Inhaltsverzeichnis

0 Einführung

Webseite der Vorlesung: http://www.matha.mathematik.uni-dortmund.de/~logik/crypto.html

Literatur (mehr auf der Webseite):

1. Neil Koblitz: A course in number theory and cryprography, Springer Verlag

0.1 Hauptaufgaben der Kryptografie

a) Geheimhaltung: Eine Nachricht soll übertragen werden, aber der Übertragungsweg ist unsicher. Unbefugte Empfänger sollen die Nachricht nicht lesen können.

b) Datenschutz: Texte oder Daten sollen vor Unbefugten geschützt werden. Der befugte Empfänger soll die Integrität der Daten verifizieren können.

c) Authentisierung: Der Urheber der Nachricht soll eindeutig identifizierbar sein.

0.2 Grundprinzip (Shannon, Kerckhoff)

Der Angreifer kennt das verwendete Kryptosystem. Die Sicherheit der Verfahrens beruht alleine darauf, dass der Angreifer den geheimen Schlüssel nicht kennt.

0.3 Definition (Kryptosysteme)

a) Die ursprüngliche Nachricht heißt Klartext ("plain text"). Sie besteht aus Klartexteinheiten (Buchstaben, bits, ...). Die Menge aller möglichen Klartexteinheiten wird mit $\mathcal{P}$ bezeichnet.

b) Die verschlüsselte Nachricht heißt Geheimtext ("cipher text"). Die Menge aller möglichen Geheimtexteinheiten wird mit $\mathcal{C}$ bezeichnet.

c) Eine Chiffrierung oder Verschlüsselung ist eine injektive Abbildung $f : \mathcal{P} \to \mathcal{C}$.

d) Eine Dechiffrierung oder Entschlüsselung ist eine Abbildung $g : Bild(f) \to \mathcal{P}$ bzw. $g : \mathcal{C} \to \mathcal{P}$ mit $g \circ f = id_{\mathcal{P}}$.

e) Ein Kryptosystem ist ein Tupel $\left(\mathcal{P}, \mathcal{C}, \{f_k\}_{k\in K}, \{g_k\}_{k\in K}\right)$ mit Chiffrier- f_k bzw. Dechiffrierabbildung g_k. Die Menge K heißt dabei die Menge der Schlüssel.

0.4 Methoden der Kryptoanalyse

Die Kryptoanalyse ("Knacken von Kryptosystemen") beschäftigt sich mit der Möglichkeit, Geheimtexte zu dechiffrieren, ohne dass man den geheimen Schlüssel kennt. Möglichkeiten:

1. "Mithören", "Nur Geheimtext-Attacke": Man kennt nur den Geheimtext und das verwendete Kryptosystem. Der Schlüssel bzw. die Nachricht sind zu finden.
2. "Nur-Klartextattacke": Der Angreifer kennt einige Klartexte mit den zugehörigen Geheimtexten. Er soll den Schlüssel finden.
3. "Wahl-Klartextattacke": Der Angreifer kann einen gewählten Klartext verschlüsseln. Man möchte den Schlüssel finden oder von jemand anders chiffrierte Nachrichten dechiffrieren.
4. "Wahl-Geheimtextattacke": Der Angreifer kann selbstgewählte Geheimtexte dechiffrieren.

0.5 Beispiel (Caesar-Chiffrierung)

$\mathcal{P}$=$\{A,B,C,D,E,F,G,H,I,L,M,N,O,P,Q,R,S,T,V,X\}$, $\mathcal{C} = \mathcal{P}$, $K = \{1\}$ wobei:

$$\begin{array}{rcl} f : \mathcal{P} & \to & \mathcal{C} \\ A & \mapsto & D \\ B & \mapsto & E \\ \vdots & & \vdots \end{array}$$

und

$$\begin{array}{rcl} g : \mathcal{C} & \to & \mathcal{P} \\ D & \mapsto & A \\ E & \mapsto & B \\ \vdots & & \vdots \end{array}$$

Beispiel:

TNQANON BDVH, OHLNRQHX VHGGH!

Dechiffriert bedeutet dies:

QINTILI VARE, LEGIONES REDDE!

0.6 Definition

a) Ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \{f_k\}_{k\in K}, \{g_k\}_{k\in K})$ heißt monoalphabetisch, wenn jede Klartexteinheit stets zu demselben Geheimtext chiffriert wird.

b) Ansonsten heißt das Kryptosystem polyalphabetisch.

0.7 Bemerkung (Kryptoanalyse des Caesarsystems)

Frequenzanalyse /Häufigkeitsanalyse: Jeder Buchstabe hat im Deutschen bzw. Englischen eine bestimmte Häufigkeit:

	A	*B*	*C*	*D*	*E*	*F*	*G*
Deutsch	6.51%	1.89%	3.06%	5.08%	17.4%	1.66%	3.01%
Englisch	7.23%	0.6%	2.82%	4.83%	15.66%	1.67%	2.16%

	H	*I*	*J*	*K*	*L*	*M*	*N*
Deutsch	4.76%	7.55%	0.27%	1.21%	3.44%	2.53%	9.87%
Englisch	4.02%	7.87%	0.06%	0.64%	3.96%	2.36%	8.14%

	O	*P*	*Q*	*R*	*S*	*T*	*U*
Deutsch	2.51%	0.79%	0.02%	7.0%	7.27%	6.15%	4.35%
Englisch	7.16%	1.61%	0.07%	7.51%	7.15%	7.73%	2.72%

	V	*W*	*X*	*Y*	*Z*
Deutsch	0.67%	1.89%	0.03%	0.04%	1.68%
Englisch	1.17%	0.78%	0.3%	1.13%	0.1%

Man stellt die Häufigkeitstabelle der Buchstaben im Geheimtext auf und vergleicht sie mit der Tabelle. Bei genügend langem Geheimtext findet man schnell die Permutation. Andernfalls ergeben sich mehrere Fälle, die durchprobiert werden können.

Exhaustation: Durchprobieren aller möglichen Schlüssel.

0.8 Beispiel (Die Vigenère-Verschlüsselung)

Dieses System war lange Zeit weit verbreitet und galt als sicher.

1) Es gibt ein “Schlüsselwort”

2) Der Buchstabe des Schlüsselworts, der gerade an der Reihe ist, gibt an, um wieviel man (gemäß Caesar) den Buchstaben des Klartextes verschieben muss.

3) Der nächste Buchstabe des Klartexts wird mit dem nächsten Buchstabens des Schlüsselwort chiffriert, ggf. wird das Schlüsselwort wiederholt.

Beispiel: Schlüsselwort “Katze”

Klartext: SENDEN BITTE HILFE

Schlüssel: KATZEKATZEKATZE $(11, 1, 20, 26, 5)$

Verschiebung: 11 1 20 26 511 1 20 26 511 1 20 26 5 11

Geheimtext: D F H D J E C C T Y P I C L K P

Modell: Das Schlüsselwort entspricht einem Tupel von Zahlen aus $\{1,2,3,\ldots,26\}$.

Es gilt: $\mathcal{P} = \mathcal{C}$=$\{A,B,C,\ldots,Z\}^N = \{(\alpha_1,\ldots,a_N) \mid \alpha_i \in \{A,\ldots,Z\}\}$ (α_i ist der i-te Buchstabe), $k = (k_1,\ldots,k_k) \in \{1,2,\ldots,26\}^l$

$$\alpha_i \quad \mapsto \quad f_j(\alpha_i)$$

mit $j = k_{r+1}$ mit $r = i \pmod l$, $g_k = f_k^{-1}$.

Kryptoanalyse: 2 Teilprobleme

1. Finde die Länge des Schlüsselwortes

2. Finde das Schlüsselwort

Zu 1: Exhaustation: Angenommen das Schlüsselwort hat 5 Buchstaben. Bestimme die Häufigkeitsverteilung für die Buchstaben 1, 6, 11, usw. des Geheimtexts und analog für 2, 7, 12 usw. und erhalten den 1. bzw. 2, usw. Buchstaben des Schlüsselwortes.

Kasiski-Test (1863): Wenn im Klartext zweimal dasselbe Wort auftritt wird der Anfangsbuchstabe i.A. verschieden chiffriert, außer wenn die Länge des Schlüsselwortes die Anzahl der dazwischen liegenden Buchstaben teilt. Suche im Geheimtext Folgen von 3 Buchstaben, die mehrfach auftreten. Die Abstände sind wahrscheinlich durch die Schlüsselwortlänge teilbar. Eventuell finde ggT möglichst vieler solcher Abstände.

Friedmann-Test (1920): “Mit welcher Wahrscheinlichkeit besteht ein aus einem Text willkürlich herausgegriffenes Buchstabenpaar aus gleichen Buchstaben?” Hieraus soll auf die Schlüsselwortlänge geschlossen werden.

0.8 Beispiel (Die Vigenère-Verschlüsselung) - Fortsetzung - MERGE

Das geheime Schlüsselwort (z.B. KATZE) entspricht einem Tupel von Zahlen $(n_1,\ldots,n_l)$ (hier z.B. $(11,1,20,26,5)$). Der i-te Buchstabe des Klartexts wird um n_j Positionen im Alphabet verschoben, wobei $j-1 = i \pmod l$.

Kryptoanalyse: “Friedmann-Test”

0.9 Bemerkung

Sei $(\alpha_1,\ldots,\alpha_n)$ eine Buchstabenfolge der Länge n. Sei n_1 die Anzahl der “A”, sei n_2 die Anzahl der “B”, … und sei n_{26} die Anzahl der “Z”.

1) Es gibt $\binom{n_1}{2} = \frac{n_1(n_1-1)}{2}$ Paare von “A” im Text, $\binom{n_2}{2} = \frac{n_2(n_2-1)}{2}$ Paare von “B” im Text, usw.

2) Insgesamt gibt es $\sum_{i=1}^{26} \binom{n_i}{2}$ Paare gleicher Buchstaben.

3) Die Wahrscheinlichkeit dafür, dass zwei zufällig ausgewählte Buchstaben gleich sind, ist

$$p_F = \frac{\sum_{i=1}^{26} \binom{n_i}{2}}{\binom{n}{2}}$$

Diese Zahl p_F heißt der Friedmannsche Koinzidenzindex des Texts.

4) Die Wahrscheinlichkeit dafür, dass ein zufällig ausgesuchter Buchstabe “A” ist, ist $p_1 = \frac{n_1}{n}$.

5) Die Wahrscheinlichkeit dafür, dass an der nächsten zufällig ausgewählten Stelle wieder “A” steht, ist

$$\frac{n_1-1}{n-1} \approx \frac{n_1}{n} = p_1$$

(für längere Texte).

6) Die Wahrscheinlichkeit dafür, dass man zweimal hintereinander ein “A” erwischt, ist also $\approx p_1^2$.

7) Insgesamt folgt:

$$p_F \approx p_1^2 + p_2^2 + \ldots + p_{26}^2$$

Für deutsche Texte gilt $p_F \approx 7.62\%$. Für zufällige Texte gilt $p_F \approx 3.85\%$.

8) Für monoalphabetische Verschlüsselungen bleibt p_F erhalten.

9) Für polyalphabetische Verschlüsselungen nimmt p_F ab, denn die Häufigkeiten der Buchstaben werden aneinander angeglichen.

0.10 Satz

Sei p_F der Friedmannsche Koinzidenzindex eines Vigenère-verschlüsselten Textes der Länge n. Sei d die Länge des Schlüsselwortes. Sei p_L der Koinzidenzindex der Sprache des Klartexts. Dann gilt:

$$d \approx \frac{\left(p_L - \frac{1}{26}\right) n}{(n-1)\, p_F - \frac{1}{26} n + p_L}$$

Beweis: Sei $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ der Geheimtext. Schreibe ihn in d Spalten:

S_1	S_2	$\ldots$	S_d
α_1	α_2	$\ldots$	α_d
α_{d+1}	α_{d+2}	$\ldots$	α_{2d}
$\vdots$	$\vdots$		$\vdots$

In jeder Spalte liegt eine monoalphabetische Verschlüsselung vor. Der Koinzidenzindex jeder Spalte ist also $\approx p_L$. Für Paare von Buchstaben aus verschiedenen Spalten ist die Wahrscheinlichkeit dafür, dass sie gleich sind etwa $\frac{1}{26}$. Jede Spalte hat etwa $\frac{n}{d}$ Buchstaben.

1) Die Anzahl der Paare von Buchstaben die in derselben Spalte stehen ist

$$d \binom{\frac{n}{d}}{2} = \frac{n(n-d)}{2d}$$

wobei d die Anzahl der Spalten und $\binom{\frac{n}{d}}{2}$ die Paare in einer Spalte ist.

2) Die Anzahl der Paare von Buchstaben, die in verschiedenen Spalten stehen ist

$$\binom{d}{2} \left(\frac{n}{d}\right)^2 = \frac{n^2 (d-1)}{2d}$$

$\binom{d}{2}$ ist die Zahl der Spaltenpaare.

3) Die Anzahl aller Paare gleicher Buchstaben ist also

$$A = \frac{n(n-d)}{2d} \cdot p_L + \frac{n^2 (d-1)}{2d} \cdot \frac{1}{26}$$

4) Damit folgt:

$$\begin{aligned} p_F &= \frac{A}{\binom{n}{2}} \\ &= \frac{n-d}{d(n-1)} \cdot p_L + \frac{n(d-1)}{d(n-1)} \cdot \frac{1}{26} \\ &= \frac{1}{d(n-1)} \left[\left(n p_L - \frac{n}{26} \right) + d \left(\frac{n}{26} - p_L \right) \right] \\ &= \frac{1}{d} \frac{n p_L - \frac{n}{26}}{n-1} - \frac{p_L - \frac{n}{26}}{n-1} \end{aligned}$$

Damit folgt:

$$\begin{aligned} p_F (n-1) + p_L - \frac{n}{26} &= \frac{1}{d} \left(n p_L - \frac{n}{26} \right) \\ \Leftrightarrow \qquad d &= \frac{\left(p_L - \frac{1}{26}\right) n}{(n-1)\, p_F - \frac{1}{26} n + p_L} \end{aligned}$$

□

1 Klassische Kryptosysteme

Referenz zur Geschichte der Kryptographie: David Kahn, The Codebreakers

1.1 Beispiel (Die Tafel des Polybius - 200BC-120BC)

1) Ordne die Buchstaben in einem 5x5 Schachbrett an:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Chiffriere “A” als $(1,1)$, “B” als $(1,2)$, usw.

Der Geheimtext zu TABAK ist $(4,4,1,1,1,2,1,1,2,5)$.

Verwendung bis ins 19. Jahrhundert, auch bekannt als nihilistische Verschlüsselung in russischen Gulags.

Kryptoanalyse:

1) Der Geheimtext besteht aus einer geraden Anzahl von Zeichen.

2) Es kommen nur die Ziffern $1,\ldots,5$ vor.

$\rightsquigarrow$ Jedem Buchstaben entsprechen wahrscheinlich zwei Ziffern.

3) Es liegt eine monoalphabetische Verschlüsselung vor. Frequenzanalyse der Ziffernpaare bricht das System.

