäftigt sich in diesem Zusammenhang mit der Darstellung einer Nachricht, also nicht mit dem Inhalt und auch nicht mit der Information, die durch die Nachricht bei der Senke ankommt. Der Nachrichteninhalt ist vorgegeben und die Frage, ob diese Nachricht für die Senke einen Informationsgewinn bedeutet, ist in der Kryptographie irrelevant. Zur Verdeutlichung der Aufgabenstellung der Kryptographie betrachten wir ein erweitertes Nachrichtenübertragungssystem:



Nun wird davon ausgegangen, daß nicht nur die Senke die Nachricht erhält, sondern auch andere, im allgemeinen unbefugte Personen oder Institutionen die Nachricht (genauer: die endliche Folge von Zeichen) erhalten. Die Aufgabe der Kryptographie besteht darin, die Darstellung der Nachricht so zu wählen, daß Unbefugten die Bedeutung der Nachricht verschlossen bleibt. Die Kryptographie hat also *nicht* die Aufgabe zu verheimlichen, daß überhaupt eine Nachricht übertragen wird. Das ist das Ziel der Steganographie.

Eine Nachricht wird im folgenden als „Klartext“ bezeichnet. Die durch kryptographische Methoden verschlüsselte Nachricht (also die Nachricht, die tatsächlich übermittelt wird) wird „Geheimtext“ genannt.

1.1.1 Transposition und Substitution

Aus historischer Sicht sind zwei prinzipielle Vorgehensweisen bei der Verschlüsselung (Chiffrierung) von Nachrichten wichtig: die Transposition und die Substitution. Bei der Transposition wird einfach die Reihenfolge der einzelnen Zeichen nach einem festen Schema, das natürlich der Senke bekannt sein muß, geändert.

Kennt ein anonymer Empfänger dieses Schema nicht, so erhält er im allgemeinen eine Nachricht ohne Bedeutung. Die Transposition ist die älteste, durch literarische Quellen überlieferte Verschlüsselungstechnik. Nach dem Zeugnis des griechischen Historikers Plutarch benutzte die Regierung in Sparta die folgende Methode zur Übermittlung geheimer Nachrichten an ihre Generale:

Sender (Quelle) und Empfänger (Senke) mußten beide eine Skytale haben; das waren Zylinder mit genau dem gleichen Radius. Der Sender wickelte ein schmales Band aus Pergament spiralförmig um seinen Zylinder und schrieb dann die Nachricht der Länge nach auf das Band. War das Band abgewickelt, konnte die Nachricht nur von einer Person gelesen werden, die einen Zylinder genau desselben Umfangs hatte - hoffentlich nur der Empfänger. Die Wirkung der Skytale läßt sich an folgendem Beispiel zeigen. Nehmen wir an, wir hätten einen Papierstreifen mit folgender Buchstabenfolge abgefangen:

SIEIYHITIEPICINLTEHSZDO!ETIEG RDGRR HAEKA ESZRP

Die Skytale des Senders hat einen Umfang, den wir durch die Anzahl u von Buchstaben ausdrücken können.

$u = 5$:

SHP...
III...
ETC...
III...
YEN...

Man kann hier erkennen, daß aus den gegebenen Buchstabenkombinationen kein deutscher Text entstehen wird.

$u = 6$:

SICHERHE
ITISTDAS
EINZIGES
IELDERKR
YPTOGRAP
HIE!

Hier wurde u richtig gewählt; wie man oben sieht, lautet die Nachricht im Klartext: *„Sicherheit ist das einzige Ziel der Kryptographie!“*

Die Skytale ist der Prototyp eines Transpositionsalgorithmus. Die Buchstaben bleiben, was sie sind, aber nicht, wo sie sind. Im Gegensatz dazu wird bei der Substitution jedes Zeichen durch ein anderes Zeichen ersetzt.

Ein Spezialfall der Substitutionsmethode ist die von C. I. Caesar verwendete Verschiebetechnik.

ABCDEFGH...WXYZ $\rightarrow$ Klartext

DEFGHIJ...ZABC $\rightarrow$ Geheimtext

Für die Ver- und Entschlüsselung muß man sich nur die Anzahl der Verschiebestellen (nach links oder rechts) merken.

Wenn man zur Verschlüsselung von Buchstaben Computer verwenden will, so identifiziert man möglicherweise „A“ mit 1, „B“ mit 2, ..., „Y“ mit 25 und „Z“ mit 0. Mit dieser Darstellung kann man die Verschiebechiffrierung besonders gut darstellen:

- Zunächst wird der Klartext in die entsprechende Zahl übersetzt;
- dann wird zu dieser Zahl die Zahl s addiert (entspricht einer Verschiebung um s Stellen);
- vom Ergebnis betrachtet man den Rest bei Division durch 26 (man rechnet *modulo 26*).

- Die so erhaltene Zahl repräsentiert den Geheimtextbuchstaben.

Beispiel: Caesar-Chiffre, $s = 3$

Klartext	entspr. Zahl	$+s$	Ergebnis	<i>modulo 26</i>	Geheimtext
A	1	3	4	4	D
B	2	3	5	5	E
C	3	3	6	6	F
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
W	23	3	26	0	Z
X	24	3	27	1	A
Y	25	3	28	2	B
Z	0	3	3	3	C

Bei der Dechiffrierung ist einfach 3 zu subtrahieren, wobei gilt:

$$2 - 3 = 25 \pmod{26}$$

$$1 - 3 = 24 \pmod{26}$$

$$0 - 3 = 23 \pmod{26}$$

Mit dieser Methode kann man quasi Buchstaben addieren. Es stellt sich nun die Frage, ob man auch Multiplizieren könnte. Dazu ein Beispiel. Multipliziert man zum Beispiel mit der Zahl 2, so erhält man:

Klartext	entspr. Zahl	$\cdot t$	Ergebnis	<i>modulo 26</i>	Geheimtext
A	1	2	2	2	B
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
H	8	2	16	16	P
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
U	21	2	42	16	P

Beim Dechiffrieren könnte man dem Buchstaben „P“ im Geheimtext keinen eindeutigen Klartextbuchstaben zuordnen. Solche Verschlüsselungen sind unbrauchbar. Allerdings gibt es Faktoren t , die eine sinnvolle Chiffrierung liefern, nämlich $t \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ (alle zu 26 teilerfremden natürlichen Zahlen). Dabei wird eine Chiffrierung als sinnvoll bezeichnet, falls jedem Buchstaben des Geheimtextes eindeutig ein Klartextbuchstabe zugeordnet werden kann.

Selbstverständlich kann man Multiplikation und Addition verknüpfen und erhält somit eine von $12 \cdot 26 = 312$ möglichen Tauschchiffren, gegeben durch

$$t \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \text{ und } s \in \{0, \dots, 25\}.$$

Die Verschlüsselung ist durch die Chiffrierabbildung

$$f : \{0, \dots, 25\} \rightarrow \{0, \dots, 25\}, x \mapsto (x \cdot t) + s \pmod{26}$$

gegeben.

Beispiel: $t = 3, s = 5$

Klartext	entspr. Zahl	Ergebnis	Geheimtext
A	1	8	H
B	2	11	K
⋮	⋮	⋮	⋮
L	12	$41 \rightarrow 15$	O
⋮	⋮	⋮	⋮

Die Senke hat nun mit Wissen der beiden Zahlen (s, t) die Verschlüsselung rückgängig zu machen, also die Chiffrierabbildung f umzukehren (z. B. aus 15 (O) wird 12 (L)).

Es gilt somit $(15 - 5) \div 3 = 12 \pmod{26}$, denn $((12 \cdot 3) + 5) \div 26 = 1 \text{ Rest } 15$.

Das Zahlenpaar (s, t) wird als Schlüssel bezeichnet und repräsentiert die Information, die zum Entschlüsseln von Tauschchiffren nötig ist. Es gibt für das deutsche Alphabet 312 verschiedene Schlüssel.

Die entscheidende Frage: Sind diese 312 Tauschchiffren gute Chiffren? Die Antwort liefert das in der Kryptographie grundlegende **Prinzip von Kerckhoff**:

Die Sicherheit (und damit die Güte) einer Verschlüsselungstechnik darf nicht von der Geheimhaltung der Art der Verschlüsselung abhängen (z. B. Transposition, Tauschchiffren, ...), sondern nur von der Geheimhaltung des Schlüssels.

Da es bei den Tauschchiffren nur 312 verschiedene Schlüssel für das deutsche Alphabet gibt, ist diese Art der Verschlüsselung sehr unsicher.

1.1.2 Kryptoanalyse monoalphabetischer Chiffren

Eine Chiffrierung heißt monoalphabetisch, falls jeder Buchstabe des Alphabets stets zu demselben (Geheimtext-) Buchstaben verschlüsselt wird. Eine monoalphabetische Chiffrierung kann man immer so darstellen, da man unter das Klartextalphabet das Geheimtextalphabet schreibt. Diese Alphabete müssen nicht übereinstimmen:

Klartext	A	B	C	D	E	...
Geheimtext	N	f	ð	R	©	...

Die Substitutionsalgorithmen beschreiben monoalphabetische Chiffren. Während sich die Kryptographie mit der Verschlüsselung von Nachrichten beschäftigt, besteht die Aufgabe der Kryptoanalyse im (vom Sender unerwünschten) Brechen der

Chiffrierung. Beide - die Kryptographie und die Kryptoanalyse - werden unter dem Oberbegriff Kryptologie zusammengefaßt. Da eine Nachricht im allgemeinen in einer Sprache formuliert wird und da in keiner Sprache jeder Buchstabe gleich häufig vorkommt, sind monoalphabetische Chiffren leicht zu brechen.

Für das Deutsche gilt folgende Statistik:

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
A	6,51	N	9,78
B	1,89	O	2,51
C	3,06	P	0,79
D	5,08	Q	0,02
E	17,4	R	7,00
F	1,66	S	7,27
G	3,01	T	6,15
H	4,76	U	4,35
I	7,55	V	0,67
J	0,27	W	1,89
K	1,21	X	0,03
L	3,44	Y	0,04
M	2,53	Z	1,13

Für Buchstabenpaare gilt:

Buchstabenpaar	Häufigkeit in %	Buchstabenpaar	Häufigkeit in %
en	3,88	er	3,75
ch	2,75	te	2,26
de	2,00	nd	1,99
ei	1,88	ie	1,79
in	1,67	es	1,52
⋮	⋮	⋮	⋮

Mit Statistiken dieser Art hat der Kryptoanalytiker keine Probleme, mit dem Rechner in Deutsch verfasste Klartexte, die monoalphabetisch chiffriert werden, aus dem Geheimtext zu rekonstruieren, obwohl es für das deutsche Alphabet $26! \approx 4 \cdot 10^{26}$ verschiedene Chiffrierungen gibt.

Beispiel:

MRNBNA CNGC RBC WRLQC VNQA PNQNRV

1. Setze $E \Rightarrow N$.

MRNBNA CNGC RBC WRLQC VNQA PNQNRV
 ..E.E. .E..E.. .E.E..

2. Teste alle Möglichkeiten mit R, C, Q ersetzt durch A, D, H, I, N, R, S, T, U ($\geq 4\%$).

MRNBNA CNGC RBC WRLQC VNQA PNQNRV
 .IE.E. TE.T I.T .I.HT .EH. .EHEI.

3. Vervollständige zu sinnvollen deutschen Wörtern, d. h. setze
 $B \Rightarrow S$, $M \Rightarrow D$, $G \Rightarrow X$.

MRNBNA CNGC RBC WRLQC VNQA PNQNRV
 DIESE. TEXT IST .I.HT .EH. .EHEI.

4. ...
 5. Als Klartext ergibt sich schließlich: DIESER TEXT IST NICHT MEHR
 GEHEIM.

1.2 Perfekte Sicherheit

1.2.1 Kryptosysteme

Bei der Frage der Sicherheit von Chiffren benötigt man den Begriff des Kryptosystems.

Definition Kryptosystem

Ein Kryptosystem ist ein Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ bestehend aus fünf Mengen.

- $\mathcal{P}$ heißt **Klartextraum**. In dieser Menge werden alle in Betracht kommenden Klartexte (Nachrichten) gesammelt (z. B. alle möglichen endlichen Folgen von Buchstaben aus dem deutschen Alphabet, die aus Wörtern der deutschen Sprache gebildet sind und aus weniger als 1000 Zeichen bestehen).
- $\mathcal{C}$ heißt **Geheimtextraum**: in dieser Menge werden alle in Frage kommenden Geheimtexte gesammelt: $\mathcal{C} := \{e_k(p), k \in \mathcal{K}, p \in \mathcal{P}\}$.
- $\mathcal{K}$ heißt **Schlüsselraum**. Darin sind alle zu betrachtenden Schlüssel gesammelt.
- $\mathcal{E}$ ist eine Menge $\{e_k : \mathcal{P} \rightarrow \mathcal{C}; k \in \mathcal{K}\}$ von **Verschlüsselungsfunktionen**.
- $\mathcal{D}$ ist eine Menge $\{d_k : \mathcal{C} \rightarrow \mathcal{P}; k \in \mathcal{K}\}$ von **Entschlüsselungsfunktionen** derart, daß es zu jedem Schlüssel $k_1 \in \mathcal{K}$ ein $k_2 \in \mathcal{K}$ gibt mit $d_{k_2}(e_{k_1}(p)) = p \forall p \in \mathcal{P}$. Mit anderen Worten: zu jedem Schlüssel $k_1 \in \mathcal{K}$ muß es einen anderen Schlüssel $k_2 \in \mathcal{K}$ geben, so daß die mit k_1 verschlüsselte Nachricht mit k_2 wieder entschlüsselt werden kann. Ist $k_1 = k_2$, so nennt man das Kryptosystem „symmetrisch“, ansonsten „asymmetrisch“.

Betrachten wir ein Beispiel:

Sei $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, \dots, 25\}$ und $\mathcal{E} = \{e_k : \mathcal{P} \rightarrow \mathcal{C}; x + k \pmod{26}\}$, $\mathcal{D} = \{d_k : \mathcal{C} \rightarrow \mathcal{P}; x - k \pmod{26}\}$, so ist dies gerade die Verschiebechiffre. Es gilt $d_k(e_k(p)) = ((p + k) \pmod{26} - k) \pmod{26} = p$, also ist $k_1 = k_2$, d. h. bei diesem Kryptosystem muß der Schlüssel geheimgehalten werden.

1.2.2 Perfekte Sicherheit

Wir untersuchen die Frage, wann es sinnvoll ist, ein gegebenes Kryptosystem als perfekt sicher zu bezeichnen. Bei der Kryptoanalyse der monoalphabetischen Chiffrierung wurde trotz einer sehr großen Zahl von Schlüsseln klar, daß diese Chiffrierung unsicher ist, denn die Struktur der deutschen Sprache, die natürlich im Klartext zum Ausdruck kommt, wurde auf den Geheimtext übertragen. Dadurch waren Rückschlüsse vom Geheimtext auf den Klartext möglich. Um nun Abhängigkeiten der inneren Struktur der Klar- und Geheimtexte ausschließen zu können, benötigt man

ein formales Werkzeug. Dieses Werkzeug ist die Wahrscheinlichkeitstheorie. Dabei gehen wir von gegebenen Wahrscheinlichkeitsverteilungen

$$\mathbf{P}_{\mathcal{P}} : \mathcal{P} \rightarrow [0, 1], p \mapsto \mathbf{P}_{\mathcal{P}}(p) > 0$$

und

$$\mathbf{P}_{\mathcal{K}} : \mathcal{K} \rightarrow [0, 1], k \mapsto \mathbf{P}_{\mathcal{K}}(k) > 0$$

aus. $\mathbf{P}_{\mathcal{P}}(p)$ ist also die Wahrscheinlichkeit, daß der Klartext p übertragen werden soll, und $\mathbf{P}_{\mathcal{K}}(k)$ ist die Wahrscheinlichkeit dafür, daß für die Übertragung der Schlüssel k verwendet wird. Ferner nehmen wir an, daß die Wahl des Schlüssels nicht vom Klartext abhängt, d. h. wir haben eine Wahrscheinlichkeitsverteilung

$$\mathbf{P}_{\mathcal{P} \times \mathcal{K}} : \mathcal{P} \times \mathcal{K} \rightarrow [0, 1], (p, k) \mapsto \mathbf{P}_{\mathcal{P} \times \mathcal{K}}(p, k) = \mathbf{P}_{\mathcal{P}}(p) \cdot \mathbf{P}_{\mathcal{K}}(k) \quad \forall p \in \mathcal{P}, k \in \mathcal{K}$$

(stochastische Unabhängigkeit). $\mathbf{P}_{\mathcal{P} \times \mathcal{K}}(p, k)$ ist also die Wahrscheinlichkeit, daß der Klartext p mit dem Schlüssel k übertragen wird.