Variante: Polybius mit Schlüsselwort.

Das Schlüsselwort sei “SEMMELKNOEDEL”.

	1	2	3	4	5
1	S	E	M	L	K
2	N	O	D	A	B
3	C	F	G	H	I/J
4	P	Q	R	T	U
5	V	W	X	Y	Z

Schreibe erst die verschiedenen Buchstaben des Schlüsselworts auf und dann die restlichen Buchstaben des Alphabets. Dieses Verfahren ist immer noch sehr unsicher (siehe weiter unten).

1.2 Beispiel (Vernam-Kryptosystem, 1920) (One Time Pad)

Verfahren:

1) Verwandle den Klartext mit Polybius in eine Ziffernfolge.

2) Man braucht einen Schlüssel aus n ($= 2\times$Länge des Klartextes) absolut zufällig gewählten Ziffern.

3) Addiere die Polybius-Ziffernfolge auf den Schlüssel und reduziere jeden Eintrag modulo 10.

Beispiel: Klartext HELLOWORLD

Polybius:	2	3	1	5	3	1	3	1	3	4	5	2	3	4	4	2	3	1	1	4
Schlüssel:	3	7	8	3	5	9	2	1	9	9	0	4	4	3	2	1	6	7	6	7
Geheimtext:	5	0	9	8	8	0	5	2	2	3	5	6	7	7	6	3	9	8	7	1

Dies ist das einzige klassische Verfahren, von dem man beweisen kann, dass es absolut sicher ist.

Kryptoanalyse:

1) Das Pad darf wirklich nur ein einziges Mal verwendet werden.

2) Die Ziffern müssen wirklich zufällig sein.

3) Der Schlüsselaustausch ist eventuell unsicher.

1.3 Beispiel (Anagramme)

Galileo Galilei veröffentlichte 1610 folgende Zeichenkette:

SMAISMRMILMEPOETALEUMIBUNENUGTTAUIRAS

Die ist ein Anagramm, also eine Permutation einer anderen Zeichenkette. Dies war die Permutation von

ALTISSIMUM PLANETAM TERGEMINUM OBSERVI

(“Ich beobachte den äußersten Planten (Saturn) in drei Gestalten”). Niemand konnte den Satz entschlüsseln, aber Galilei war stets in der Lage zu beweisen, daß er die Ringe des Saturn entdeckt hatte.

Permutationen des Klartexts heißen auch Transpositionen.

1.4 Beispiel (Die Spalten-Transposition)

a) ohne Schlüsselwort: Schreibe den Klartext zeilenweise in ein oder mehrere Rechtecke:

E	*S*	*W*	*A*
R	*S*	*C*	*H*
O	*N*	*D*	*U*
N	*K*	*E*	*L*

Der Geheimtext entsteht durch spaltenweises auslesen:

ERONSSNKWCDEAHUL

b) mit Schlüsselwort: Das Kennwort übermittelt eine Permutation der Spalten, z.B.

D	*A*	*M*	*E*
2	1	4	3

(Position im Alphabet).

2	1	4	3
E	*S*	*W*	*A*
R	*S*	*C*	*H*
O	*N*	*D*	*U*
N	*K*	*E*	*L*

Der Geheimtext wird spaltenweise in der neuen Spaltenreihenfolge ausgelesen:

SSNKERONAHULWCDE

1.4 Beispiel (Die Spalten-Transposition) - Fortsetzung - MERGE

Kryptoanalyse: Der Geheimtext hat 16 Buchstaben und die Häufigkeitsverteilung entspricht der der deutschen Sprache. Die vermutete Blockgröße ist 4x4. Spaltenweises Aufschreiben des Geheimtexts liefert

S	*E*	*A*	*W*
S	*R*	*H*	*C*
N	*O*	*U*	*D*
K	*N*	*L*	*E*

Analyse der Spaltenpermutationen: Wähle eine Spalte mit vielen häufigen Buchstaben und stellen sie anderen Spalten gegenüber.

		%			%			%
E	*S*	1.4	*E*	*A*	0.26	*E*	*W*	0.23
R	*S*	0.54	*R*	*H*	0.19	*R*	*C*	0.09
O	*N*	0.64	*O*	*U*	0.1	*O*	*D*	0.07
N	*K*	0.25	*N*	*L*	0.05	*N*	*E*	1.22

Es ergeben sich “Bigramme” (Kombinationen von zwei Buchstaben), die ebenfalls eine gewisse Häufigkeitsverteilung haben (aufgeführt jeweils in der dritten Spalte). Die erste Gegenüberstellung hat wesentlich höhere Wahrscheinlichkeiten als die anderen.

		%			%
S	*W*	0.10	*S*	*Q*	0.36
S	*C*	0.89	*S*	*H*	0.09
N	*D*	1.87	*N*	*U*	0.33
K	*E*	0.26	*K*	*L*	0.10

Auch hier hat die erste Gegenüberstellung die größte Wahrscheinlichkeit. Nun kombiniere die Spalten in der so gefundenen Reihenfolge:

E	*S*	*W*	*A*
R	*S*	*C*	*H*
O	*N*	*D*	*U*
N	*K*	*E*	*L*

Hat man noch nicht die richtige Startspalte, so füge die passende zyklische Vertauschung an.

1.5 Beispiel (Enigma: rotierende Alphabete)

1927-1945 in Deutschland verwendet.

Schemata:

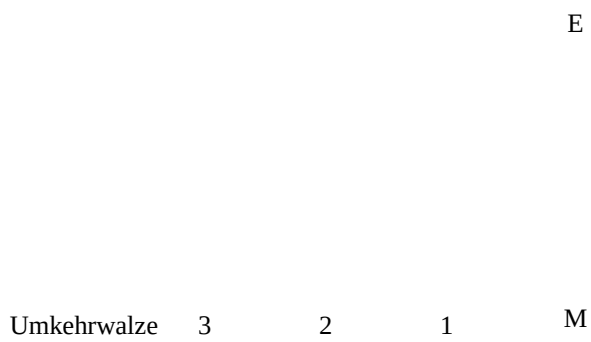

Abbildung 1: Bildchen

Wenn Stromkontakt besteht, dann wird *E* zu *M* verschlüsselt. Nach jedem Chiffrierschritt wird der Rotor 1 um $\frac{360^\circ}{26}$ weiterbewegt. Nach 26 Schritten bewegt er der Rotor 2 um $\frac{360^\circ}{26}$ weiter, etc.

Schlüssel:

a) Wahl der Rotoren (jedes Exemplar hat eine andere Verdrahtung)

b) Anfangsstellung der Rotoren

Kryptographisches Modell: Ein Rotor erzeugt ein “rotierendes Alphabet”:

0	*E*	*N*	*I*	*G*	*M*	*A*	*B*	*X*	*C*	…	…	…	…	…
1	∗	*F*	*O*	*J*	*H*	*N*	*B*	*C*	*Y*	*D*	…	…	…	…
2	∗	∗	*G*	*P*	*K*	*I*	*O*	*C*	*D*	*Z*	*E*	…	…	…
3	∗	∗	∗	*H*	*Q*	*L*	*J*	*P*	*D*	*E*	*A*	*F*	…	…
4	∗	∗	∗	∗	*I*	*R*	*M*	*K*	*Q*	*E*	*F*	*B*	*G*	…

Permutiertes Alphabet entsprechend der Verdrahtung. Das Alphabet steht immer in der Diagonalen.

Es liegt ein mechanisches Vigenère-Kryptosystem (mit Permutation) vor. Schlüsselanzahl:

(# Rot 1)·(# Rot 2)·(# Rot 3)·(26 Pos. an 1)·(26 Pos. an 2)·(26 Pos. an 3)·(26 Pos. an 4)

Also $\approx 125 \cdot 26^4 = 57122000$ verschiedene Permutationen.

Kryptoanalyse:

a) Täglich wechselnde Schlüssel, immer von der Form XYZXYZ (zwei gleiche Dreiergruppen). Ein ganzen Tag verwendete man also dieselbe Ausgangsstellung.

b) Die Umkehrwalze schränkt die möglichen Permutationen stark ein. Vorteil: Man kann mit derselben Einstellung ver- und entschlüsseln, d.h. die Permutation ist involutorisch, $\sigma^2 = id$ mit $\mathcal{P} = \mathcal{C}$.

c) Ein Buchstabe kann nicht zu sich selbst verschlüsselt werden.

d) Innerhalb eines Monats durfte aus Sicherheitsgründen dieselbe Rotorenlage nicht zweimal verwendet werden.

1.6 Beispiel (Pseudozufallsgeneratoren und Vigenère-Verschlüsselung)

Das Problem beim One-Time-Pad war der extreme lange Schlüssel.

Idee: Erzeuge eine lange Liste von "zufällig aussehenden" Zahlen (eine sogenannte "pseudozufällige Folge) aus wenigen Daten. Eine solches Verfahren heißt Pseudozufallsgenerator.

Sei $\mathbb{Z}/_{m\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}$ mit Multiplikation und Addition modulo m (meistens ist $m = 2^n$ mit $n \geq 1$). Eine bijektive Abbildung $f : \begin{array}{ccc} \mathbb{Z}/_{m\mathbb{Z}} & \to & \mathbb{Z}/_{m\mathbb{Z}} \\ \overline{x} & \mapsto & \overline{a}\overline{x}+\overline{b} \end{array}$ mit $a, b \in \mathbb{Z}$ heißt linearer Kongruenzgenerator. Wähle einen Samen (englisch "seed") $s \in \mathbb{Z}$ und erzeuge die Folge $\overline{s}, f(\overline{s}), f(f(\overline{s})), \ldots, f^i(\overline{s})$. Die Folge $x_0 = \overline{s}$, $x_i = f(x_{i-1})$ für $i \geq 1$ wird irgendwann periodisch. Wir möchten gerne die Periodenlänge m haben. Dann werden bei sehr langen Folgen alle Restklassen gleichhäufig erzeugt.

Kryptosystem:

1) Man verständigt sich auf einen "guten" Pseudozufallsgenerator f. Man übermittelt den Samen s als geheimen Schlüssel.

2) Jetzt wird die Nachricht mit dem Vigenère-Kryptosystem verschlüsselt mit Schlüsselwort $(s, f(s), f(f(s)), \ldots)$.

Probleme:

I) Wie muss man a, b, m wählen, so dass f bijektiv ist und $\overline{s}$ maximale Periodenlänge hat?

II) Wie kann man f im Fall $m = 2^n$ technisch realisieren?

III) Wie sicher ist das entstehende Kryptosystem?

1.7 Lemma

Die Abbildung $f : \begin{array}{ccc} \mathbb{Z}/_{m\mathbb{Z}} & \to & \mathbb{Z}/_{m\mathbb{Z}} \\ \overline{x} & \mapsto & \overline{a}\overline{x}+\overline{b} \end{array}$ ist bijektiv $\Leftrightarrow \mathrm{ggT}(a, m) = 1$.

Beweis: Aufgabe auf Übungszettel 2.

1.8 Satz

Seien $a, b \in \mathbb{Z}$ und $m = 2^n$ mit $n \geq 1$. Ferner sei $f : \begin{array}{ccc} \mathbb{Z}/_{m\mathbb{Z}} & \to & \mathbb{Z}/_{m\mathbb{Z}} \\ \overline{x} & \mapsto & \overline{a}\overline{x}+\overline{b} \end{array}$. Für $s \in \mathbb{Z}$ sei $(x_i)_{i\geq 0}$ definiert durch $x_0 = \overline{s}$, $x_i = f(x_{i-1})$ für $i \geq 1$. Genau dann ist $(x_i)_{i\geq 0}$ periodisch mit Periodenlänge m, wenn gilt:

a) a ist ungerade.

b) $4 \mid a-1$, falls $n \geq 2$.

c) b ist ungerade.

Beweis:

Zu "⇒":

Zu Bedingung "a)": Die Gleichung $f(x) = x$ ist äquivalent zu $(\overline{a}-1)x = -\overline{b}$. Ist a gerade, so ist $\overline{a}-1 \in \mathbb{Z}/_{m\mathbb{Z}}$ nach 1.7 invertierbar, also

$$x = -\frac{\overline{b}}{\overline{a}-1}$$

ein Fixpunkt von f, also hat f nicht maximale Periodenlänge.

Zu Bedingung "b)": Sei $n \geq 2$, also $4 \mid m$. Wir wissen schon, dass a ungerade ist. Wir müssen zeigen, daß $a \equiv 3 \pmod 4$ nicht möglich ist. In diesem Fall wäre $a+1 \equiv 0 \pmod 4$. Dann folgt:

$$1 + a + a^2 + \ldots + a^{2i-1} = (1-a)\left(1 + a^2 + a^4 + \ldots + a^{2i-2}\right) \equiv 0 \pmod 4$$

Es gilt:

$$\begin{aligned} x_{i+1} - x_i &= f(x_i) - f(x_{i-1}) \\ &= \overline{a}x_i - \overline{a}x_{i-1} \\ &= \overline{a}(x_i - x_{i-1}) \end{aligned}$$

Damit folgt:

$$\begin{aligned} x_k - x_0 &= (x_k - x_{k-1}) + (x_{k-1} - x_{k-2}) + \ldots + (x_1 - x_0) \\ &= \left(\sum_{i=0}^{k} \overline{a}^i \right) (x_1 - x_0) \qquad (*) \end{aligned}$$

Für $k = 2j-1$ folgt:

$$\begin{aligned} x_k - x_0 &\equiv 0 \,(\mathrm{mod}\, 4) \\ x_{2j+1} &\equiv x_1 \,(\mathrm{mod}\, 4) \end{aligned}$$

Daher kann es keinen Zyklus $(x_0, x_1, \ldots)$ maximaler Länge geben, da die Hälfte der Elemente die gleiche Restklasse mod 4 hat.

Zu Bedingung "c)": In einer Folge mit maximaler Periodenlänge muss Null vorkommen. OE sei $x_0 = \overline{s} = 0 \Rightarrow x_1 = f(x_0) = \overline{b}$. Wegen $(*)$ gilt

$$x_k = \left(\sum_{i=0}^{k-1} \overline{a}^i \right) \overline{b}$$

Es gibt ein $k \geq 1$ mit $x_k = \overline{1}$. Also ist $\overline{b} \in \mathbb{Z}/_{m\mathbb{Z}}$ invertierbar, d.h. b ist ungerade.

Zu "$\Leftarrow$": $m = 2$ ist trivial.