Nehmen wir an, wir haben den Geheimtext $c \in \mathcal{C}$ abgehört, wir kennen das verwendete Kryptosystem und wir kennen die Wahrscheinlichkeitsverteilungen $\mathbf{P}_{\mathcal{P}}, \mathbf{P}_{\mathcal{K}}$. Unsere Aufgabe besteht nun darin, das zu $c \in \mathcal{C}$ gehörige $p \in \mathcal{P}$ zu finden. Hätten wir c nicht, so stünde nur $\mathbf{P}_{\mathcal{P}}(p)$ und $\mathbf{P}_{\mathcal{K}}(k)$ zur Verfügung. Wenn es möglich ist, mit Hilfe von c eine neue Wahrscheinlichkeitsverteilung

$$\mathbf{P}_{\mathcal{P}|c} : \mathcal{P} \rightarrow [0, 1]$$

auf $\mathcal{P}$ anzugeben, die nicht gleich $\mathbf{P}_{\mathcal{P}}$ ist und somit die Aufgabe erleichtert, das zu c gehörige p zu finden, dann hat uns das Abhören von c geholfen, ansonsten nicht. Aufgrund von $\mathbf{P}_{\mathcal{P}}, \mathbf{P}_{\mathcal{K}}$ und der stochastischen Unabhängigkeit sind wir in der Lage, eine neue Wahrscheinlichkeitsverteilung auf $\mathcal{C}$ anzugeben:

$$\mathbf{P}_{\mathcal{C}} : \mathcal{C} \rightarrow [0, 1], \xi \mapsto \sum_{p \in \mathcal{P}, k \in \mathcal{K}, e_k(p) = \xi} \mathbf{P}_{\mathcal{P}}(p) \cdot \mathbf{P}_{\mathcal{K}}(k)$$

Summiert werden hier also alle $p \in \mathcal{P}$ und $k \in \mathcal{K}$, für die die Bedingung $e_k(p) = \xi$ gilt.

Ferner können wir eine Wahrscheinlichkeitsverteilung $\mathbf{P}_{\mathcal{C}|p}$ auf $\mathcal{C}$ angeben, die davon ausgeht, daß der Klartext $p \in \mathcal{P}$ gesendet wurde.

$$\mathbf{P}_{\mathcal{C}|p} : \mathcal{C} \rightarrow [0, 1], \xi \mapsto \sum_{k \in \mathcal{K}, e_k(p) = \xi} \mathbf{P}_{\mathcal{K}}(k)$$

Mit diesen Zutaten ist es nun unter Verwendung des **Satzes von Bayes**¹ möglich, $\mathbf{P}_{\mathcal{P}|c}$ zu berechnen:

¹Beispiel zum Satz von Bayes:

gegeben seien die Ereignisse F: „Person ist eine Frau“ und R: „Person ist Raucher“. Die Wahrscheinlichkeiten $\mathbf{P}(F), \mathbf{P}(R), \mathbf{P}(R|F)$ seien bekannt. Die Wahrscheinlichkeit $\mathbf{P}(F|R)$ läßt sich folgendermaßen berechnen: $\mathbf{P}(F|R) = \frac{\mathbf{P}(R|F)}{\mathbf{P}(R)} \cdot \mathbf{P}(F)$.

$$\mathbf{P}_{\mathcal{P}|c} : \mathcal{P} \rightarrow [0, 1], p \mapsto \frac{\mathbf{P}_{c|p}(c)}{\mathbf{P}_c(c)} \cdot \mathbf{P}_{\mathcal{P}}(p)$$

Ist somit der Faktor $\frac{\mathbf{P}_{c|p}(c)}{\mathbf{P}_c(c)}$ gleich 1, so hat sich unser Wissen über die Wahrscheinlichkeitsverteilung durch das Abhören von c nicht verbessert. Ein solches Kryptosystem bezeichnen wir im folgenden als „perfekt sicher“.

Definition perfekt sicherer Kryptosysteme

Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit den entsprechenden Wahrscheinlichkeitsverteilungen $\mathbf{P}_{\mathcal{P}}, \mathbf{P}_{\mathcal{K}}$ und der stochastischen Unabhängigkeit von Klartext- und Schlüsselwahl. Dieses Kryptosystem heißt perfekt sicher, falls

$$\mathbf{P}_{\mathcal{P}}(p) = \mathbf{P}_{\mathcal{P}|c}(p) \quad \forall p \in \mathcal{P}, c \in \mathcal{C}$$

Das in der obigen Definition für perfekte Sicherheit gegebene Kryptosystem ist im allgemeinen nicht praktikabel (aber suggestiv), da in dieser Form kaum überprüfbar. Daher ist der folgende Satz von Claude Shannon von zentraler Bedeutung.

Kriterium für perfekte Sicherheit von Claude Shannon

Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem und die Anzahl der Elemente von $\mathcal{C}$ gleich der Anzahl der Elemente von $\mathcal{K}$ und $\mathcal{P}$. (in Zeichen: $|\mathcal{C}| = |\mathcal{K}| = |\mathcal{P}|$). Das Kryptosystem ist genau dann perfekt sicher, wenn

$$\mathbf{P}_{\mathcal{K}}(k) = \frac{1}{|\mathcal{K}|} \quad \forall k \in \mathcal{K}$$

(Gleichverteilung) und wenn es zu jedem $p \in \mathcal{P}$ und $c \in \mathcal{C}$ genau einen Schlüssel $k \in \mathcal{K}$ mit $e_k(p) = c$ gibt.

Entscheidend an diesem Satz ist die „genau dann“-Aussage, d. h.

- gilt für ein Kryptosystem $|\mathcal{C}| = |\mathcal{K}| = |\mathcal{P}|$, $\mathbf{P}_{\mathcal{K}}(k) = \frac{1}{|\mathcal{K}|}$ und existiert zu jedem $p \in \mathcal{P}, c \in \mathcal{C}$ genau ein $k \in \mathcal{K}$ mit $e_k(p) = c$, so ist dieses Kryptosystem perfekt sicher.
- ist das Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein perfekt sicheres Kryptosystem mit $|\mathcal{C}| = |\mathcal{K}| = |\mathcal{P}|$, so gilt: $\mathbf{P}_{\mathcal{K}}(k) = \frac{1}{|\mathcal{K}|}$ und zu jedem $p \in \mathcal{P}, c \in \mathcal{C}$ gibt es genau ein $k \in \mathcal{K}$ mit $e_k(p) = c$.

Das bekannteste Kryptosystem, dessen perfekte Sicherheit man mit Satz 2.2.2 beweisen kann, ist das 1917 von Gilbert Vernam erfundene und patentierte **One-Time-Pad**.

Dabei betrachtet man Bitstrings der Länge n , also $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n, n \in \mathbb{N}$. Die Verschlüsselungsfunktion e_k zum Schlüssel $k \in \{0, 1\}^n$ ist gegeben durch

$$e_k : \{0, 1\}^n \rightarrow \{0, 1\}^n, (p_1, \dots, p_n) \mapsto (p_1 \oplus k_1, \dots, p_n \oplus k_n)$$

(Addition ohne Übertrag). Will man einen Klartext p verschlüsseln, so wählt man gemäß einer Gleichverteilung einen Schlüssel $k \in \{0, 1\}^n$ und berechnet $c = e_k(p)$. Da es zu jedem $p \in \{0, 1\}^n, c \in \{0, 1\}^n$ genau einen Schlüssel $k \in \{0, 1\}^n$ gibt mit $c_i = p_i \oplus k_i, i = 1, \dots, n$, nämlich $k_i = p_i \oplus c_i$, ist dieses Kryptosystem perfekt sicher. Da auch $p_i = c_i \oplus k_i, i = 1, \dots, n$ gilt, ist dieses Kryptosystem zudem symmetrisch. Die perfekte Sicherheit ist dadurch erkaufte, daß zu jeder Übertragung eines Klartextes ein neuer gemäß Gleichverteilung erzeugter Schlüssel zu verwenden ist. Dieser Schlüssel muß der Senke bekannt sein. Entweder legt man die Schlüssel a priori fest, dann muß man sie speichern und geheimhalten, oder man überträgt den Schlüssel gesondert.

Kapitel 2

Mathematische Grundlagen

Die modernen Verfahren der Kryptographie nutzen im Wesentlichen Strukturen der diskreten Mathematik. Die mathematischen Gebiete der Algebra und der Zahlentheorie finden somit in der Kryptographie eine Anwendung. Algebra beschäftigt sich mit der Theorie algebraischer Strukturen, also mit Mengen und Verknüpfungen und gewissen Axiomen, die diese Verknüpfungen betreffen. Die Zahlentheorie hat die Menge der ganzen Zahlen $\mathbb{Z}$ und ihre Strukturen zum Gegenstand. In diesem Kapitel werden einige grundlegende Tatsachen aus der Algebra und der Zahlentheorie zusammengestellt, die für die Kryptographie gebraucht werden.

2.1 Gruppen, erzeugende Elemente

Ein zentraler Begriff der Algebra ist der Begriff einer Gruppe:

Definition 2.1 *Es sei $G \neq \emptyset$ eine Menge und $\circ : G \times G \rightarrow G$ eine Verknüpfung. $(G, \circ)$ heißt Gruppe, wenn die folgenden Bedingungen erfüllt sind:*

1. *$\circ$ ist assoziativ, d.h. für $a, b, c \in G$ gilt stets $(a \circ b) \circ c = a \circ (b \circ c)$.*
2. *Es gibt ein neutrales Element $e \in G$ mit $e \circ a = a \circ e = a$ für alle $a \in G$.*
3. *Zu jedem $a \in G$ gibt es ein $a^{-1} \in G$ mit $a \circ a^{-1} = a^{-1} \circ a = e$; a^{-1} heißt inverses Element.*

Gilt zusätzlich für alle $a, b \in G$ $a \circ b = b \circ a$, so heißt die Gruppe G kommutativ oder abelsch.

Eine Menge $H \neq \emptyset$ mit einer Verknüpfung $\circ$ bezeichnet man als Halbgruppe, falls $\circ$ assoziativ ist. $(H, \circ)$ kann ein neutrales Element e enthalten. Wegen $e \circ e = e$ enthält H dann auch ein zu e inverses Element. Allgemein heißt ein Element $x \in H$ Einheit, wenn H ein neutrales Element e und ein zu x inverses Element y enthält. Die Einheiten einer Halbgruppe H bilden sogar eine Gruppe $E(H)$. Wegen $e \in E(H)$ gilt $E(H) \neq \emptyset$.

Die Verknüpfung $\circ$ einer Gruppe wird meist als Addition $+$ oder Multiplikation $\cdot$ geschrieben. Beispiele kommutativer Gruppen sind $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ und

$(\mathbb{Z}, +)$. $(\mathbb{Z}, \cdot)$ ist eine kommutative Halbgruppe mit neutralem Element 1, aber keine Gruppe.

Eine Teilmenge U einer Gruppe $(G, \circ)$ heißt Untergruppe von G , falls U mit der auf U eingeschränkten Verknüpfung $\circ$ selbst eine Gruppe ist. Man schreibt dann $U < G$. Ein leicht überprüfbares Kriterium, ob eine gegebene Teilmenge $U \neq \emptyset$ von G eine Untergruppe ist, ist das folgende:

$$U < G \iff a, b \in U \Rightarrow a \circ b^{-1} \in U.$$

Offensichtlich sind also G und $\{e\}$ Untergruppen von $(G, \circ)$. Die Menge aller Untergruppen wird mit $\mathcal{U}(G)$ bezeichnet. Mit zwei Untergruppen $U, V \in \mathcal{U}(G)$ ist auch ihr Durchschnitt eine Untergruppe von G :

$$U, V \in \mathcal{U}(G) \Rightarrow U \cap V \in \mathcal{U}(G).$$

Damit ist die folgende Definition sinnvoll:

Definition 2.2 Seien G eine Gruppe und $X \subseteq G$. Der Durchschnitt aller Untergruppen von G , die X enthalten, wird als die von X erzeugte Untergruppe $\langle X \rangle$ bezeichnet:

$$\langle X \rangle = \bigcap_{\substack{U \in \mathcal{U}(G) \\ X \subseteq U}} U.$$

Eine Gruppe G heißt zyklisch, falls G von einem Element erzeugt wird, falls also ein $x \in G$ existiert mit $\langle x \rangle = G$.

Es sei nun $(H, \cdot)$ eine multiplikative Halbgruppe mit neutralem Element e . Dann definiert man die Potenz a^n eines Elementes $a \in H$ für alle $n \in \mathbb{N}$ rekursiv durch

$$a^0 := e, \quad a^n := a \cdot a^{n-1}.$$

Entsprechend definiert man für eine additive Halbgruppe $(H, +)$ das Vielfache na für alle $n \in \mathbb{N}$:

$$1a := a, \quad na := (n-1)a + a.$$

Sei G eine endliche Gruppe. Für die von einem Element $x \in G$ erzeugte Untergruppe in der Gruppe G gilt in multiplikativer Schreibweise

$$\langle x \rangle = \{x^n \mid n \in \mathbb{N}\}$$

und in additiver Schreibweise

$$\langle x \rangle = \{nx \mid n \in \mathbb{N}\}.$$

Damit ist es leicht einzusehen, daß jede zyklische Gruppe kommutativ ist.

2.2 Rechnen in Restklassengruppen

Ein wichtiges Beispiel einer zyklischen Gruppe ist die Menge $\mathbb{Z}$ der ganzen Zahlen mit der üblichen Addition. Es gilt

$$(\mathbb{Z}, +) = \langle 1 \rangle.$$

Zu jedem $n \in \mathbb{N}_0$ gibt es eine von n erzeugte Untergruppe:

$$n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}.$$

Es kann gezeigt werden, daß dies bereits alle Untergruppen von $(\mathbb{Z}, +)$ sind. Mit diesen Untergruppen definiert man eine neue Verknüpfung. Für $a, b \in \mathbb{Z}$ gelte

$$a \equiv b \pmod{n} : \Longleftrightarrow a - b \in n\mathbb{Z}.$$

Die rechte Seite besagt, daß es eine ganze Zahl $z \in \mathbb{Z}$ gibt mit $a - b = nz$; damit folgt, daß n die Differenz $a - b$ teilt, man schreibt auch $n \mid a - b$. Da $\equiv$ mit der Addition $+$ verträglich ist, kann gezeigt werden, daß

$$\mathbb{Z}_n := \{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$$

eine Gruppe ist mit dem neutralen Element $n\mathbb{Z}$, die Restklassengruppe modulo n . Dabei ist für $a \in \{1, \dots, n-1\}$ die Nebenklasse $a + n\mathbb{Z}$ definiert als $\{a + nz \mid z \in \mathbb{Z}\}$. $\mathbb{Z}_n$ enthält n Elemente und wird von $1 + n\mathbb{Z}$ erzeugt. Insbesondere ist $\mathbb{Z}_n$ eine zyklische Gruppe. Häufig wird $\mathbb{Z}_n$ kürzer dargestellt als

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}.$$

Dies sind die kleinsten nichtnegativen Reste modulo n . Für nichtnegative ganze Zahlen $m \in \mathbb{N}_0$ erhält man den zugehörigen kleinsten Rest modulo n durch ganzzahlige Division durch n . Um einer negativen ganzen Zahl $-m, m \in \mathbb{N}$, ihren kleinsten nichtnegativen Rest modulo n zuzuordnen, kann man zunächst ein geeignetes Vielfaches von n addieren, so daß eine positive ganze Zahl entsteht, und anschließend durch n dividieren.