Sei $m \geq 4$: Wir zeigen, dass für $x_0 = 0$ ein Zyklus maximaler Länge m erzeugt wird. Wir hatten bereits gezeigt:

$$x_k = \left(\sum_{i=0}^{k-1} \overline{a}^i \right) \overline{b}$$

Da b ungerade ist, ist $\overline{b} \in \mathbb{Z}/_{m\mathbb{Z}}$ eine Einheit. Also ist $x_k = 0$ genau dann, wenn

$$1 + a + \ldots + a^{k-1} \in m\mathbb{Z} = 2^n\mathbb{Z}$$

Schreibe $k = 2^\kappa l$ mit l ungerade, $\kappa \geq 0$. Dann:

$$1 + a + \ldots + a^{k-1} = \left[1 + a^{2^\kappa} + \left(a^{2^\kappa}\right)^2 + \ldots + \left(a^{2^\kappa}\right)^{l-1} \right] \left[1 + a + \ldots + a^{2^\kappa - 1} \right]$$

Da a ungerade ist, gilt

$$1 + a^{2^\kappa} + \ldots + \left(a^{2^\kappa}\right)^{l-1} \geq l \equiv 1 \,(\mathrm{mod}\, 2)$$

und es folgt

$$\begin{aligned} 1 + a + \ldots + a^{k-1} \in m\mathbb{Z} \qquad &\Leftrightarrow \qquad \underbrace{1 + a + \ldots + a^{2^\kappa - 1}}_{(\#)} \in 2^n\mathbb{Z} \\ &\Leftrightarrow \qquad \kappa \geq n \\ &\Leftrightarrow \qquad 2^n \mid k \end{aligned}$$

$(\#)$ ist eine Summe von 2^κ ungeraden Zahlen, die durch 2^κ teilbar ist, aber nicht durch $2^{\kappa+1}$. □

Zu Problem II): Wie kann man einen Pseudozufallsgenerator $f : \mathbb{Z}/_{m\mathbb{Z}} \to \mathbb{Z}/_{m\mathbb{Z}}$ technisch realisieren?

1.9 Bemerkung (Schieberegister)

Ein Schieberegister besteht aus einer endlichen Folge von Bit-Speicherplätzen, die in einem gewissen Takt jeweils ihren Inhalt an die nächste Zelle weitergeben.

Abbildung 2: Bildchen

Man kann eine lineare Rückkopplung einbauen.

Abbildung 3: Bildchen

Die Zelle $\oplus$ enthält bei jedem Takt die Summe (in $\mathbb{Z}/_{2\mathbb{Z}}$) der letzten und drittletzten Zellen.
Beispiel: Initialisierung:

a_0	a_1	a_2	a_3		OUT
1	0	0	0	$\rightarrow$	0
0	1	0	0	$\rightarrow$	0
1	0	1	0	$\rightarrow$	0
0	1	0	1	$\rightarrow$	1
0	0	1	0	$\rightarrow$	0
0	0	0	1	$\rightarrow$	1
1	0	0	0		

Der Output (auf der rechten Seite) hat die Periodenlänge sechs.
Interpretation: Zustand a_0, a_1, a_2, a_3 entspricht der Restklasse

$$x = a_0 + 2a_1 + 4a_2 + 8a_3 \in \mathbb{Z}/_{16\mathbb{Z}}$$

Der nächste Zustand ist

$$f(x) \quad = \quad (a_1 + a_3) \bmod 2 + 2a_0 + 4a_1 + 8a_2$$

FIXME: Überprüfen, hier stimmt wohl was nicht!!

1.10 Bemerkung (Sicherheit von linearen Kongruenzgeneratoren)

a) $f: \begin{array}{ccc} \mathbb{Z}/_{2^n\mathbb{Z}} & \rightarrow & \mathbb{Z}/_{2^n\mathbb{Z}} \\ \bar{x} & \mapsto & \overline{ax}+\overline{b} \end{array}$ liefert abwechselnd gerade und ungerade Zahlen.

b) Die letzten beiden Ziffern (Bits) in der 2^n-adischen Darstellung sind ebenfalls periodisch, ebenso die Folgen der letzten drei Ziffern, etc. $\Rightarrow$ man darf nur die ersten Ziffern verwenden. Beim Schieberegister verwendet man nur die erste Stelle.

1.11 Beispiele (DES=Data Encryption Standard)

Etwa von 1975-2000 offizieller Standard, von IBM und NSA entwickelt. Mathematische Arbeiten über Kryptographie waren zeitweise "classified material"

I) DES ist ein Blockverschlüsselungsverfahren, d.h. der Quelltext wird in Blöcke von 8 Byte zerlegt, evtl. mit Zufallsbits aufgefüllt.

II) geheimer Schlüssel hat 56 Bits (plus 8 "Party Bits")

III) Verschlüsselung in mehreren "Runden":

1. Komposition von Addition, Multiplikation, XOR-Verknüpfungen und Permutationen.
2. Bei jeder Runde wird der 8 Byte Block in ein linke Hälfte L_i und eine rechte Hälfte R_i zerlegt.
3. Man macht 16 Runden mit $L_i = R_{i-1}$ und $R_i = L_i \oplus f(R_{i-1}, K_1)$, wobei $\oplus$ die bitweise Addition symbolisiert. K_i ist ein 48 Bit Schlüssel, dieser wird aus dem ursprünglichen Schlüssel berechnet. f ist eine "komplizierte" Funktion. Schema:

Dieses Verfahren ist effizient durchführbar (Kryptochip), zudem ist eine effiziente Entschlüsselung möglich: Verwende die Schlüssel K_i in umgekehrter Reihenfolge. Datenrate (1980) bis zu 200 MB/s.

Kryptoanalyse:

R_{i-1}

Expansion

$E(R_{i-1})$ K_i

$\oplus$

S-Boxen

P-Box

L_i

Abbildung 4: Bildchen

1) Die schnelle Verschlüsselung ermöglicht die Attacke durch Exhaustion.

2) Nur-Klartextattacke: Serienbriefe, Standardfloskeln and leicht zu erratender Stelle $\Rightarrow$ Man braucht nicht alle 2^{56} Schlüssel auszuprobieren.

3) Der geheime Schlüssel wurde oft zu lange verwendet.

4) Differenzielle Kryptoanalyse/lineare Kryptoanalyse $\rightsquigarrow$ 2^{43}Schlüssel sind durchzuprobieren

1.12 Beispiel (AES - Advanced Encryption Standard)

- 1997 Wettbewerb um DES zu ersetzen. Sieger im Jahr 2000: Rijndael
- Blocklängen: 128 Bit, 192 Bit oder 256 Bit.
- Schlüssellängen bis 256 Bit.
- Blockchiffre: 4 Zeilen, 4 oder 8 Spalten
- Zellen: 1 Byte
- Es werden eine gewisse Anzahl von Runden durchgeführt ($10 \leq r \leq 14$ je nach Blockgröße)
- Ablauf:
  1. Schlüsselexpansion, Rundenschlüssel K_i werden aus dem geheimen Schlüssel erzeugt
  2. Vorrunde: “Key Addition” (XOR-Verknüpfung)
  3. Verschlüsselungsrunden:
     (a) Substitution $\rightarrow$ S-Box
     (b) Verschiebung der Zeilen$\rightarrow$ Teil der P-Box
     (c) Permutation der Zeilen$\rightarrow$ Teil der P-Box
  4. Schlussrunden:
     (a) Substitution $\rightarrow$ S-Box
     (b) Zeilenverschiebung
- Entschlüsselung: Alles genau rückwärts durchführen. XOR ist selbstinvers, also wie Verschlüsselung.
- Performance: FIXME

Korrektur zur letzten Vorlesung vom 21.4.2005 - 1/2

Sei $a \in \mathbb{Z}$ mit $a \equiv 1 \pmod 4$. Dann gilt für alle $k \geq 1$:

a) 2^k teilt $1 + a + a^2 + \ldots + a^{2^k-1}$

b) 2^{k+1} teilt nicht $1 + a + a^2 + \ldots + a^{2^k-1}$

Beweis: Mit vollständiger Induktion nach k:

$k = 1$: Klar.

$k > 1$:

$$1 + a + a^2 + \ldots + a^{2^k-1} \quad = \quad \left(1 + a^{2^{k-1}}\right)\left(1 + a + a^2 + \ldots + a^{2^{k-1}-1}\right)$$

$1 + a^{2^{k-1}}$ ist durch 2, aber nicht durch 4 teilbar, da $a \equiv 1 \bmod 4$ und damit auch $a^i \equiv 1 \bmod 4$. $1 + a + a^2 + \ldots + a^{2^{k-1}-1}$ ist nach Induktionsvoraussetzung durch 2^{k-1}, aber nicht durch 2^k teilbar. □

Korrektur zur letzten Vorlesung vom 21.4.2005 - 2/2

Zu Bemerkung 1.9 (Schieberegister)

Diese Schieberegister werden als LFSR = “linear feedback shift register” bezeichnet.

1) Besser ist es

Abbildung 5: Bildchen

zu verwenden $\rightsquigarrow$ Periodenlänge 15 (Jeder Zustand außer “0 0 0 0” kommt vor).

Berechnung der Periodenlänge über charakteristisches Polynom $1 + x + x^4$ (primitiv). Das andere Beispiel hatte das charakteristische Polynom $1 + x^2 + x^4$ (nicht primitiv).

2) Zu jeder periodischen Folge “0 1 0 0 1”, “0 1 0 0 1”, … kann man ein Schieberegister mit diesem Output konstruieren (“Berlekamp-Massy Algorithmus”).

2 Public-Key Kryptosysteme

A Grundlagen

Idee: Finde ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \{f_k\}_{k\in K}, \{g_k\}_{k\in K})$ mit $f = f_k$ unabhängig von k.

2.1 Definition (Einweg-Funktion)

a) Eine injektive Abbildung $f : \mathcal{P} \to \mathcal{C}$ heißt Einweg-Funktion ("one way function"), wenn gilt:

1. Für jedes $x \in \mathcal{P}$ gibt es ein effizientes Verfahren zur Berechnung von $f(x)$.
2. Es gibt kein effizientes Verfahren zur Berechnung von x, wenn $f(x) \in \text{Bild}(f)$ gegeben ist.

b) Eine injektive Abbildung $f : \mathcal{P} \to \mathcal{C}$ heißt Einweg-Funktion mit Falltür ("trap-door one-way function"), wenn gilt:

1. Für jedes $x \in \mathcal{P}$ gibt es ein effizientes Verfahren zur Berechnung von $f(x)$.
2. Besitzt man eine Zusatzinformation, so ist x aus $y = f(x)$ effizient berechnen.
3. Besitzt man diese Zusatzinformation nicht, so kann man x nicht effizient aus $y = f(x)$ berechnen.
4. Man kann die Zusatzinformation nicht aus der Kenntnis von f ableiten.

2.2 Beispiel

a) Sei p Primzahl und $n \geq 0$ und $\text{ggT}(n, p-1) = 1$.

1) $f : \begin{array}{ccc} \mathbb{Z}/_{p\mathbb{Z}} & \to & \mathbb{Z}/_{p\mathbb{Z}} \\ x & \mapsto & x^n \end{array}$ effizient berechenbar.

2) Kennt man ein $n \in \mathbb{N}$ mit $m \cdot n \equiv 1 \pmod{(p-1)}$, so ist die Abbildung $g : \begin{array}{ccc} \mathbb{Z}/_{p\mathbb{Z}} & \to & \mathbb{Z}/_{p\mathbb{Z}} \\ x & \mapsto & x^m \end{array}$ invers zu f und damit effizient berechenbar.

3) Kennt man kein solches m, so ist die Abbildung f auf $\text{Bild}(f)$ nicht effizient umkehrbar: Zu $y = x^n$ ist x gesucht.

b) Seien $p, q \geq 3$ verschiedene Primzahlen und $n = pq$. Betrachte die Abbildung $\varphi : \begin{array}{ccc} (\mathbb{Z}/_{n\mathbb{Z}})^x & \to & (\mathbb{Z}/_{n\mathbb{Z}})^x \\ x & \mapsto & x^2 \end{array}$, wobei $(\mathbb{Z}/_{n\mathbb{Z}})^x$ die multiplikative Gruppe der zu n teilerfremden Zahlen ist.

1) Zu $y \in \text{Bild}(\varphi)$ gibt es vier $x \in (\mathbb{Z}/_{n\mathbb{Z}})^x$ mit $\varphi(x) = y$. Dies folgt aus dem Chinesischen Restsatz:

$$\begin{array}{rcl} \mathbb{Z}/_{n\mathbb{Z}} & \cong & \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{q\mathbb{Z}} \\ x & \mapsto & (x + p\mathbb{Z}, x + q\mathbb{Z}) = (\bar{x}_1, \bar{x}_2) \end{array}$$

denn für $y = x^2$ gilt $(\bar{y}_1, \bar{y}_2) = (\pm\bar{x}_1, \pm\bar{x}_2)^2$.

2) Kennt man p, q, so kann man aus $y = x^2$ das Urbild x effizient berechnen.

3) Kennt man nur n, aber nicht p, q, so ist kein effizienter Weg zur Berechnung von x bekannt.

4) Alle bekannten Algorithmen zur Faktorisierung von n haben exponentielle Laufzeit.

2.3 Definition

Ein Public-Key-Kryptosystem besteht aus den folgenden Daten:

1. Einer Menge $\mathcal{P}$ von Klartexteinheiten
2. Einer Menge $\mathcal{C}$ von Geheimtexteinheiten
3. Einer Menge $\{f_k\}_{k\in K}$ von Einwegfunktionen $f_k : \mathcal{P} \to \mathcal{C}$ mit Falltür, wobei $k \in K$ ein "öffentlicher Schlüssel" ist.
4. Für jedes $k \in K$ einer effizient berechenbaren Funktion existiert $g_k : \text{Bild}(f_k) \to \mathcal{P}$ mit $g_k \circ f_k = id_{\mathcal{P}}$. Die Abbildungsfunktion von g_k bzw. eine Information mit der wir die Abbildung g_k beschreiben können, heißt der Geheimschlüssel zu k.