Es läßt sich nun zeigen, daß $\equiv$ auch mit der Multiplikation $\cdot$ von $\mathbb{Z}$ verträglich ist, daß also durch

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := ab + n\mathbb{Z}$$

eine innere Verknüpfung in $\mathbb{Z}_n$ definiert wird. $(\mathbb{Z}_n, \cdot)$ ist eine kommutative Halbgruppe mit dem neutralen Element $1 + n\mathbb{Z}$. Die Einheitengruppe von $(\mathbb{Z}_n, \cdot)$ ist

$$E(\mathbb{Z}_n) = \{a + n\mathbb{Z} \mid \text{ggT}(a, n) = 1\}.$$

Sie wird als prime Restklassengruppe modulo n bezeichnet; man schreibt $E(\mathbb{Z}_n) = \mathbb{Z}_n^*$. Für die Anzahl der Elemente in $\mathbb{Z}_n^*$ gilt also

$$|\mathbb{Z}_n^*| = |\{k \in \mathbb{N} \mid k < n, \text{ggT}(n, k) = 1\}| =: \varphi(n).$$

Dabei heißt die Funktion $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ Eulersche φ -Funktion.

Beispiel 1 Für eine Primzahl $p \in \mathbb{N}$ läßt sich die Eulersche φ -Funktion leicht auswerten. Offensichtlich gilt $\varphi(p) = p - 1$. Für das Produkt zweier Primzahlen $p, q \in \mathbb{N}$ gilt $\varphi(pq) = (p - 1)(q - 1)$.

2.3 Der größte gemeinsame Teiler

Es seien $a, b \in \mathbb{Z} \setminus \{0\}$. Da die Untergruppen von $(\mathbb{Z}, +)$ bekannt sind, weiß man, daß es zu der von a, b erzeugten Untergruppe ein $d \in \mathbb{N}$ gibt mit $\langle a, b \rangle = d\mathbb{Z}$. Da außerdem a und b in $\langle a, b \rangle$ enthalten sind, folgt $d|a, b$, d. h. d ist ein gemeinsamer Teiler von a und b . Es gilt

$$d\mathbb{Z} = \langle a, b \rangle = \{ra + sb | r, s \in \mathbb{Z}\}.$$

Also gibt es Zahlen $x, y \in \mathbb{Z}$ für die gilt $d = xa + yb$. Für alle $t \in \mathbb{Z}$ mit $t|a, b$ gilt somit $t|d$, d. h. d ist der größte gemeinsame Teiler von a und b ; man schreibt $d = \text{ggT}(a, b)$. Es stellt sich nun die Frage, ob man den größten gemeinsamen Teiler zweier ganzer Zahlen leicht berechnen kann. Eine Antwort ist der euklidische Algorithmus (Euklid von Alexandria, um 365-300 v. Chr.).

Satz 2.3 (Euklidischer Algorithmus) Seien $a, b \in \mathbb{Z}, b \neq 0$. Mit $r_1 := a, r_2 := b$ bricht die Division mit Rest

$$r_i := q_i r_{i+1} + r_{i+2}$$

mit $|r_{i+2}| < |r_{i+1}|$ falls $r_{i+2} \neq 0$ nach höchstens $n \leq |b|$ Schritten ab, d. h. es gibt ein $n \leq |b|$ mit $r_{i+1} \neq 0$ für $i < n$ und $r_n = q_n r_{n+1} + 0$. Dann gilt: $d := r_{n+1} = \text{ggT}(a, b)$ und es können $x, y \in \mathbb{Z}$ bestimmt werden mit $d = xa + yb$.

Zur Begründung überlegt man sich, daß folgendes gilt:

$$\left. \begin{array}{l} r_{n+1} | r_n \\ r_{n-1} = q_{n-1} r_n + r_{n+1} \end{array} \right\} \Rightarrow r_{n+1} | r_{n-1} \Rightarrow \dots \Rightarrow r_{n+1} | b \Rightarrow r_{n+1} | a.$$

Die Schranke für die Anzahl der Iterationen kann wesentlich verbessert werden: Seien dazu $a > b > 0$ und $\theta := \frac{1+\sqrt{5}}{2}$. Dann ist die Anzahl der Iterationen im euklidischen Algorithmus höchstens $\frac{\log b}{\log \theta} + 1$. Den Ablauf des Algorithmus verdeutlicht man sich am besten anhand eines Beispiels.

Beispiel 2 Gesucht ist $d = \text{ggT}(36, 21)$. Der euklidische Algorithmus liefert

$$\begin{array}{ll} 36 &= 1 \cdot 21 + 15 \\ 21 &= 1 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{array} \qquad \begin{array}{ll} 15 &= 36 - 21 \\ 6 &= 21 - 15 \\ 3 &= 15 - 2 \cdot 6. \end{array}$$

Somit gilt $3 = \text{ggT}(36, 21)$ und $3 = 36 - 21 - 2(21 - (36 - 21)) = 3 \cdot 36 - 5 \cdot 21$.

Im letzten Abschnitt wurde die Einheitengruppe von $\mathbb{Z}_n$ angegeben, die prime Restklassengruppe modulo n . Um zu einem gegebenen Element aus $\mathbb{Z}_n^*$ ein inverses Element zu bestimmen, kann der euklidische Algorithmus verwendet werden. Sei also $c \in \mathbb{Z}_n^*$, d. h. $\text{ggT}(c, n) = 1$. Dann können Elemente d und m bestimmt werden mit $1 = cd + mn$; folglich gilt $cd \equiv 1 \pmod{n}$, d. h. d ist in $\mathbb{Z}_n^*$ das zu c inverse Element.

2.4 Primzahlen

Eine ganze Zahl $p \in \mathbb{Z}$ heißt Primzahl, falls aus $p = ab$ für $a, b \in \mathbb{Z}$ stets folgt $a \in E(\mathbb{Z}, \cdot) = \{1, -1\}$ oder $b \in E(\mathbb{Z}, \cdot)$. Eine Primzahl ist in diesem Sinne also unzerlegbar. Primzahlen spielen in $\mathbb{Z}$ eine fundamentale Rolle, wie der folgende Satz zeigt.

Satz 2.4 *Es sei $a \in \mathbb{Z} \setminus \{1, -1, 0\}$. Dann gibt es Primzahlen $p_1, \dots, p_n$ und eine Einheit e mit $a = ep_1 \cdot \dots \cdot p_n$. Diese Produktdarstellung ist bis auf Einheiten und die Reihenfolge der Faktoren eindeutig.*

Die Existenz der Produktdarstellung liefert noch kein effizientes Verfahren, wie man zu einer gegebenen ganzen Zahl ihre Primfaktoren bestimmt. Tatsächlich ist ein solches Verfahren bis heute nicht bekannt und im nächsten Kapitel wird ein kryptographisches Verfahren vorgestellt, das auf der Schwierigkeit des Faktorisierungsproblems beruht.

2.5 Körper

Bisher wurden Gruppen betrachtet, also Mengen mit einer inneren Verknüpfung, die meist als Addition oder Multiplikation interpretiert wurde. Körper sind Mengen mit zwei inneren Verknüpfungen.

Definition 2.5 *Eine Menge $(K, +, \cdot)$ mit zwei inneren Verknüpfungen $+$ und $\cdot$ heißt Körper, falls die folgenden Bedingungen erfüllt sind:*

1. $(K, +)$ ist eine abelsche Gruppe (mit neutralem Element 0).
2. $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe (mit neutralem Element 1).
3. Für alle $x, y, z \in K$ gilt das Distributivgesetz $x \cdot (y + z) = (x \cdot y) + (x \cdot z) := x \cdot y + x \cdot z$ (Punktrechnung geht vor Strichrechnung).

Man beachte, daß aus der Definition folgt, daß $0 \cdot x = 0$ für alle $x \in K$ gilt. Wichtige (unendliche) Körper sind der Körper der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$, der Körper der reellen Zahlen $(\mathbb{R}, +, \cdot)$ und der Körper der komplexen Zahlen $(\mathbb{C}, +, \cdot)$. In der Kryptographie spielen dagegen endliche Körper eine wichtige Rolle, beispielsweise bei der Definition des diskreten Logarithmus und bei der Kryptographie mit elliptischen Kurven. Das folgende Beispiel ist von fundamentaler Bedeutung.

Beispiel 3 *Sei p eine Primzahl. Wegen $\mathbb{Z}_p^* = \{a + p\mathbb{Z} \mid \text{ggT}(a, p) = 1\} = \{1, 2, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\}$ ist $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ eine (multiplikative) abelsche Gruppe. $\mathbb{Z}_p^*$ ist sogar zyklisch. Da $(\mathbb{Z}_p, +)$ eine (additive) abelsche Gruppe ist und da das Distributivgesetz erfüllt ist, ist somit $(\mathbb{Z}_p, +, \cdot)$ ein Körper. Für die Anzahl der Elemente dieses Körpers gilt $|\mathbb{Z}_p| = p$. Wegen $p \cdot x = 0 \cdot x = 0$ für alle $x \in \mathbb{Z}_p$ sagt man, daß $\mathbb{Z}_p$ die Charakteristik p hat.*

Kapitel 3

Public-Key-Kryptographie

3.1 Trapdoor-Einwegfunktionen

Im Jahr 1976 veröffentlichten Whitfield Diffie und Martin Hellman das Prinzip der Public-Key-Kryptographie. Bis zu diesem Zeitpunkt mussten zwei Teilnehmer (Quelle, Senke), die geheim kommunizieren wollten, schon vorher ein gemeinsames Geheimnis haben, den geheimen Schlüssel (Verwendung symmetrischer Kryptosysteme). Ab 1976 war es möglich, ohne jeden vorherigen Kontakt einer Person eine verschlüsselte Nachricht zu schicken, die nur sie selbst entschlüsseln kann. Grundlage dafür sind Trapdoor-Einwegfunktionen.

Betrachtet man ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, so ist eine Verschlüsselungsfunktion $e_{k_1} : \mathcal{P} \rightarrow \mathcal{C}$ eine Trapdoor-Einwegfunktion, falls e_{k_1} trotz Kenntnis des Schlüssels k_1 (und damit Kenntnis der kompletten Funktion e_{k_1}) praktisch (im Sinne der Komplexitätstheorie) nicht umkehrbar ist, also aus $c = e_{k_1}(p)$ das entsprechende p nicht berechnet werden kann (Einwegfunktionen), auf der anderen Seite mit Hilfe einer Zusatzinformation $k_2 \in \mathcal{K}$ eine einfach auszuwertende Funktion $d_{k_2} : \mathcal{C} \rightarrow \mathcal{P}$ angegeben werden kann mit $d_{k_2}(e_{k_1}(p)) = p$ für alle $p \in \mathcal{P}$ (Trapdoor-Eigenschaft). Ist nun für jedes $k \in \mathcal{K}$ die Funktion e_k eine Trapdoor-Einwegfunktion, so kann man $|\mathcal{K}|$ Teilnehmern jeweils einen Schlüssel k_i zuordnen und sowohl den Teilnehmer als auch den entsprechenden Schlüssel publizieren („Telefonbuch“).

Die Frage, ob es überhaupt Trapdoor-Einwegfunktionen gibt, ist bis heute unbeantwortet. Man kann allerdings Funktionen angeben, die nach dem jetzigen Stand der Technik Trapdoor-Einwegfunktionen sind. Dazu betrachten wir die Menge $(\mathbb{Z}_n, \cdot)$ mit der Multiplikation $x \cdot y := xy \bmod n$. Für jedes $k \in \mathbb{N}$ kann durch die Multiplikation auch das Potenzieren in $\mathbb{Z}_n$ definiert werden:

$$x^0 := 1, \quad x^k := x \cdot x^{k-1}$$

Sei nun $n = p \cdot q$ das Produkt zweier Primzahlen $p \neq q$, so betrachten wir die Funktionen

$$e_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n, \quad x \mapsto x^k, \quad k \in \mathbb{N}$$

für alle k , die teilerfremd zu $\varphi(n) = (p-1)(q-1)$ sind. Es läßt sich zeigen, daß

für jedes dieser k die jeweilige Funktion e_k bijektiv ist und daß es ein $\bar{k} \in \mathbb{N}$ gibt mit

$$d_{\bar{k}} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n : x \mapsto x^{\bar{k}} \text{ und } d_{\bar{k}}(e_k(x)) = e_k(d_{\bar{k}}(x)) = x \quad \forall x \in \mathbb{Z}_n$$

Die natürliche Zahl $\bar{k}$ ist charakterisiert durch

$$k \cdot \bar{k} = 1 \bmod \varphi(n)$$

Kennt man die Primfaktorzerlegung $n = p \cdot q$ von n , so läßt sich $\bar{k}$ aus p und q relativ einfach mit dem erweiterten euklidischen Algorithmus berechnen. Kennt man aber nur die Zahlen n und k , die die Funktion e_k vollständig charakterisieren, so ist zwar e_k leicht auszuwerten aber bis heute p und q (und damit $\bar{k}$) im allgemeinen nicht in adäquater Zeit zu berechnen.

3.2 Das RSA-Verfahren

Das von R. Rivest, A. Shamir und L. Adleman 1978 erfundene und nach ihnen benannte RSA-Verfahren verwendet die im letzten Abschnitt angegebenen Trapdoor-Einwegfunktionen

$$e_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n, x \mapsto x^k$$

mit öffentlichem Schlüssel (n, k) , der Primfaktorzerlegung $n = pq$ mit $p \neq q$ und dem geheimen Schlüssel $\bar{k}$ mit

$$k \cdot \bar{k} = 1 \bmod \varphi(n)$$

und $(x^k)^{\bar{k}} = (x^{\bar{k}})^k = x$ für alle $x \in \mathbb{Z}_n$. Entscheidend für die Sicherheit des RSA-Verfahrens ist die Größe der beiden Primzahlen p und q , die in Binärdarstellung durch die Anzahl der nötigen Bits charakterisiert werden. Heute werden für p und q 256 Bits (entspricht etwa 100 Dezimalstellen) verwendet. Somit entspricht n einer ganzen Zahl aus 512 Bits. Nehmen wir nun an, unser Klartext bestehe aus Buchstaben, Ziffern und Sonderzeichen, so wird zum Beispiel im ASCII-Code jedes der möglichen 256 Zeichen durch 8 Bits dargestellt (American Standard Code for Information Interchange)

ASCII-Zeichen	Binäre Form
Zwischenraum	00100001
0	00110000
1	00110001
⋮	
9	00111000
A	01000001
Z	01011010
⋮	

Somit entspricht einer Zahl $m \in \{0, 1, \dots, 2^{512} - 1\}$ (darstellbar durch 512 Bits) ein Text bestehend aus maximal 64 Zeichen ($64 \cdot 8 = 512$). Dem Klartext "ALLES KLAR!" entspricht eine natürliche Zahl $m \approx 1,57 \cdot 10^{26}$. Zwei entscheidende Nachteile des RSA-Verfahrens führten auf die Suche nach anderen Trapdoor-Einwegfunktionen und damit auch alternativer kryptographischer Verfahren.

1. Sobald es jemandem gelingt, die Primfaktorzerlegung natürlicher Zahlen effizient durchführen zu können, muß das RSA-Verfahren sofort ersetzt werden. Es ist dann zu spät, mit der Suche nach Alternativen zu beginnen.
2. Die bisherigen Algorithmen zur Primfaktorzerlegung zwingen den Kryptographen, Primzahlen mit mindestens 512 Bits zu verwenden. Diese Größen machen die Ver- und Entschlüsselung zu sehr komplexen Vorgängen. Gesucht sind Public-Key-Verfahren, die mit kleineren Zahlen auskommen.

3.3 Der diskrete Logarithmus

Für jede Primzahl p ist die Einheitengruppe von $(\mathbb{Z}_p, \cdot)$ die multiplikative Gruppe

$$\mathbb{Z}_p^* = \{a + p\mathbb{Z} \mid \gcd(a, p) = 1\} = \{1, 2, \dots, p-1\}.$$

Man kann zeigen, daß diese Gruppe zyklisch ist, d. h. es gibt in $\mathbb{Z}_p^*$ mindestens ein erzeugendes Element g mit $\mathbb{Z}_p^* = \langle g \rangle = \{g^k \mid k = 1, 2, \dots, p-1\}$. Nun betrachten wir die Abbildung

$$\exp_g : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^* : x \mapsto g^x$$

für jedes erzeugende Element g von $(\mathbb{Z}_p^*, \cdot)$. Die Abbildung $\exp_g$ ist bijektiv. Analog zum Vorgehen in der Analysis wird nun die Umkehrabbildung zu $\exp_g$ als diskreter Logarithmus bezeichnet:

$$\log_g : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*, \quad x \mapsto \log_g(x) \text{ mit } g^{\log_g(x)} = x.$$

Das Problem des diskreten Logarithmus in $(\mathbb{Z}_p^*, \cdot)$ lautet also folgendermaßen: Finde zur Basis g mit $\langle g \rangle = \mathbb{Z}_p^*$ und zu $b \in \mathbb{Z}_p^*$ ein $x \in \mathbb{Z}_p^*$ mit $g^x = b$. Man schreibt $\log_g b = x$. Da diese Funktion im allgemeinen nur mit größtem Aufwand auszuwerten ist (im Gegensatz zu $\exp_g$) ist die Exponentialfunktion zu speziellem erzeugendem Element g für spezielles p eine Einwegfunktion. Allerdings sind diese Funktionen zunächst für die Kryptographie nicht geeignet, da keine Trapdoor-Information in Sicht ist. Dennoch kann man die diskreten Exponentialfunktionen wie Trapdoor-Einwegfunktionen verwenden, wenn man dem zu verschlüsselnden Geheimtext noch gewisse Zusatzinformationen beifügt. Dies geschieht im Verschlüsselungsverfahren von El Gamal.