2.4 Satz (Erweiterter Euklidischer Algorithmus)

Seien $a,b \in \mathbb{Z}$. Betrachte folgende Instruktionen:
1) Ist $a = b = 0$, so gibt $(0,0,0)$ aus und stoppe.
2) Ist $a = 0$ und $b \neq 0$, so gib $\left(0, \frac{|b|}{b}, |b|\right)$ aus und stoppe.
3) Ist $a \neq 0$ und $b = 0$, so gib $\left(0, \frac{|a|}{a}, |a|\right)$ aus und stoppe.
4) Bilde die Tripel $(c_0,d_0,e_0) = \left(\frac{|a|}{a}, 0, |a|\right)$ und $(c_1,d_1,e_1) = \left(0, \frac{|b|}{b}, |b|\right)$.
5) Prüfe, ob $e_1 \leq e_0$ gilt. Ist dies nicht der Fall, so vertausche die Tupel (c_0,d_0,e_0) und (c_1,d_1,e_1).
6) Schreibe $e_0 = qe_1 + r$ mit $q \geq 0$ und $0 \leq r < e_1$. Bilde das neue Tupel $(c_2,d_2,e_2) = (c_0 - qc_1, d_0 - qd_1, r)$.
7) Ersetze (c_0,d_0,e_0) durch (c_1,d_1,e_1) und (c_1,d_1,e_1) durch (c_2,d_2,e_2).
8) Prüfe ob $e_1 = 0$ gilt. In diesem Fall gib (c_0,d_0,e_0) aus und stoppe. Andernfalls fahre mit Schritt 6 fort.
Dies ist ein Algorithmus, der ein Tripel (c_0,d_0,e_0) berechnet mit $e_0 = \mathrm{ggT}(a,b)$ und $e_0 = c_0 a + d_0 b$.
Beweis: Knuth, The art of computer programming, Band 1. □

2.5 Satz (Der kleine Fermatsche Satz)

Sei p eine Primzahl. Für alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \pmod{p}$. Falls a nicht durch p teilbar ist gilt: $a^{p-1} \equiv 1 \pmod{p}$.
Beweis: Sei $a \in \mathbb{Z}$ mit $p \nmid a$. Die Menge $\{0a, 1a, \ldots, (p-1)a\}$ ist ein Repräsentantensystem für $\mathbb{Z}/_{p\mathbb{Z}}$, denn wären $0 \leq 1 < j \leq p-1$ mit $ia \equiv ja \pmod{p}$, so folgt aus $p \mid (j-i)a$, dass $p \mid j-i$ oder $p \mid a$ gilt. (Widerspruch)
Damit folgt

$$(1a)(2a)\ldots((p-1)a) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

und daher

$$p \mid (p-1)!\left(a^{p-1} - 1\right)$$

Damit folgt unmittelbar, das $p \mid a^{p-1} - 1$. □

2.6 Korollar

Sei p Primzahl und seien $n,m \in \mathbb{Z}$ mit $mn \equiv 1 \pmod{(p-1)}$, dann sind die Abbildungen

$$f: \begin{array}{ccc} \mathbb{Z}/_{p\mathbb{Z}} & \to & \mathbb{Z}/_{p\mathbb{Z}} \\ x & \mapsto & x^n \end{array} \qquad \text{und} \qquad g: \begin{array}{ccc} \mathbb{Z}/_{p\mathbb{Z}} & \to & \mathbb{Z}/_{p\mathbb{Z}} \\ x & \mapsto & x^m \end{array}$$

invers zueinander.
Beweis: Schreibe $mn = (p-1)a + 1$ mit $a \in \mathbb{Z}$. Dann gilt:

$$(gf)(x) = (x^n)^m = x^{mn} = x^{(p-1)a} = x$$

da $x^{p-1} = 1$ für $x \in (\mathbb{Z}/_{p\mathbb{Z}})^x$ und analog $(fg)(x) = x^{mn} = x$. □

2.7 Satz (Chinesischer Restsatz)

Seien $m_1,\ldots,m_r \in \mathbb{Z}$ paarweise teilerfremd und seien $a_1,\ldots,a_r \in \mathbb{Z}$ beliebig. Dann besitzt das System

$$\begin{array}{rcl} x & \equiv & a_1 \pmod{m_1} \\ \vdots & & \vdots \\ x & \equiv & a_r \pmod{m_r} \end{array}$$

eine Lösung $b \in \mathbb{Z}$ und jede weitere Lösung unterscheidet sich von dieser um ein Vielfaches von $m_1,\ldots,m_r$.
Algebraisch: Die Abbildung

$$\begin{array}{rcl} \mathbb{Z}/_{(m_1\ldots m_r)\mathbb{Z}} & \to & \mathbb{Z}/_{m_1\mathbb{Z}} \times \ldots \times \mathbb{Z}/_{m_r\mathbb{Z}} \\ x & \mapsto & (x + m_1\mathbb{Z}, \ldots, x + m_r\mathbb{Z}) \end{array}$$

ist bijektiv.

Beweis: Wir zeigen Existenz und Eindeutigkeit:

Existenz: Sei $m = m_1 \dots m_r$ und $k_i = \frac{m}{m_i} = \prod_{j \neq i} m_j$ für $i = 1, \dots, r$. Dann gilt $\mathrm{ggT}(m_i, k_i) = 1$ und daher gibt es ein $l_i \in \mathbb{Z}$ mit $k_i l_i \equiv 1 \pmod{m_i}$. Nun betrachte

$$b = \sum_{i=1}^{r} a_i k_i l_i$$

Daher $b \equiv a_i k_i l_i \equiv a_i \pmod{m_i}$ für $i = 1, \dots, r$.

Eindeutigkeit: Seien b' und b'' zwei Lösungen und $b = b'' - b'$, dann gilt: $b \equiv 0 \pmod{m_i}$ für $i = 1, \dots, r$. Daher $m_i \mid b$ für $i = 1, \dots, r$ und daher folgt:

$$\underbrace{\prod_{i=1}^{r} m_i}_{m} \mid b \qquad \Rightarrow \qquad b' \equiv b'' \pmod{m}$$

□

2.8 Definition (Eulersche Phi-Funktion)

Die Abbildung $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ sei definiert durch

$$\varphi(n) = \#\{a \in \{0, \dots, n-1\} \mid \mathrm{ggT}(a, n) = 1\} = \#(\mathbb{Z}/_{n\mathbb{Z}})^x$$

Sie heißt die Eulersche Phi-Funktion.

2.9 Beispiel

Für eine Primzahl p gilt $\varphi(p) = p - 1$.

2.10 Korollar

a) Die Eulersche Phi-Funktion ist multiplikativ, d.h.

$$\varphi(mn) = \varphi(m)\varphi(n)$$

für $m, n \in \mathbb{N}_+$ mit $\mathrm{ggT}(m, n) = 1$.

b) Sei $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primfaktorzerlegung von $n \in \mathbb{N}_+$ mit paarweise verschiedenen Primzahlen $p_1, \dots, p_r$ und mit $\alpha_1, \dots, \alpha_r \in \mathbb{N}_+$. Dann gilt

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \dots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right) = n - \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Beweis:

Zu "*a*)": Die Zahl $\varphi(mn)$ ist die Zahl der Einheiten des Rings $\mathbb{Z}/_{(mn)\mathbb{Z}}$. Nach dem Chinesischen Restsatz gilt $\mathbb{Z}/_{(mn)\mathbb{Z}} \cong \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$. Hierbei gilt:

$$x \text{ Einheit} \qquad \Leftrightarrow \qquad x_1, x_2 \text{ Einheiten}$$

Dies liefert die Behauptung $\varphi(mn) = \varphi(m)\varphi(n)$.

Zu "*b*)": Nach (a) ist nur zu zeigen, dass für $n = p^\alpha$ gilt:

$$\varphi(n) = p^\alpha - p^{\alpha - 1}$$

Die zu n nicht teilerfremden Zahlen in $\{0, 1, 2, \dots, p^\alpha - 1\}$ sind $\left\{0, p, 2p, \dots, p\left(p^{\alpha-1} - 1\right) = p^\alpha - p\right\}$ und ihre Anzahl ist $p^{\alpha-1}$. □

2.11 Satz (Der Satz von Euler)

Sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}_+$ mit $\mathrm{ggT}(a,m) = 1$. Dann gilt $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Beweis:

1. Fall: p ist eine Primzahlpotenz. Induktion nach α:

$\alpha = 1$: Kleiner Fermatscher Satz.

$\alpha > 1$: Nach Induktionsvoraussetzung:

$$a^{\varphi\left(p^{\alpha-1}\right)} = a^{p^{\alpha-1}-p^{\alpha-2}} \equiv 1 \pmod{p^{\alpha-1}}$$

Daher gibt er ein $b \in \mathbb{Z}$ mit $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + bp^{\alpha-1}$. Für die p-te Potenz gilt: $(1+x)^p \equiv 1 + x^p \pmod{p}$. Damit:

$$a^{p^{\alpha}-p^{\alpha-1}} = 1 + b^p p^{\alpha} + cp \quad \text{mit } p^{\alpha-1} \mid c$$

Dann folgt:

$$a^{\varphi(p^{\alpha})} \equiv 1 \pmod{p^{\alpha}}$$

2. Fall: $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Dann folgt $a^{\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$ daraus, dass man $a^{\varphi\left(p_i^{\alpha_i}\right)} \equiv 1 \pmod{p_i^{\alpha_i}}$ zur entsprechenden Potenz erhebt. Nun liefert der Chinesische Restsatz die Behauptung. □

<FIXME>

Korrektur zur letzten Vorlesung vom 25.4.2005 - 1/3

Beispiel 2.2.a (neu)

Sei p Primzahl und $\overline{g} \in (\mathbb{Z}/_{p\mathbb{Z}})^{\times}$ ein Erzeuger, d.h. eine Restklasse, so dass $\left\{1, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2}\right\}$ paarweise verschieden sind.

1) Die Abbildung f : $\begin{array}{ccc} \mathbb{Z}/_{(p-1)\mathbb{Z}} & \to & (\mathbb{Z}/_{p\mathbb{Z}})^{\times} \\ x & \mapsto & \overline{g}^x \end{array}$ ist effizient berechenbar.

2) Ist $y = \overline{g}^x$ gegeben, so ist kein effizientes Verfahren zur Berechnung von x bekannt ("diskretes Log-Problem").

Also ist f ein Kandidat für eine Einweg-Funktion.

Korrektur zur letzten Vorlesung vom 25.4.2005 - 2/3

Beispiel 2.2.c

Seien p, q verschiedene Primzahlen und $n = pq$. Ferner seien $d, e \in \mathbb{Z}$ mit $de \equiv 1 \pmod{\varphi(n)}$, wobei für n Primzahl gilt, dass $\varphi(n) = (p-1)(q-1)$,

1) Die Abbildung f : $\begin{array}{ccc} \mathbb{Z}/_{n\mathbb{Z}} & \to & \mathbb{Z}/_{n\mathbb{Z}} \\ x & \mapsto & x^e \end{array}$ ist effizient berechenbar.

2) Kennt man d, so ist die Abbbildung g : $\begin{array}{ccc} \mathbb{Z}/_{n\mathbb{Z}} & \to & \mathbb{Z}/_{n\mathbb{Z}} \\ x & \mapsto & x^d \end{array}$ effizient berechenbar.

3) Kennt man d, p, q nicht, so ist kein effizientes Verfahren bekannt, aus $y = x^e$ die Restklasse x zu bestimmen.

4) Für $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x,n) = 1$ gilt

$$(g \circ f)(x) = (x^e)^d = x^{c\varphi(n)+1} \equiv x \pmod{n}$$

5) Man kann d genau dann aus n, e effizient berechnen, wenn man p, q kennt. Für die Primfaktorzerlegung von n ist kein effizientes Verfahren bekannt.

Also ist f ein Kandidat für eine Einweg-Funktion mit Falltür.

Korrektur zur letzten Vorlesung vom 25.4.2005 - 3/3

Beweis zu 2.11 (Ende)

$a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + bp^{\alpha-1}$ mit $b \in \mathbb{Z}$. Für die p-te Potenz gilt nun:

$$\begin{aligned} a^{p^{\alpha}-p^{\alpha-1}} &= 1 + p\left(bp^{\alpha-1}\right) + \binom{p}{2}\left(bp^{\alpha-1}\right)^2 + \ldots + \binom{p}{p}\left(bp^{\alpha-1}\right)^p \\ &\equiv 1 \pmod{p^{\alpha}} \end{aligned}$$

</FIXME>

B Das RSA-Kryptosystem

RSA="Rivest, Shamir, Ademan" (Arbeit von 1978)

2.12 Beispiel

Das RSA-Kryptosystem besteht aus folgenden Teilen:

1) Wir arbeiten mit dem Alphabet mit $N = 26$ Buchstaben. Wähle $k < l$ "groß genug", z.B. so dass N^k mindestens 200 Stellen hat.

2) Sei $\tilde{\mathcal{P}} = \{\text{Blöcke von } k \text{ Klartextzeichen}\} \cong \mathbb{Z}/_{N^k\mathbb{Z}}$ und $\tilde{\mathcal{C}} = \{\text{Blöcke von } l \text{ Geheimtextzeichen}\} \cong \mathbb{Z}/_{N^l\mathbb{Z}}$.

3) Wähle "sehr große" Primzahlen p,q, z.B. mindestens 100 Stellen, und berechne $n = pq$. Wähle dabei p,q so, dass $N^k < n < N^l$ gilt.

4) Berechne $\varphi(n) = (p-1)(q-1) = n-p-q+1$ und wähle eine Zufallszahl $e \in \{1,\ldots,\varphi(n)\}$ mit $\mathrm{ggT}(e,\varphi(n)) = 1$.

5) Berechne eine Zahl $d \in \{1,\ldots,\varphi(n)\}$ mit $de \equiv 1 \pmod{\varphi(n)}$ mit Hilfe des erweiterten Euklidischen Algorithmus.

6) Das Paar (n,e) heißt der öffentliche Schlüssel.

7) Wir wählen $\mathcal{P} = \mathcal{C} = \mathbb{Z}/_{n\mathbb{Z}}$. Der Klartext wird mit eine injektiven Abbildung $\varphi : \tilde{\mathcal{P}} \to \mathcal{P}$ in eine Folge von Restklassen in $\mathbb{Z}/_{n\mathbb{Z}}$ umgewandelt.

8) Die Verschlüsselungsfunktion ist $f : \begin{array}{ccc} \mathbb{Z}/_{n\mathbb{Z}} & \to & \mathbb{Z}/_{n\mathbb{Z}} \\ x & \mapsto & x^e \end{array}$.

9) Die Entschlüsselungsfunktion ist $g : \begin{array}{ccc} \mathbb{Z}/_{n\mathbb{Z}} & \to & \mathbb{Z}/_{n\mathbb{Z}} \\ x & \mapsto & x^d \end{array}$. Der Geheimschlüssel ist die Zahl d. Nach Anwendung von g gilt:

$$(g \circ f)(x) = (x^e)^d \overset{(1)}{=} x \quad (\text{in } \mathbb{Z}/_{n\mathbb{Z}})$$

Zu (1): Nach Euler.

10) Der Geheimtext wird (meist) mit Hilfe einer injektiven Abbildung $\psi : \mathcal{C} \to \tilde{\mathcal{C}}$ in eine Folge von Geheimtextblöcken aus je l Buchstaben umgewandelt, die dann übertragen werden.

2.13 Bemerkung (Durchführbarkeit von RSA)

a) Es gibt schnelle Tests dafür, zu entscheiden, ob eine groß Zahl Primzahl ist. Angenommen wir suchen eine Primzahl p mit $10^a < p < 10^b$ mit $a < b$. Wähle eine ungerade Zufallszahl $\tilde{p}$ in diesem Intervall. Teste, ob $\tilde{p}$ eine Primzahl ist. Wenn nicht, dann teste $\tilde{p}+2$, $\tilde{p}+4$, usw. bis eine Primzahl gefunden wird. Dies ist effizient. Wir erhalten p und analog q und damit $n = pq$.

b) Wähle eine ungerade Zufallszahl $\tilde{e} \in \{1,\ldots,\varphi(n)\}$. Test mit dem Euklidischen Algorithmus, ob $\mathrm{ggT}(\tilde{e},\varphi(n)) = 1$ gilt. Wenn nicht, versuche $\tilde{e}+2$, usw. Wir erhalten e und d dann mit Hilfe der erweiterten Euklidischen Algorithmus.