3.4 Das Verschlüsselungsverfahren von El Gamal

Ausgangspunkt ist die multiplikative Gruppe $\mathbb{Z}_p^*$ mit einem erzeugenden Element g . Ein Teilnehmer, der mit einem öffentlichen Schlüssel in ein Verzeichnis ein-

getragen werden will, wählt zufällig ein $t \in \mathbb{N}$ und berechnet seinen öffentlichen Schlüssel (τ, g) aus $\tau := g^t \bmod p$. Eine Quelle, die dem Teilnehmer mit öffentlichem Schlüssel τ eine Nachricht senden will, wählt sich zufällig eine Zahl $a \in \mathbb{N}$ und berechnet die Zahlen $\alpha := g^a \bmod p$ und $k := \tau^a \bmod p$. Dann verwendet er ein vorher festgelegtes, symmetrisches Kryptosystem mit Schlüsselmenge $\mathcal{K} = \mathbb{Z}_p^*$ und Verschlüsselungsfunktion e_k für $k \in \mathcal{K}$ und sendet seine geheime Nachricht $c = e_k(p)$ und die Information $\alpha = g^a \bmod p$ mit dem berechneten Schlüssel an den Empfänger. Da nun

$$k = \tau^a \bmod p = (g^t)^a \bmod p = (g^a)^t \bmod p = \alpha^t \bmod p$$

gilt, kann der Empfänger mit dem geheimen Schlüssel t den Schlüssel k unter Verwendung von α berechnen und somit dechiffrieren. Ein Angreifer, der nur τ , α und g kennt, hat somit $t = \log_g(\tau)$ zu berechnen, um k zu erhalten.

3.5 Elliptische Kurven

Bisher haben wir den diskreten Logarithmus für die multiplikativen Gruppen $(\mathbb{Z}_p^*, \cdot)$ betrachtet. Analog dazu kann man auch für andere zyklische Gruppen den diskreten Logarithmus definieren. In der additiven zyklischen Gruppe $(\mathbb{Z}_p, +)$ mit einer Primzahl p lautet die der Exponentialfunktion entsprechende Abbildung

$$e_g : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad x \mapsto \begin{cases} \underbrace{g + \dots + g}_{x\text{-mal}} =: x \cdot g, & x \neq 0 \\ 0 & x = 0. \end{cases}$$

für ein erzeugendes Element g , d. h. für ein Element mit $\langle g \rangle = \{k \cdot g \mid k \in \{0, \dots, p-1\}\} = \mathbb{Z}_p$. Es läßt sich zeigen, daß in $(\mathbb{Z}_p, +)$ alle von Null verschiedenen Elemente $g \in \mathbb{Z}_p \setminus \{0\}$ erzeugende Elemente sind. Die Abbildung e_g mit $g \in \mathbb{Z}_p \setminus \{0\}$ ist bijektiv. Daher existiert eine dem diskreten Logarithmus entsprechende Umkehrabbildung

$$d_g : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad x \mapsto d_g(x) \text{ mit } e_g(d_g(x)) = x.$$

Das Problem des diskreten Logarithmus in $(\mathbb{Z}_p, +)$ lautet also: Finde zur Basis $g \in \mathbb{Z}_p \setminus \{0\}$ und zu $b \in \mathbb{Z}_p$ ein x mit $x \cdot g = b$. Die Lösung ist $x = g^{-1}b$, wobei g^{-1} das multiplikative Inverse von g in $\mathbb{Z}_p^*$ bezeichnet. Da das inverse Element in $\mathbb{Z}_p^*$ mit dem erweiterten euklidischen Algorithmus effizient berechenbar ist, muß man nach anderen endlichen zyklischen oder allgemeiner abelschen (additiven) Gruppen suchen, in denen der diskrete Logarithmus praktisch nicht auszuwerten ist. Diese abelschen Gruppen erhält man unter anderem durch elliptische Kurven.

Seien $p > 3$ eine Primzahl und $a, b \in \mathbb{Z}_p$. Man betrachtet folgende Gleichungen in drei Unbekannten $x, y, z \in \mathbb{Z}_p$, wobei jetzt $\mathbb{Z}_p$ bezüglich $+$ und $\cdot$ (als endlicher Körper) gegeben ist:

$$y^2 \cdot z = x^3 + a \cdot x \cdot z^2 + b \cdot z^3.$$

Man interessiert sich nun für alle $(x', y', z') \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, die für feste $a, b \in \mathbb{Z}_p$ die obige Gleichung erfüllen. Dabei heißen zwei Lösungen (x', y', z') und (x'', y'', z'') äquivalent, falls es ein $c \in \mathbb{Z}_p$ mit $c \neq 0$ gibt, so daß

$$(x'', y'', z'') = (c \cdot x', c \cdot y', c \cdot z').$$

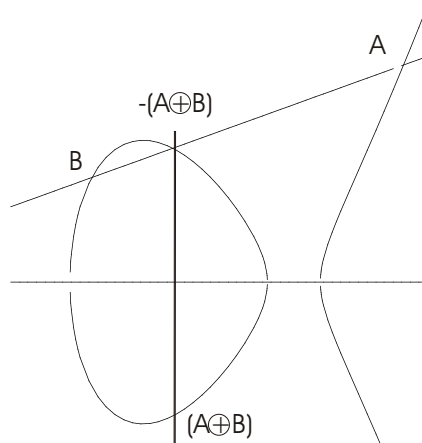
Interessant sind alle nichtäquivalenten Lösungen, von denen man sich immer genau eine in einer Menge $E(p, a, b)$ notiert. Es läßt sich zeigen, daß man alle nichtäquivalenten Lösungen der obigen Gleichung folgendermaßen darstellen kann (die Lösung $(0, 0, 0)$ wird nicht berücksichtigt):

$$E(p, a, b) = \{(x', y', 1) | y'^2 = x'^3 + a \cdot x' + b, x', y' \in \mathbb{Z}_p\} \cup \{0, 1, 0\}.$$

Nun soll eine Addition $\oplus$ auf $E(p, a, b)$ definiert werden. Dazu betrachten wir elliptische Kurven zunächst über den reellen Zahlen. Fordert man als Bedingung an die Parameter $a, b \in \mathbb{R}$, daß für die Diskriminante D der rechten Seite

$$D := \frac{a^3}{27} + \frac{b^2}{4} \neq 0$$

gilt, so kann man zeigen, daß für die zugehörige implizite Gleichung $F(x', y') = 0$ für y' als Funktion von x' , also für $F(x', y') = y'^2 - x'^3 - ax' - b$, in jedem Punkt (x', y') mindestens eine der partiellen Ableitungen $\frac{\partial F}{\partial x'}$, $\frac{\partial F}{\partial y'}$ ungleich Null ist. Insbesondere gibt es dann immer einen (falls $D > 0$) oder drei (falls $D < 0$) verschiedene Schnittpunkte mit der x -Achse. Es ergeben sich Lösungspunkte der folgenden Art:



Die Addition $\oplus$ wird nun folgendermaßen definiert: Sei $E(a, b)$ eine elliptische Kurve und seien $A = (x_1, y_1, 1) \in E(a, b)$.

$$A \oplus (0, 1, 0) := (0, 1, 0) \oplus A = A,$$

also ist $(0, 1, 0) =: 0$ das neutrale Element bezüglich $\oplus$. Das zu A inverse Element $-A$ wird definiert als

$$-A := (x_1, -y_1, 1).$$

Sei $B = (x_2, y_2, 1) \in E(a, b)$. Haben A und B verschiedene x' -Koordinaten, so schneidet die Gerade $\overline{AB}$ den (x', y') -Graphen der Menge $E(a, b)$ in einem weiteren Punkt $C = (\hat{x}, \hat{y}, 1)$. Es gilt dann

$$A \oplus B := -C \quad \text{und} \quad -C = (\hat{x}, -\hat{y}, 1).$$

Sind die x' -Koordinaten gleich, die y' -Koordinaten jedoch nicht, so setzt man $A \oplus B = 0$, da dann $B = -A$ gilt. Für $B = A$ verwendet man die Tangente an den (x', y') -Graphen, um C zu erhalten. Ist die Tangente parallel zur y' -Achse, so ist $A \oplus A = 0$. Ist A ein Wendepunkt, so ist $A \oplus A = -A$.