Kryptoanalyse:

Idee: Seien p,q,n,e,d wie im RSA Kryptosystem. Man kann d aus (n,e) genau dann berechnen, wenn man die Primfaktorzerlegung von $n = pq$ berechnen kann.

"$\Leftarrow$": klar.

"$\Rightarrow$": Siehe folgende Sätze.

2.14 Satz

Sei $n \in \mathbb{N}_+$ eine Zahl, die das Produkt zweier verschiedener Primzahlen p,q ist. Man kennt (p,q) genau dann, wenn man $\varphi(n)$ kennt. Aus dem Paar (p,q) kann man $\varphi(n)$ effizient berechnen und umgekehrt.

Beweis:

Zu "$\Rightarrow$": $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n-p-q+1$ effizient berechenbar.

Zu "$\Leftarrow$": $p+q = n-\varphi(n)+1$ und $pq = n$. Daher sind p,q die Lösungen der quadratischen Gleichung

$$x^2 - (n-\varphi(n)+1)x + n = 0$$

und damit effizient berechenbar. □

2.15 Satz

Sei $n \in \mathbb{N}_+$ eine Zahl, die das Produkt zweier verschiedener Primzahlen p,q ist. Angenommen man kennt eine Zahl $m > 0$ mit

$$a^m \equiv 1 \pmod{n}$$

für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Dann kann man die Primfaktorzerlegung $n = pq$ mit folgendem probabilistischen Algorithmus bestimmen:

1) Prüfe für viele Zahlen, z.B. für 100, zufällig gewählte Zahlen $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ ob $a^{\frac{m}{2}} \equiv 1 \pmod{n}$ gilt. Ist dies der Fall, so ersetze m durch $\frac{m}{2}$.

2) Wiederhole Schritt 1 so oft wie möglich.

3) Für zufällige gewähltes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ berechne

$$\tilde{p} = \mathrm{ggT}\left(n, a^{\frac{m}{2}} - 1\right)$$

und prüfe, ob $\tilde{p}$ ein echter Teiler von n ist.

4) Wiederhole Schritt 3, so lange bis ein echter Teiler von n gefunden wird.

Dies ist ein probabilistischer Algorithmus, d.h. mit einer genügend nahe bei 1 liegenden Wahrscheinlichkeit erhalten wir nach endlich vielen Schritten das korrekte Ergebnis.

2.16 Lemma

Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ und $a^{\frac{m}{2}} \not\equiv 1 \pmod{n}$. So ist dies für mindestens 50% der Elemente $\overline{a} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ der Fall.

Beweis: Sei $\overline{b} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$. Gilt $b^{\frac{m}{2}} \equiv 1 \pmod{n}$ und $a^{\frac{m}{2}} \not\equiv 1 \pmod{n}$, dann folgt

$$(ab)^{\frac{m}{2}} \not\equiv 1 \pmod{n}$$

Also: Die Elemente $\overline{b}$ mit $\overline{b}^{\frac{m}{2}} = 1$ in $(\mathbb{Z}/_{n\mathbb{Z}})^\times$ bilden höchstens 50% von $(\mathbb{Z}/_{n\mathbb{Z}})^\times$, da die Elemente $\overline{ab}$ paarweise verscheiden sind. □

2.17 Lemma

Es gebe ein $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$, $a^m \equiv 1 \pmod{n}$ und $a^{\frac{m}{2}} \not\equiv 1 \pmod{n}$. Dann gilt: $\overline{b}^{\frac{m}{2}} = 1$ für genau 50% der Elemente $\overline{b} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ und $\overline{b}^{\frac{m}{2}} = -1$ für die restlichen 50%.

Beweis: Sei $n = pq$. Aus $a^m \equiv 1 \pmod{n}$ folgt $a^m \equiv 1 \pmod{q}$ nach dem Chinesischen Restsatz $\begin{array}{ccc} \mathbb{Z}/_{n\mathbb{Z}} & \to & \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{q\mathbb{Z}} \\ \overline{1} & \mapsto & (\overline{1},\overline{1}) \end{array}$.

In dem Körper $\mathbb{Z}/_{q\mathbb{Z}}$ folgt $\overline{a}^{\frac{m}{2}} \in \{-1,1\}$, denn $x^2 = 1$ hat genau zwei Lösungen $x = \pm 1$. Anders ausgedrückt in $\mathbb{Z}/_{q\mathbb{Z}}[x]$ gilt $x^2 - 1 = 0 \Rightarrow (x+1)(x-1) = 0 \Rightarrow x = \pm 1$.

Es gibt mindestens ein $\overline{a}$ mit $\overline{a}^{\frac{m}{2}} = -1$. Nach Lemma 2.16 folgt: Höchstens 50% der $\overline{c}$ erfüllen $\overline{c}^{\frac{m}{2}} = 1$. Für alle $\overline{b} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ mit $\overline{b}^{\frac{m}{2}} = -1$ gilt:

$$\left(\overline{a}\overline{b}\right)^{\frac{m}{2}} = 1$$

Höchstens 50% der $\overline{c}$ erfüllen $\overline{c}^{\frac{m}{2}} = -1$. □

Beweis von Satz 2.15

1) Die Schleife aus Schritt 1-2 terminiert mit beliebig hoher Wahrscheinlichkeit und liefert ein $\overline{a} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ mit $\overline{a}^{\frac{m}{2}} = -1$ für 50% der Restklassen $\overline{a}$ und $\overline{a}^{\frac{m}{2}} = 1$ für die restlichen 50% nach Lemma 2.17. Sei nun $\tilde{a} \in \mathbb{Z}$ mit $\mathrm{ggT}(\tilde{a},n) = 1$ und $\tilde{a}^{\frac{m}{2}} \equiv 1 \pmod{n}$ .Dann gilt es zwei Fälle:

1. Fall: $(p-1) \mid \frac{m}{2}$ oder $(q-1) \mid \frac{m}{2}$. OE gelte $(p-1) \mid \frac{m}{2}$. Dann kann nicht $(q-1) \mid \frac{m}{2}$, da sonst $\varphi(n) \mid \frac{m}{2}$. Dies ist ein Widerspruch zu $\tilde{a}^{\frac{m}{2}} \not\equiv 1$ (Euler). Daher:

$$\begin{aligned} a^{\frac{m}{2}} &\equiv 1 \pmod{p} \quad \text{für alle } a \\ a^{\frac{m}{2}} &\not\equiv 1 \pmod{q} \quad \text{für mindestens ein } a \end{aligned}$$

Wenn man den Schritt 3 oft genug wiederholt, so findet man ein solches a mit $a^{\frac{m}{2}} \equiv 1 \pmod{1}$ und $a^{\frac{m}{2}} \not\equiv 1 \pmod{q}$. Damit folgt: $\mathrm{ggT}\left(n, a^{\frac{m}{2}} - 1\right) = p$ und damit ist n faktorisiert.

2. Fall: $\frac{m}{2}$ ist weder durch $p-1$ noch durch $q-1$ teilbar.

Nach Lemma 2.17 gibt es drei Fälle:

a) $a^{\frac{m}{2}} \equiv 1 \pmod{p}$ und $a^{\frac{m}{2}} \equiv 1 \pmod{q}$ in 25% aller Fälle

b) $a^{\frac{m}{2}} \equiv -1 \pmod{p}$ und $a^{\frac{m}{2}} \equiv -1 \pmod{q}$ in 25% aller Fälle

c) $a^{\frac{m}{2}} \equiv -1 \pmod{p}$ und $a^{\frac{m}{2}} \equiv 1 \pmod{q}$ oder $a^{\frac{m}{2}} \equiv 1 \pmod{p}$ und $a^{\frac{m}{2}} \equiv -1 \pmod{q}$ in 50% aller Fälle

Wenn man Schritt 3 oft genug wiederholt, dann tritt der Fall c) ein und dann $\mathrm{ggT}\left(a^{\frac{m}{2}}-1, n\right) \in \{p,q\}$ und n ist faktorisiert. □

2.18 Korollar

In obiger Situation sind folgende Bedingungen äquivalent:

a) Man kann aus (n,e) effizient das d berechnen.

b) Man kann die Primfaktoren p,q von n effizient berechnen.

Beweis:

Zu $(a) \Rightarrow (b)$: Kennt man d, so gilt $de \equiv 1 \pmod{\varphi(n)}$. Also ist $de-1$ durch $(p-1)(q-1)$ teilbar. Nach dem Satz von Euler folgt $a^{de-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Daher kann man p,q mit dem Algorithmus aus Satz 2.15 effizient berechnen.

Zu $(b) \Rightarrow (a)$: Es gilt $\varphi(n) = (p-1)(q-1)$. Dann kann man mit dem erweiterten Euklidischen Algorithmus c,d bestimmen mit $c\varphi(n) + de = 1$. Dann ist $de \equiv 1 \pmod{n}$. □

2.19 Bemerkung (Kryptoanalyse des RSA-Kryptosystems)

a) Die Primzahlen p,q müssen geschickt gewählt sein, weil es sonst möglich ist das n zu faktorisieren. Zum Beispiel muß gelten:

1) p und q müssen verschieden viele Stellen haben.

2) $p-1$ und $q-1$ müssen einen vergleichsweise kleinen ggT haben.

3) $p-1$ und $q-1$ müssen jeweils einen großen Primfaktor haben.

d) Es gibt Zahlentypen für n, die sich leichter zerlegen lassen, z.B. Zahlen n, die knapp unter einer 2-er Potenz liegen.

c) Ist die zu verschlüsselnde Nachricht sehr klein, oder der letzte Block des Klartextes zu kurz, so muss der Klartext mit Zufallsbits aufgefüllt werden.

d) Zu kleine Werte von e können aus mehreren Gründen unsicher sein. Z.B. ist der häufig verwendete Werte $e = 3$ unsicher. Man sollte $e \geq 20$ wählen.

e) Man darf nicht an mehrere Empfänger die gleiche Nachricht mit unterschiedlichem n aber gleichem e senden.

f) Es ist sehr wichtig, dass auch d genügend groß ist.

g) Die Methode zur Erzeugung von p und q muss ein wirklich zufälliges Paar von Primzahlen erzeugen.

h) Der Kryptoanalyst kann versuchen den Klartext zu erraten und seinen Tipp sofort nachprüfen.

i) Man muss eine große (ca. 200-stellige) Zahl geheimhalten.

j) Die schnellsten RSA Chips schaffen nur 10-100 kbits/s. Da dies zu langsam ist, muss man auf "Hybridverfahren" ausweichen, z.B. PGP, SWIFT. Dabei: Schlüsselaustausch mit RSA, dann Übertragung der Daten mit klassischem Kryptosystem.

2.20 Bemerkung

Im Jahr 1999 hat die 16-jährige Sarah Flannery (aus Irland) ein RSA-ähnliches Kryptosystem veröffentlich, das Multiplikationen von 2×2 Matrizen verwendet und so die Verschlüsselungsgeschwindigkeit um den Faktor 10 erhöht. Allerdings wurde das Verfahren gebrochen.

C: Das ElGamal Kryptosystem

1985 von Taher ElGamal vorgeschlagen. Idee: Die Berechnung von "diskreten Logarithmen" ist schwer.

2.21 Definition (Diskreter Logarithmus)

Sei G eine endliche Gruppe, $b \in G$ und $y \in G$ eine Potenz von b. Dann heißt jedes $x \in \mathbb{Z}$ mit $b^x = y$ ein diskreter Logarithmus von y zur Basis b. Schreibweise $x = \log_b(y)$.

2.22 Beispiel

In $G = (\mathbb{Z}/_{19\mathbb{Z}})^\times$ gilt $6 = \log_2(7)$, denn $2^6 = 64 \equiv 7 \pmod{19}$

2.23 Definition

Das ElGamal Kryptosystem besteht aus folgenden Daten:

1) Wähle eine große Primzahl p und $g \in \mathbb{N}_+$, die öffentlich sind. Vorzugsweise sollte $\overline{g}$ ein Erzeuger von $(\mathbb{Z}/_{p\mathbb{Z}})^\times$ sein.

2) Wähle ein festes, invertierbares Verfahren zur Übertragung der Klartexteinheiten in Restklassen in $\mathcal{P} = (\mathbb{Z}/_{p\mathbb{Z}})^\times$.

3) Wähle einen geheimen Schlüssel $a \in \{1,\dots,p-1\}$ und berechne $b = g^a \pmod{p}$. Diese Zahl $b \in \{1,\dots,p-1\}$ wird als öffentlicher Schlüssel bekannt gegeben.

4) Um eine Klartexteinheit $m \in (\mathbb{Z}/_{p\mathbb{Z}})^\times$ zu verschlüsseln wähle eine Zufallszahl $k \in \{1,\dots,p-1\}$ und berechne $c = \left(\overline{g^k}, \overline{mb^k}\right) \in (\mathbb{Z}/_{p\mathbb{Z}})^\times \times (\mathbb{Z}/_{p\mathbb{Z}})^\times$. Dies sei die zu m gehörige Geheimtexteinheit.

5) Also gilt $\mathcal{C} = (\mathbb{Z}/_{p\mathbb{Z}})^\times \times (\mathbb{Z}/_{p\mathbb{Z}})^\times$.

6) Um ein Paar $(x,y) \in \mathcal{C}$ zu entschlüsseln, berechnet man mit Hilfe von a die Potenz $\overline{x}^a \in (\mathbb{Z}/_{p\mathbb{Z}})^\times$ und erhält $m = \frac{y}{x^a} \in (\mathbb{Z}/_{p\mathbb{Z}})^\times$.

Korrektheit: $\overline{x}^a = \left(\overline{g}^k\right)^a = (\overline{g}^a)^k = \overline{b}^k \Rightarrow y/x^a = mb^k/b^k = m$.

2.24 Bemerkungen

a) Man kann im ElGamal Kryptosystem auch andere Gruppen (statt $(\mathbb{Z}/_{p\mathbb{Z}})^\times$) verwenden, in denen der diskrete Logarithmus schwer zu berechnen ist, z.B. $\mathbb{F}_q^x$ mit $q = p^e$, $e > 0$ und p prim. $\mathbb{F}_q^x$ sind die Einheitengruppen der endlichen Körper. Besonders effizient implementierbar ist der Fall $q = 2^e$.

b) Man kann das ElGamal Kryptosystem brechen, wenn man zu $\overline{g}^a$ den diskreten Logarithmus $a = \log_g(g^a)$ berechnen kann.

2.25 Bemerkung (Kryptoanalyse des ElGamal Kryptosystems)

a) Es genügt von $\overline{g}^a = b$ und $\overline{g}^k$ auf $\overline{g}^{ak}$ zu schließen, um ElGamal zu brechen. Es wird vermutet, dass der Schluss von $\overline{g}^a$ und $\overline{g}^k$ auf $\overline{g}^{ak}$ den gleichen Rechenaufwand benötigt wie der Schluss von $\overline{g}^a$ auf a.

b) Man muss das p so wählen, dass $p-1$ nicht nur "kleine" Primfaktoren hat (siehe unten), günstig ist z.B. wenn $\frac{p-1}{2}$ prim ist.

c) Die zur Verschlüsselung verwendeten Zufallszahlen k dürfen nicht rekonstruierbar sein.

d) Die Zahlen k müssen zu $p-1$ teilerfremd sein.

e) Im Fall $q = 2^e$ gibt es einen schnellen Algorithmus von D. Coppersmith zur Berechnung diskreter Algorithmen. In diesem Fall ist mindestens $e > 1000$ nötig, damit ElGamal sicher ist.