Analog dazu führt man nun $\oplus$ in $E(p, a, b)$ über $\mathbb{Z}_p$ ein. Man erhält eine additive abelsche Gruppe $(E(p, a, b), \oplus)$. Die Anzahl der Elemente N dieser Gruppe läßt sich abschätzen durch

$$p + 1 - 2\sqrt{p} \leq N \leq 2\sqrt{p} + p + 1$$

(Theorem von Hasse). Durch Variation von a, b lassen sich alle in diesem Intervall liegenden N erzeugen.

Man verwendet nun Gruppen $(E(p, a, b), \oplus)$, um durch die Funktionen e_g und ihre Umkehrfunktionen d_g zu einer ElGamal-Verschlüsselung zu kommen. In der additiven Schreibweise ist die Exponentialfunktion e_g dabei gegeben als Multiplikation mit einer ganzen Zahl. Diese Funktion ist genau dann bijektiv, wenn g ein erzeugendes Element ist. Da die hier betrachteten abelschen Gruppen jedoch nicht zyklisch sein müssen, sucht man nur einen Punkt $B \in E(p, a, b)$, der eine möglichst große Untergruppe erzeugt. In der von B erzeugten Untergruppe lautet das Problem des diskreten Logarithmus zur Basis B : Finde zu einem gegebenen Punkt $P \in E$ ein $x \in \mathbb{Z}$ mit $xB = P$. Die Multiplikation mit einer ganzen Zahl ist dabei wie in $(\mathbb{Z}_p, +)$ mit Hilfe der Addition definiert. Bei einer ElGamal-Verschlüsselung mit Elliptischen Kurven kommt man im Gegensatz zum RSA-Algorithmus mit etwa 163-Bit-Zahlen für p aus. Bereits dann ist der diskrete Logarithmus sehr komplex zu berechnen. Dies rechtfertigt den hohen Aufwand zur Berechnung von $E(p, a, b)$ für geeignet gewählte a, b und die etwas kompliziertere Arithmetik. Es ist wichtig festzuhalten, daß die Gruppe $E(p, a, b)$ a priori gewählt werden kann. Der Aufwand dafür ist zwar im allgemeinen sehr hoch, ist aber vor der Implementierung eines Kryptosystems zu leisten.

Kapitel 4

Zero-Knowledge-Verfahren

4.1 Authentifikationssysteme

In diesem Abschnitt betrachten wir spezielle Authentifikationssysteme, bei denen sich eine Person A gegenüber einer Person B durch den Nachweis eines bestimmten Geheimnisses identifizieren muß. Idealerweise sollte das so erfolgen, daß

- B das Geheimnis von A nicht vorher kennen muß,
- B während der Identifikation von A nichts über dieses Geheimnis erfährt.

Somit kann sich B Dritten gegenüber nicht als A ausgeben. Ziel ist es, daß sich B von A 's Identität mit beliebig großer Sicherheit überzeugt, ohne irgendwelche Informationen über das Geheimnis von A zu erhalten. Dies wird als Zero-Knowledge-Eigenschaft bezeichnet.

Wir wollen uns anhand eines Beispiels klarmachen, daß ein Authentifikationssystem mit den oben genannten Eigenschaften möglich ist. Eine Person A soll gegenüber einer Person B nachweisen, daß sie quadratische Gleichungen

$$ax^2 + bx + c = 0$$

für beliebige Koeffizienten $a, b, c \in \mathbb{R}$ lösen kann. Das Verfahren läuft folgendermaßen ab:

- B nennt drei reelle Zahlen a, b, c .
- A berechnet die beiden Lösungen der Gleichung $ax^2 + bx + c = 0$ und teilt diese B mit.
- B überprüft die Richtigkeit von A 's Lösung durch Einsetzen in die Gleichung.

Dieses Verfahren kann beliebig oft wiederholt werden und somit kann sich B beliebig sicher davon überzeugen, daß A das Geheimnis (die Lösung der quadratischen Gleichung) kennt, ohne daß B etwas von diesem Geheimnis erfährt.

In der Public-Key-Kryptographie werden Zero-Knowledge-Verfahren verwendet, für die sich beweisen läßt, daß B während der Authentifikation nichts über A 's Geheimnis erfährt.

4.2 Der Fiat-Shamir-Algorithmus

Das bekannteste und in der Praxis wichtigste Zero-Knowledge-Verfahren ist der Fiat-Shamir-Algorithmus. Die Idee dieses Algorithmus beruht darauf, daß es praktisch unmöglich ist, Quadratwurzeln in $(\mathbb{Z}_n^*, \cdot)$ zu berechnen. Es läßt sich zeigen, daß dieses Problem genauso schwer zu lösen ist wie das Problem, die Primfaktoren von n zu finden. Der Fiat-Shamir-Algorithmus besteht aus zwei Phasen, der Schlüsselerzeugungsphase und der Anwendungsphase. In der ersten Phase erzeugt A zunächst zwei große Primzahlen p und q und bildet ihr Produkt $n = pq$. Die Zahl n ist öffentlich, während p und q nur A bekannt sein dürfen. Dann wählt A eine Zahl s und berechnet $v := s^2 \bmod n$. Die Zahl s ist das individuelle Geheimnis des Teilnehmers A , während man mit Hilfe von v verifizieren kann, ob eine Person das Geheimnis kennt oder nicht. Das heißt, daß s geheim bleiben muß und v publiziert wird.

In der Anwendungsphase muß A eine Person B davon überzeugen, daß sie das Geheimnis s kennt, ohne daß B dieses Geheimnis mitgeteilt wird. Dazu führen A und B folgendes Protokoll durch:

- A wählt zufällig ein Element r aus $\mathbb{Z}_n^*$ und quadriert dieses: $x := r^2 \bmod n$. Danach sendet A den Wert x an B ;
- B wählt zufällig ein Bit b und sendet dieses an A ;
- ist $b = 0$, so sendet A den Wert $y := r$ an B ;
ist $b = 1$, so sendet A den Wert $y := r \cdot s \bmod n$ an B .
- B verifiziert diese Antworten: Im Falle $b = 0$ überprüft sie, ob $y^2 \bmod n = x$ ist; im Fall $b = 1$ testet sie die Richtigkeit der Gleichung $y^2 \bmod n = x \cdot v \bmod n$.

Durchführbarkeit: Wenn A das Geheimnis s kennt, so kann sich B davon überzeugen, denn es gilt

$$y^2 = (r \cdot s^b)^2 \bmod n = r^2 \cdot s^{2b} \bmod n = r^2 v^b \bmod n = x \cdot v^b \bmod n.$$

Korrektheit: Eine betrügerische Person $\tilde{A}$, die s nicht kennt, kann nicht beide Fragen $b = 0$ und $b = 1$ korrekt beantworten, denn sonst könnte sie aus der korrekten Antwort $y_0 = r$ und $y_1 = r \cdot s$ den Schlüssel $s = y_1 y_0^{-1} \bmod n$ berechnen. $\tilde{A}$ kann also höchstens mit der Wahrscheinlichkeit $\frac{1}{2}$ betrügen. Diese Wahrscheinlichkeit $\frac{1}{2}$ kann $\tilde{A}$ erzwingen: Wenn sie vermutet, daß B "0" sendet, so wählt sie $x := r^2 \bmod n, y = r$. Wenn sie vermutet, daß "1" von B gesendet wird, so wählt sie $x = r^2 \cdot v^{-1} \bmod n$ und $y = r$, denn dann ist $y^2 = xv \bmod n$.