Korrektheit: Es gilt:

$$\left(mb^k\right)\left(\left(g^k\right)^a\right)^{-1} = mg^{ak}g^{-ak} = m$$

Ziel: Breche El Gamal, falls $p-1$ nur "keine" Primfaktoren besitzt.

2.26 Satz (Der Algorithmus von Silver-Pohlig-Hellman)

Gegeben sei eine Primzahl p, ein Erzeuger $\langle g \rangle = (\mathbb{Z}/_{p\mathbb{Z}})^\times$ und $y \in (\mathbb{Z}/_{p\mathbb{Z}})^\times$. Gesucht: $x \in \{0,\dots,p-2\}$ mit $g^\times = y$.

a) Schreibe $p-1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ Primfaktorzerlegung. Es genügt die Restklasse $\overline{x} \in \mathbb{Z}/_{p_i^{\alpha_i}\mathbb{Z}}$ zu finden für $i = 1,\dots,r$.

b) Sei $i \in \{1,\dots,r\}$ fest. Setze $g_i = p_i^{\alpha_i}$. Betrachte folgende Instruktionen:

1) Für $j = 1, \ldots, p-1$ berechne $r_{i,j} = g^{j\frac{p-1}{p_i}} \in \mathbb{Z}/_{p\mathbb{Z}}$.

2) Berechne $y^{\frac{p_i-1}{p}}$ und finde $j \in \{0, \ldots, p_i - 1\}$ mit $r_{i,j} = y^{\frac{p-1}{p_i}}$. Setze $x_0 = j$.

3) Für $k = 1, \ldots, \alpha_i - 1$ und berechne $y_k = y^{x_0 + x_1 p_i + \ldots + x_{k-1} p_i^{k-1}}$ und finde ein j mit $y_k^{\frac{p-1}{p^{k+1}}} = r_{i,j}$. Setze $x_k = j$.

4) Gib $x = x_0 + x_1 p_i + \ldots x_{\alpha_i - 1} p_i^{\alpha_i - 1} \,(\mathrm{mod}\, q_i)$ aus.

Dies ist ein Algorithmus der $\bar{x} \in \mathbb{Z}/_{q_i\mathbb{Z}}$ berechnet mit $\bar{g}^{\bar{x}} = \bar{y}$ in $\mathbb{Z}/_{p\mathbb{Z}}$.

Beweis:

Zu "a": Folgt aus dem Chinesischen Restsatz.

Zu "b": Schreibe das gesuchte $\bar{x} \in (\mathbb{Z}/_{q_i\mathbb{Z}})$ inder Form

$$\bar{x} = x_0 + x_1 p_i + \ldots + x_{\alpha_i - 1} p_i^{\alpha_i - 1}$$

(Repräsentant $\in \{0, \ldots, p_i^{\alpha_i} - 1\}$)

Zu zeigen ist, dass der Algorithmus die $x_0, \ldots, x_{\alpha_i - 1}$ korrekt berechnet. $\bar{y} = \bar{g}^x$.

Für $j = 0$:

$$y^{\frac{p-1}{p_i}} = \bar{g}^{x\frac{p-1}{p_i}} = \bar{g}^{x_0\frac{p-1}{p_i}} \underbrace{\left(\bar{g}^{x_1 p_i \frac{o-1}{p_1}} \ldots\right)}_{(*)} = \bar{g}^{x_0\frac{p-1}{p_i}}$$

Da $(*) = \bar{g}^{z(p-1)} = 1$ in $(\mathbb{Z}/_{p\mathbb{Z}})^\times$ da $\bar{g}^{p-1} = 1$ in $(\mathbb{Z}/_{p\mathbb{Z}})^\times$.

Für $j \geq 1$: Es gilt:

$$\begin{aligned} y_k^{\frac{p-1}{p_i^{k+1}}} &= \left(\frac{g^x}{g^{x_0 + x_1 p_i + \ldots + x_{k-1} p_i^{k-1}}}\right)^{\frac{p-1}{p_i^{k+1}}} \\ &= \left(g^{x_{k_i} p_i^{k_i} + \ldots + x_{\alpha_1 - 1} p_i^{\alpha_i - 1}}\right)^{\frac{p-1}{p_i^{k+1}}} \\ &= g^{x_k p_i^l \frac{p-1}{p_i^{k+1}}} g^{\tilde{z}(p-1)} \\ &= g^{x_k \frac{p-1}{p_i}} \\ &= x_{i,x_k} \end{aligned}$$

Daher ist x_k korrekt. □

Anwendung: Nachdem eine Primzahl $p \gg 0$ gewählt wurde, spalte "kleine" Primfaktoren von $p-1$ ab so lange wie möglich. Führt dies zu einer vollständigen Faktorisierung von $p-1$, so ist p ungeeignet für ElGamal.

2.27 WTF 2.27 - FIXME

D. Pseudozufallszahlen

Frage: Wie findet man "große" Primzahlen? Gesucht sind also Primzahltests.

2.28 Bemerkung

a) Ist $n \in \mathbb{N}_+$ ungerade und nicht zu groß, so kann man für $i = 3, 5, 7, \ldots$ mit $i \leq \sqrt{n}$ nachprüfen, ob n durch i teilbar ist. Dieser Test ist nicht effizient.

b) Ist $n \in \mathbb{N}_+$ Primzahl und $b \in \mathbb{N}_+$ mit $\mathrm{ggT}(n, b) = 1$, so gilt $b^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$ nach dem kleinen Fermatschen Satz. Finden wir also ein b mit $\mathrm{ggT}(n, b) = 1$ mit $b^{n-1} \not\equiv 1 \,(\mathrm{mod}\, n)$, so ist n keine Primzahl.

2.29 Definition (Pseudoprimzahl)

Ist $n \in \{3, 5, 7, \ldots\}$ und $b \in \mathbb{N}$mit $\mathrm{ggT}(n, b) = 1$ und $b^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$, so heißt n eine Pseudoprimzahl zur Basis b.

2.30 Beispiel

a) $n = 91$ ist Pseudoprimzahl zur Basis 3, denn $3^{90} \equiv 1 \pmod{91}$.

b) $n = 91$ ist keine Pseudoprimzahl zur Basis 2, denn $2^{90} \equiv 64 \pmod{91}$. Also ist 91 keine Primzahl.

2.31 Satz

Sei $n \in \mathbb{N}_+$.

a) Sei $b \in \mathbb{N}_+$ mit $\mathrm{ggT}(n,b) = 1$. Genau dann ist n eine Pseudoprimzahl zur Basis b, wenn die Ordnung von $\overline{b} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ ein Teiler von $n-1$ ist. Hierbei ist $\mathrm{ord}(\overline{b}) = \min\left\{ i > 0 \mid \overline{b}^i = 1 \right\}$.

b) Seien $b_1, b_2 \in \mathbb{N}_+$ mit $\mathrm{ggT}(n,b_1) = \mathrm{ggT}(n,b_2) = 2$. Ist n eine Pseudoprimzahl zur Basis b_1 und zur Basis b_2, so ist n auch eine Pseudoprimzahl zu Basis $b_1 b_2$ und zur Basis $b_1 \tilde{b}_2$ mit $\tilde{b}_2 = b_2^{-1}$ in $(\mathbb{Z}/_{n\mathbb{Z}})^\times$.

c) Ist n keine Pseudoprimzahl zu Basis $\tilde{b}$, so ist n keine Pseudoprimzahl zu Basis b für mindestens 50% aller Basen $b \in \{1,\ldots,n-1\}$ mit $\mathrm{ggT}(n,b) = 1$.

Beweis:

Zu (a): Zu "$\Rightarrow$" : Die folgt aus $\overline{b}^{n-1} = 1$ in $(\mathbb{Z}/_{n\mathbb{Z}})^\times$. Daher $\mathrm{ord}(b) \mid (n-1)$.

Zu "$\Leftarrow$" : Schreibe $n-1 = c\,\mathrm{ord}(b)$. Dann folgt

$$\overline{b}^{n-1} = \left(\overline{b}^{\mathrm{ord}(b)}\right)^c = 1^c = 1$$

in $(\mathbb{Z}/_{n\mathbb{Z}})^\times$. Also ist n Pseudoprimzahl zu Basis b.

Zu (b): Es gilt $b_1^{n-1} = 1 \pmod{n}$ und $b_2^{n-1} = 1 \pmod{n}$. Daher folgt:

$$(b_1 b_2)^{n-1} = b_1^{n-1} b_2^{n-1} = 1 \pmod{n} \quad \text{und} \quad \tilde{b}_2^{n-1} = \tilde{b}_2^{n-1} b_2^{n-1} = \left(\tilde{b}_2 b_2\right)^{n-1} = 1 \pmod{n}$$

und damit $\left(b_1 b_2^2\right)^{n-1} = 1 \pmod{n}$.

Zu (c): Seien $\{b_1,\ldots,b_s\} \subseteq \{1,\ldots,n-1\}$ die Basen mit $\mathrm{ggT}(n,b_i) = 1$ bzgl. denen n Pseudoprimzahl ist. Weiter sei $\tilde{b} \in \mathbb{N}_+$ mit $\tilde{b}^{n-1} \not\equiv 1 \pmod{n}$.

Dann folgt: Für paarweise verschiedene Elemente $b_i \tilde{b} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ gilt

$$\left(b_i \tilde{b}\right)^{n-1} = b_i^{n-1} \tilde{b}^{n-1} = \tilde{b}^{n-1} \not\equiv 1 \pmod{n}$$

Also gibt es mindestens 50% der Basen $b \in \{1,\ldots,n-1\}$ mit $\mathrm{ggT}(n,b) = 1$ bzgl. denen n keine Pseudoprimzahl ist. □

2.32 Korollar (Pseudoprimzahltest)

Sei $n \in \mathbb{N}_+$ ungerade. Betrachte die folgenden Instruktionen:

1) Wähle eine Zufallszahl $b \in \{1,\ldots,n-1\}$.

2) Berechne $\mathrm{ggT}(b,n)$. Gilt $\mathrm{ggT}(n,b) > 0$, so gib "n zusammengesetzte Zahl aus" und stoppe.

3) Berechne $b^{n-1} \pmod{n}$. Gilt $b^{n-1} \not\equiv 1 \pmod{n}$, so gib "$n$ zusammengesetzte Zahl aus" und stoppe.

4) Wiederhole die Schritte 1-3 k-mal (mit einem fest gewählten k). Ergibt sich stets $b^{n-1} \equiv 1 \pmod{n}$, so gib "Test bestanden" aus und stoppe.

Dies ist ein probabilistischer Algorithmus, der mit Wahrscheinlichkeit $> 1 - \frac{1}{2^k}$ korrekt feststellt, ob n zu jeder Basis $b \in \{1,\ldots,n-1\}$ mit $\mathrm{ggT}(n,b) = 1$ Pseudoprimzahl ist.

Beweis: Folgt sofort aus Satz 2.31. □

2.33 Definition (Carmichael Zahl)

Eine zusammengesetzte Zahl $n \geq 3$ mit $b^{n-1} \equiv 1 \pmod{n}$ für alle $b \in \{1,\ldots,n-1\}$ mit $\mathrm{ggT}(n,b) = 1$ heißt Carmichael Zahl.

2.34 Bemerkung

Sei p ungerade Primzahl und $p-1 = 2^s t$ mit $s \geq 1$ und t ungerade. Für $i = 0,\ldots,s$ betrachte $\overline{b^{2^i t}} \in (\mathbb{Z}/_{p\mathbb{Z}})^\times$. Gibt es ein $i \in \{0,\ldots,s-1\}$ mit $\overline{b^{2^i t}} \neq 1$ und $\overline{b^{2^{i+1} t}} = 1$, so gilt $\overline{b^{2^i t}} = -1$. Dies folgt daraus, dass die Gleichung $x^2 - 1 = 0$ in dem Körper nur die Lösungen $x = \pm 1$ besitzt.

2.35 Definition

Sei $n > 3$ eine ungerade zusammengesetzte Zahl. Schreibe $n-1 = 2^s t$ mit $s \geq 1$ und t ungerade. Ferner sei $b \in \{1,\ldots,n-1\}$ mit $\mathrm{ggT}(n,b) = 1$. n heißt starke Pseudoprimzahl zur Basis b, wenn entweder $b^t \equiv 1 \pmod n$ gilt oder es gibt eine Zahl $i \in \{0,\ldots,s-1\}$ mit $b^{2^i t} \equiv -1 \pmod n$.

2.36 Satz

Ist $n > 3$ eine ungerade zusammengesetzte Zahl, so ist n eine starke Pseudoprimzahl zur Basis b für höchstens 25% der Zahlen $b \in \{1,\ldots,n-1\}$ mit $\mathrm{ggT}(n,b) = 1$.

Beweis: Vgl. Koblitz, Seiten 117-121. □

2.37 Korollar (Der Miller-Rabin Primzahltest)

Sei $n \gg 3$ eine ungerade Zahl. Betrachte folgende Instruktionen:

1) Schreibe $n-1 = 2^s t$ mit $s \geq 1$ und t ungerade.

2) Wähle eine Zufallszahl $b \in \{1,\ldots,n-1\}$ und berechne $\mathrm{ggT}(n,b)$. Gilt $\mathrm{ggT}(n,b) > 1$, so gib "n ist zusammengesetzt" aus und stoppe.

3) Berechne $b^t \pmod n$. Gilt $b^t \equiv 1 \pmod n$ oder $b^t \equiv -1 \pmod n$, so fahre mit Schritt 5 fort.

4) Berechne $(b^t)^2 \pmod n$, $(b^t)^4 \pmod n$ und prüfe, ob es ein $i < s$ gibt mit $p^{2^i t} \equiv -1 \pmod n$. Ist dies irgendwann der Fall, so fahre mit Schritt 5 fort. Andernfalls erhalte $i \in \{0,\ldots,s-1\}$ mit $b^{2^i t} \not\equiv 1 \pmod n$ und $b^{2^i t} \not\equiv -1 \pmod n$ und $b^{2^{i+1} t} \equiv 1 \pmod n$. In diesem Fall gib "$n$ ist zusammengesetzt" aus und stoppe.

5) Widerhole die Schritte 2-4 k-mal mit einer fest gewählten Zahl k. Ergibt sich stets $b^t \equiv 1 \pmod n$ oder $b^{2^i t} \equiv -1 \pmod n$ für ein $i \in \{0,\ldots,s-1\}$, so gib "Test bestanden" aus und stoppe.

Dies ist ein probabilistischer Algorithmus, der mit Wahrscheinlichkeit $> 1 - \frac{1}{4^k}$ korrekt feststellt, ob n zusammengesetzt ist oder nicht.

Beweis: Folgt aus Satz 2.36. □

2.38 Bemerkung

a) In der Praxis braucht man nur für wenige Basen b zu prüfen, ob n eine starke Pseudoprimzahl zu Basis b ist. Für $n < 2.5 \cdot 10^{10}$ gibt es nur eine einzige starke Pseudoprimzahl zu den Basen $2,3,5$und 7, nämlich 3215031751. Ist die verallgemeinerte Riemannsche Vermutung richtig, so gibt es zu jeder zusammengesetzten Zahl $n > 3$ eine Basis $b < 2(\log(n))^2$, so dass der obige Test fehlschlägt.

3 Protokolle

Ziel: Mehrere Personen/Parteien wollten gemeinsam eine gewisse Aufgabe erledigen. Jede Partei muss sich dann an gewisse Regeln halten. Die Gesamtheit dieser Regeln nennt man ein Protokoll.

Konkrete Fälle:

- Würfeln übers Internet
- Digitale Signaturen (Unterschrift)
- Authentifikation
- Zero-Knowledge Beweise

A Hashfunktionen

3.1 Definition

Seien M_1, M_2 Mengen. Eine (Einweg-)Hashfunktion oder kryptographische Hashfunktion ist eine Abbildung $f : M_1 \to M_2$ mit den folgenden Eigenschaften:

1. f ist kollisionsfrei, d.h. es gibt kein effizientes Verfahren um zwei Elemente $x_1, x_2 \in M_1$ zu finden mit $f(x_1) = f(x_2)$.
2. Die Abbildung f ist eine Einwegfunktion, d.h. es gibt ein effizientes Verfahren zur Berechnung von $y = f(x)$ aus $x \in M$, aber kein effizientes Verfahren um aus $y \in \text{Bild}(f)$ ein $x \in M_1$ zu bestimmen.

Gute Hashfunktionen sind in der Praxis seht selten.

3.2 Beispiel (Münzwurf übers Internet)

A und B wollen übers Internet ein gemeinsames Zufallsbit erzeugen.

Problem: Wer zuletzt antwortet besitzt alle Informationen und kann gegebenenfalls seine Nachricht anpassen.

Lösung: Man braucht eine Bit-Commitment-Technik, also eine Hashfunktion $f : \{0,1\} \times M_1 \to M_2$, die bezüglich des ersten Arguments kollisionsfrei ist. Dann gehen A und B wie folgt vor:

1) A wählt ein zufälliges Element $(\varepsilon, m) \in \{0,1\} \times M_1$ und übermittelt $f(\varepsilon, m)$ an B.

2) B wählt ein zufälliges $\varepsilon' \in \{0,1\}$ und übermittelt es an A.

3) A sendet das Paar (ε, m), so daß B mit Hilfe von f prüfen kann welches ε von A gewählt wurde.

4) A und B berechnen nun $\varepsilon + \varepsilon' \pmod 2$. Dies verwenden sie als gemeinsames Zufallsbit.

Die Abbildung f kann wie folgt realisiert werden: Sei $n = pq$ ein Produkt zweier großer Primzahlen. Sei $y \in \{1, \ldots, n-1\}$ mit $\text{ggT}(n, y) = 1$ ein quadratischer Nichtrest modulo n, d.h. es gebe kein x mit $y = x^2 \pmod n$. Ferner gelte eine der folgenden Bedingungen:

(I) y ist quadratischer Rest $\pmod p$ und $\pmod q$.

(II) y ist quadratischer Nichtrest $\pmod p$ und $\pmod q$.

Jetzt definiere $f : \{0,1\} \times \{0,1,\ldots,N\} \to \{0,\ldots,n-1\}$, $(\varepsilon, m) \mapsto y^\varepsilon m^2 \pmod n$.

a) Für $\varepsilon = 0$ ist $y^\varepsilon m^2 \pmod n$ ein quadratischer Rest $\pmod n$. Für $\varepsilon = 1$ ist $y^\varepsilon m^2 \pmod n$ ein quadratischer Nichtrest $\pmod n$. Die Funktion f ist kollisionsfrei im ersten Argument.

b) Für eine Zahl mit der Eigenschaft (I) oder (II) ist kein effizienter Weg bekannt um festzustellen, ob sie ein quadratischer Rest $\pmod n$ ist oder nicht. Die Zahl $f(\varepsilon, m)$ besitzt Eigenschaft (I) oder (II). Also liegt eine Hashfunktion vor.

B Digitale Signaturen

3.3 Definition

Gegeben seien zwei Parteien A und B.

a) Verabreden A und B ein geheime Information (Passwort, PIN-Nummer) und kann sich A gegenüber B dadurch identifizieren, dass er diese nennt, so heißt ein diesbezügliches Protokoll ein Authentifikationsverfahren.

In diesem Fall besitzt B die geheime Information und kann sich eventuell als A ausgeben.

b) Ein Protokoll bei dem A gegenüber B seine Identität beweisen kann, ohne dass er B vertrauen muss, also ohne dass B sich als A ausgeben kann heißt Signaturverfahren.

3.4 Beispiele

a) Geheime Erkennungszeichen sind Authentifikationsverfahren.

b) Die Passworteingabe am Computer ist ein Authentifikationsverfahren.

c) Mit Hilfe eines vertrauenswürdigen Vermittlers ("Trust Center") kann man ein Signaturverfahren realisieren:

1. A und B haben jeweils einen Geheimschlüssel, der nur ihnen und dem Trust Center bekannt ist.
2. A verschlüsselt seine Nachricht und sendet diese an das Trust Center.
3. Das Trust Center entschlüsselt die Nachricht und verschlüsselt sie mit dem Schlüssel von B und sendet das Ergebnis sowie die von A verschlüsselt Nachricht an B.
4. B kann nun sicher sein, dass die Nachricht von A kommt, denn nur das Trust Center kennt beide Schlüssel.

B kann die Nachricht nicht nachträglich verändern, denn das Trust Center könnte die mit dem Schlüssel von A chiffrierte Version einfordern.

3.5 Beispiel (Das RSA Signaturverfahren)

Es soll eine signierte Nachricht von A an B übermittelt werden. Beide Partner haben ein RSA Verfahren (n_A, e_A, d_A) bzw. (n_B, e_B, d_B) zur Verfügung.

1) Die ursprüngliche Nachricht sei $x \in (\mathbb{Z}/_{n_A\mathbb{Z}})^N$. A berechnet den Wert $f(x)$ einer fest gewählten Hash-Funktion $f : (\mathbb{Z}/_{n_A\mathbb{Z}})^N \to \mathcal{C} = \mathbb{Z}/_{n_A\mathbb{Z}}$.

2) A berechnet $h = f(x)^{d_A} \pmod{n_A}$ und sendet $(x,h) \in (\mathbb{Z}/_{n_A\mathbb{Z}})^{N+1}$ verschlüsselt mittels e_B an B, d.h. A sendet den Geheimtext

$$x_1^{e_B} \pmod{n_B}, x_2^{e_B} \pmod{n_B}, \ldots, x_N^{e_B} \pmod{n_B}, h^{e_B} \pmod{n_B} \in (\mathbb{Z}/_{n_B\mathbb{Z}})^{N+1}$$

3) B entschlüsselt den Geheimtext mittels d_B und erhält wieder (x,h).

4) Nun berechnet B die Zahlen $f(x)$ und $h^{e_A} \pmod{n_A}$ und vergleicht sie. Sind sie gleich, so weise B, dass die Nachricht von A kommt.

Vorteile:

1) Dieses Signaturverfahren besitzt die gleiche Sicherheit wie das RSA-Kryptosystem.

2) Da (x,h) verschlüsselt versandt wurde, kann ein Mithörer weder die Nachricht lesen noch herausfinden wer die signiert.

3) A kann nachträglich nicht behaupten er habe die Nachricht nicht gesandt: Nur er kann das $f(x)$ mit d_A verschlüsseln.

Nachteile:

1) Die gesamte Nachricht muss mit RSA verschlüsselt werden $\rightsquigarrow$ sehr langsam.

3.6 Beispiel (Der Digitale Signatur-Algorithmus DSA)

1991 US National Institute of Standards and Technology (NIST) - "El Gamal Signaturverfahren". Aufgabe wie in 3.5.

1) A wählt eine große Primzahl q (≥ 160 Bits).

2) A wählt eine zweite Primzahl p mit $p \equiv q \pmod{1}$ (≥ 500 Bits).

3) Die Gruppe $(\mathbb{Z}/_{p\mathbb{Z}})^\times$ besitzt eine eindeutige zu $\mathbb{Z}/_{q\mathbb{Z}}$ isomorphe Untergruppe. A berechnet ein $g \in \mathbb{N}_+$ mit $\langle\overline{g}\rangle \subseteq (\mathbb{Z}/_{p\mathbb{Z}})^\times$, so dass genau aus q Elementen besteht, d.h. $\operatorname{ord}(\overline{g}) = q$. (Dies geschieht wie folgt: Berechne $g_0^{\frac{p-1}{q}} \pmod{p}$ für Zufallszahlen g_0 solange bis das Ergebnis $\neq 1$ ist.)

4) A wählt als Geheimschlüssel eine Zufallszahl $x \in \{1,\ldots,q-1\}$ und berechnet den öffentlichen Schlüssel $y = g^x \pmod p$.

5) Mit einer Hashfunktion $f : \mathcal{P} \to (\mathbb{Z}/_{q\mathbb{Z}})^\times$ wandelt A eine Klartexteinheit m in ein $h = f(m) \in \{1,\ldots,q-1\}$ um. Dieses h wird an B übermittelt.

6) A wählt eine Zufallszahl $k \in \{1,\ldots,q-1\}$ und berechnet $g^k \pmod p$. Das Ergebnis wird mit Rest durch q geteilt und liefert einen $r \in \{0,\ldots,q-1\}$.

7) Mit Hilfe des erweiterten Euklidischen Algorithmus findet A eine Zahl $s \in \{0,\ldots,q-1\}$ mit $sk \equiv h + xr \pmod q$.

8) A übermittelt das Paar $(r,s) \in \{0,\ldots,q-1\}^2$ als Signatur.

9) Um die Signatur zu prüfen berechnet B die Zahlen $u_1 = s^{-1}h \pmod q$ und $u_2 = s^{-1}r \pmod q$. Dann bestimmt B die Zahl $g^{u_1}y^{u_2} \pmod p$ und teilt das Ergebnis mit Rest durch q. Ist der Rest r, so akzeptiert B die Signatur.

Behauptung: Ist der letzte Divisionsrest gleich r, so weiß B, dass die Nachricht von A kommt.

Beweis: Es gilt $g^q = 1 \pmod p$. Also folgt

$$\begin{aligned} g^{u_1}y^{u_2} &= g^{s^{-1}h}(g^x)^{s^{-1}r} \\ &= g^{s^{-1}(h+xr)} \\ &= g^k \pmod p \end{aligned}$$

und damit ist die Restklasse $\pmod q$ genau r. Die Zahl s kann nur von A berechnet werden: Das Paar (r,s) kann man nur berechnen, wenn man (r,k) kennt oder wenn man aus $h = xr - sk \pmod q$ und aus $r = g^k \pmod q$ die Zahl k bestimmen kann.

Vorteile:

1) Die Signatur ist vergleichsweise kurz (2×160 Bits)

2) Die Sicherheit beruht auf der Schwierigkeit des diskreten Logarithmus.

3) Die Nachricht kann im Klartext übermittelt werden.

Nachteil:

Man braucht nur diskrete Logarithmen in einer vergleichsweise kleineren (Unter)gruppe $\langle g\rangle \subseteq (\mathbb{Z}/_{p\mathbb{Z}})^\times$ zu finden.

3.7 Beispiel (Authentifikation mit Chipkarten)

Eine Chipkarte habe folgende Eigenschaften:

1) Sie muss eine eingegebene Geheimzahl auf Gültigkeit prüfen.

2) Sie muss eine Einweg-Funktion f ausführen.

3) Sie muss zwei geheime Schlüssel $e_A, \tilde{e}_A$ speichern und vor unbefugten schützen.

4) Sie muss Kommunikationsdaten speichern können.

Der Kunde A möchte bei einem Händler H einkaufen. Der Händler soll mit der Bank B des Kunden abrechnen.

1) Die Bank erzeugt den Globalschlüssel d_B der unbedingt vor dem Kunden geheim bleiben muss. Die Bank erzeugt auch einen geheimen Kundenschlüssel $\tilde{d}_B$ (der ebenfalls nur der Bank bekannt ist).

2) Aus den Kundendaten k_A werden zwei Geheimschlüssel $e_A = f(k_A, d_B)$ und $\tilde{e}_A = f\left(k_A, \tilde{d}_A\right)$ erzeugt und in der Chipkarte abgespeichert.

3) Identifikation des Kunden gegenüber der Karte: Der Kunde steckt die Karte in den Kartenleser und gibt die Geheimzahl ein. Die Karte prüft die Geheimzahl.

4) Authentifizierung der Karte gegenüber dem Händler:

a) H liest die Kundendaten k_A aus der Karte aus.

b) H berechnet den Hashwert $e_A = f(k_A, d_B)$. Der Globalschlüssel d_B ist dabei im Kartenlesegerät gespeichert, darf aber nicht auslesbar sein.

c) H wählt eine Zufallszahl z.

d) Die Chipkarte und H berechnen jeweils $f(z, e_A)$.

e) Die Chipkarte sendet ihr Ergebnis an H und diese vergleicht es mit seinem Ergebnis.

5) Authentifizierung der Buchungsdaten:

a) Die Buchungsdaten D werden vom Kartenleser and die Karte geschickt.

b) Die Chipkarte berechnet $m = f(D, \tilde{e}_A)$. m heißt MAC ("message authentification code") und sendet ihn an H.

c) Der Händler sendet das Paar (D, m) an die Bank.

6) Die Bank prüft die Korrektheit der Buchungsdaten, indem sie aus D ebenfalls $f(D,\tilde{e}_A)$ bestimmt und mit m vergleicht.

Vorteile:

1) Der Händler kann die Buchungsdaten nicht fälschen, da er $\tilde{e}_A$ nicht kennt.

2) Der Kunde kann seine Identität nicht fälschen, da er das e_A nicht kennt.

3) Der Händler hat die Garantie, dass die Bank zahlt, falls das m stimmt. Im Zweifelsfall müsste die Bank die Zahl $\tilde{d}_A$ preisgeben.

Nachteile:

1) Verschiedene Schlüssel $(e_A,\tilde{e}_A,d_B)$ dürfen nicht auslesbar sein.

2) Elektronische und mechanische Angriffe auf die Chipkarte sind möglich.

C Weitere Authentifikationsverfahren

3.8 Beispiel (Passwörter am Computer)

Ziel: Ein Anwender soll sich einem Computer gegenüber authentifizieren.

Protokoll von Needham (1968): Man braucht eine Einweg-Funktion $f : \mathcal{P} \to \mathcal{C}$.

1) Der Benutzer tippt sein Passwort $P \in \mathcal{P}$ ein, z.B. $\mathcal{P} = \{0,1,\ldots,9,A,\ldots,Z,a,\ldots,z,\ldots\}^8$.

2) Der Computer berechnet $f(P)$ und vergleicht das Ergebnis mit dem Eintrag in einer Datei, die die verschlüsselten Passwörter aller Benutzer enthält (“Einweg-Chiffrierung”).

Kryptoanalyse:

1) Wählen die Benutzer ihre Passwörter schlecht, so kann der Angreifer alle Möglichkeiten durchprobieren.

2) Die Übertragung der Passwörter erfolgt öffentlich. Ein einmal abgehörtes Passwort kann während seiner Lebensdauer missbraucht werden. (Vermieden bei Homebanking durch die TAN).

3) Die zur Authentifikation eines Benutzers versandten Nachtichten sind immer gleich (“man in the middle-Angriff” möglich).

Problem: Wird $f(P)$ von C abgehört, so kann sich Cals A ausgeben.

3.9 Beispiel (Das Wechselcodeverfahren)

Ziel: A soll sich gegenüber B authentifizieren. Bei festem Geheimnis sollen die übermittelten Nachrichten aber möglichst variable und unvorhersehbar sein.

Verfahren: Man braucht eine Familie von Einwegfunktionen $f_k : \mathcal{P} = \mathbb{N} \to \mathcal{C}$ für $k \in K$.

a) Beide Parteien einigen sich auf einen gemeinsamen geheimen Schlüssel k und einen Anfangszählerstand $z \in \mathbb{N}$.

b) Beim ersten Authentifizierungsvorgang bildet A $c_0 = f_k(z)$ und überträgt diesen.

c) B überprüft, ob das empfangene c_0 mit $f_k(z)$ übereinstimmt.

d) Beim zweiten Authentifizierungsvorgang sendet A den Wert $c_1 = f_k(z+1)$.

Kryptoanalyse: Der Angreifer kann versuchen, sich als B auszugeben und so c_{i+1}von A zu erhalten.

Verteidigung: Der Zähler z sollte das aktuelle Datum und die aktuelle Uhrzeit enthalten und nur kurzzeitig gültig sein.

Variante: Es gibt ein Wechselcodeverfahren, bei dem B das Geheimnis von A nicht zu kennen braucht.:

a) Aund B einigen sich auf eine Einwegfunktion $f : \mathbb{N} \to \mathbb{N}$.

b) A wählt einen Startwert z_0 und schätzt ab wie of er das Verfahren benutzen wird, z.B. $n = 100$ mal.

c) A berechne $c_0 = f(z_0),\ldots,c_{99} = f(c_{98}),c_{100} = f(c_{99})$.

d) A übermittelt c_{100} an B und teilt B mit, dass er derjenige ist, der $c_0,\ldots,c_{99}$kennt.

e) A authentifiziert sich beim i-ten mal mit c_{100-i}. B vergleicht $f^i(c_{100})$ mit c_{100}.

3.10 Beispiel (challange-and-response Verfahren)

Ziel: Es soll ein Wechselverfahren entwickelt werden, bei dem keine Authentifikationsnachrichten “vorproduziert” werden.

Idee: B stellt A eine unvorhersehbare Frage, die Amit Hilfe seines geheimen Wissens beantworten muss.

Verfahren:

a) Beide Parteien einigen sich auf eine Familie von Einwegfunktionen $f_k : \mathbb{N} \to C$ und einen geheimen Schlüssel k.

b) B sendet eine Zufallszahl z (“challange”) an A.

c) A berechnet $s = f_k(z)$ (“sigend response”) und sendet sie an B.

d) B prüft, ob $s = f_k(z)$ gilt.

Anstelle von f_k kann man auch ein Signaturverfahren verwenden, so dass B das Geheimnis von A nicht zu kennen braucht.

3.11 Beispiel (Das GSM-Mobilfunknetz)

GSM steht für Groupe special mobile

Aufgaben: Schutz der Funktstrecke gegen unerlaubtes telefonieren und illegales abhören.

Verfahren:

1) Authentifikation mit einem challange-and-response Verfahren:

a) Das Mobilfunktsystem erzeugt eine Zufallszahl z.

b) Das Handy verwendet einen individuellen Schlüssel k und einen Algorithmus $A3$ um die Antwort $s = A3(k,z)$ zu erzeugen.

c) Das Handy sendet s an das System zurück.

d) Das System hat inzwischen k in einer Datenbank gelesen und vergleicht s mit dem selbstberechneten $A3(k,z)$.

2) Sowohl im Handy als auch im System wird ein Algorithmus $A8$ auf (k,z) angewandt und ein Sitzungsschlüssel $K = A8(k,z)$ berechnet.

3) Die digitalen Daten des Telefonats werden nun mit einem private-key Algorithmus $A5$ mit Schlüssel K übertragen. Es handelt sich um eine Stromchiffrierung a la Vignere mit Pseudozufallsgenerator.

Variante: In einem “fremden” Mobilfunktnetz (z.B. im Ausland) sind eventuell $A3$ und $A8$ anders implementiert. Nur $A5$ ist standardisiert. In diesem Fall schickt das Heimnetz einige vorbereitete Tripel (z,s,K) an das fremde Netz, da damit mit dem Handy nach obigem Protokoll kommuniziert werden kann.

D. Schlüsselmanagement

Ziel: Zwischen zwei Parteien A und B soll ein geheimer Schlüssel vereinbart werden, so dass dann die Verfahren der Kryptographie verwendet werden können. Dabei soll kein geheimer Kanal zur Verfügung stehen.

3.12 Beispiel (Diffie-Hellman-Schlüsselvereinbarung)

1) Die beiden Parteien vereinbaren eine große Primzahl p und eine Zahl $g \in \mathbb{N}$.

2) A wählt eine geheime Zahl $a \in \mathbb{N}$ und B analog ein Zahl $b \in \mathbb{N}$.

3) A berechnet $\alpha = g^a \pmod p$, B berechnet $\beta = g^b \pmod p$.

4) Die beiden Zahlen α, β werden (öffentlich) ausgetauscht.

5) A berechnet $k_A = \beta^\alpha \pmod p$ und B berechnet $k_B = \alpha^\beta \pmod p$. Dies ist der gemeinsame geheime Schlüssel k, denn

$$k_A = \beta^\alpha = g^{ba} = g^{ab} = \alpha^\beta = k_B$$

Kryptoanalyse:

a) Ein Angreifer kann durch zuhören die Werte α und β verschaffen, ebenso p und g. Um sich den Geheimschlüssel zu verschaffen müsste er aber das Diffie-Hellman-Problem lösen: Gegeben sei eine Primzahl p und die Zahlen g, $g^a \pmod p$ und $g^b \pmod p$. Finde

$$g^{ab} \pmod p$$

Es wird vermutet, dass das Diffie-Hellman-Problem und das Problem des diskreten Logarithmus äquivalent sind.

b) Beide Partner müssen etwa gleichzeitig “online” sein.

c) Es ist nicht klar, ob der tatsächliche Kommunikationspartner auch der beabsichtigte ist. Jemand könnte sich z.B. gegenüber B als A und gegenüber A als B ausgeben. In diesem Fall spricht man von einem man-in-the-middle Angriff. Es ist also gleichzeitig ein Signaturverfahren einzusetzen.

3.13 Beispiel (Das Breitmaulfrosch-Protokoll)

Ziel: Mit Hilfe eines Trustcenters/Trusted-Third-Party (TTP) soll ein Sitzungsschlüssel zwischen A und B vereinbart werden. Das Protokoll soll garantieren, dass alle gesendeten Nachtichten frisch sind und vorher nie gesendet wurden.

1) A einigt sich mit TTP auf einen gemeinsamen Geheimschlüssel k_{AT}, ebenso einigen sich B und TTP auch k_{BT}.

2) A sendet an TTP eine Nachricht mit folgendem Inhalt:

- den Namen von A, damit TTP den Schlüssel k_{AT} findet.
- einen Sitzungsschlüssel k_{AB}, einen Zeitstempel t_A und den Namen von B, alle mit k_{AT} verschlüsselt.

3) TTP entschlüsselt diese Nachricht und sendet eine Nachricht, die er mit k_{BT} verschlüsselt an B mit dem Inhalt

- den Namen von A
- einem neuen Zeitstempel t_T
- dem Sitzungsschlüssel k_{AB}

4) B entschlüsselt die Nachricht und startet die Kommunikation mit A mittels k_{AB}.

Vorteile: Durch die Zeitstempel ist eine Manipulation erschwert.

Nachteil: Nach dem Start der Kommunikation müssen sich A und $b$gegenseitig authentifizieren.

3.14 Beispiel (Das Otway-Rees-Protokoll)

Ziel: Wie beim Breitmaulfrosch-Protokoll. Jedoch soll eine gegenseitige Authentifikation von A und B eingeschlossen sein.

1) A erzeugt eine verschlüsselte Nachricht mittels k_{AT}, den nur A und TTP kennen, die folgendes enthält:

- einen Zeitstempel t_A
- Namen und Adressen von A und B

2) A sendet diese Nachricht an B.

3) B erzeugt eine verschlüsselte Nachricht mittels k_{BT}, die folgendes enthält:

- einen Zeitstempel t_B
- Namen und Adressen von A und B

4) B sendet beide verschlüsselten Nachrichten und die Namen von A und B an TTP.

5) TTP entschlüsselt die Nachrichten und erzeugt einen Sitzungsschlüssel k_{AB} und zwei verschlüsselte Nachrichten:

- Die eine ist mit k_{AT} verschlüsselt und enthält k_{AB} sowie die Zeitstempel t_T und t_A.
- Die andere ist analog aufgebaut und mit k_{BT} verschlüsselt.

6) TTP schickt die Nachricht an B.

7) B entschlüsselt seine Nachricht und schickt die andere an A.

8) A entschlüsselt seine Nachricht.

Vorteile:

- Nur B muß mit TTP in Verbindung treten.
- Man benötigt kein anschließendes Authentifikationsverfahren.

3.15 Beispiel (Das Needham-Schroeder Protokoll)

Ziel: A und B sollen sich mit Hilfe von TTP wechselseitig authentifizieren und einen Sitzungsschlüssel austauschen. Nur A, der die Kommunikation möchte, soll mit TTP in Verbindung treten.

Verfahren: Beide Parteien sollen Schlüssel k_{AT} bzw. k_{BT} besitzen, die jeweils nur ihnen und TTP bekannt sind.

1) A sendet an TTP die Namen und Adressen von A und B sowie einen Zeitstempel t_A.

2) TP antwortet A mit einer Nachricht, die mit k_{AT} verschlüsselt ist und folgendes enthält:

- den Sitzungsschlüssel k_{AB}
- den Zeitstempel t_A und einen Zeitstempel t_T.
- eine mit k_{BT} verschlüsselte Nachricht mit k_{AB} und Name und Adresse von A.

3) A entschlüsselt die Nachricht und schickt den für B bestimmten Teil an B.

4) B entschlüsselt die Nachricht mit k_{BT}. Er kennt nun den Sitzungsschlüssel und, dass A mit ihm kommunizieren möchte. Deshalb leitet er ein challange-and-response Verfahren ein.

5) B schickt eine mit k_{AB} verschlüsselte Nachricht an A, die einen Zeitstempel t_B enthält.

6) A antwortet mit einer Nachricht, die mit k_{AB} verschlüsselt ist und eine Funktion $f(t_B)$, z.B: $f(t_B) = t_B - 1$.

Kryptoanalyse:

1) B kann nicht prüfen, ob das Kryptosystem, dass TTP erhält, frisch ist. Ein Angreifer $\tilde{A}$ könnte längere Zeit, etwa einige Monate, versuchen k_{AB} zu erhalten. Dann leitet $\tilde{A}$ die verschlüsselte Nachricht $k_{BT}(A, k_{AB})$ an.

2) Noch schlimmer ist 5, wenn $\tilde{A}$ den Schlüssel k_{AB} kennt. Dann kann er sich von TTP viele gültige Schlüssel k_{AB} besorgen. Selbst wenn A den Missbrauch bemerkt, kann er diese Schlüssel nicht mehr ungültig machen.

Ziel: Kann man auch vertrauliche Nachrichten austauschen, ohne vorher Schlüssel zu vereinbaren?

3.16 Beispiel (Shamir no-key Protokoll)

Auch als Massey-Omara-Kryptosystem bekannt.

Ziel: A soll eine geheime Nachricht $s \in \mathbb{N}_+$ an B schicken.

1) Bei Parteien einigen sich (öffentlich) auf eine große Primzahl $p > s$.

2) A erzeugt ein Paar $(a, a') \in \mathbb{Z}^2$ mit $aa' \equiv 1 \pmod{p-1}$

3) B erzeugt ein Paar $(b, b') \in \mathbb{Z}^2$ mit $bb' \equiv 1 \pmod{p-1}$

4) A sendet $x = s^a \pmod{p}$ an B.

5) B sendet $y = x^b \pmod{p}$ an A.

6) A sendet $z = y^{a'} \pmod{p}$ an B.

7) B berechnet $z^{b'} = y^{a'b'} = x^{a'bb'} = s^{aa'bb'} \equiv s \pmod{p}$.

Kryptoanalyse:

1) Dieses Verfahren muss unbedingt von einem guten Signaturverfahren begleitet werden, sonst kann sich C als B ausgeben.

2) Kann ein Angreifer das diskrete-log Problem lösen, so kann er durch Mithören von x und $y = x^b$ b bestimmen und damit aus z die Nachricht s, da er b' berechnen kann. Er könnte auch aus $x = s^a \pmod{p}$ zur Basis $y = s^{ab}$ den Log finden, d.h. d mit $y^d = x \pmod{p} \Rightarrow d \equiv b' \pmod{p-1}$. Daher kann der Angreifer s durch $z^d \equiv z^{b'} \equiv s \pmod{p}$ berechnen. Die Sicherheit beruht auf dem diskreten-log Problem.

E Zero-Knowledge Beweise

3.17 Beispiel (Lösungsformel für Gleichungen 3. Grades)

Im Jahr 1535 fand Nicolo Tartaglia eine Lösungsformel für Gleichungen $x^3 + ax^2 + bx + c = 0$. Er konnte auf Grund seiner Herkunft keinen akademischen Grad erlangen und das Resultat nicht publizieren. Um sich die Priorität der Erfindung zu sichern ging er einen Wettstreit ein:

1) Der Mathematiker A. Fior legte ihm 30 Gleichungen 3. Grades vor, deren Lösungen nur Fior kannte.

2) Tartaglia löste mit seiner Formel die 30 Aufgaben und sandte die Lösungen an Fior.

3) Jedermann konnte die Korrektheit seiner Lösungen prüfen, ohne Informationen über die Formel zu erhalten.

3.18 Definition

Ein Protokoll zur Authentifikation von A gegenüber B habe die folgenden Eigenschaften:

a) B muss das Geheimnis von A vorher nicht kennen.

b) B erfährt während des Ablaufs der Protokolls nichts über das Geheimnis von A. Er erhält nachweislich keinerlei Informationen.

c) B kann sich (mit beliebig hoher Wahrscheinlichkeit) davon überzeugen, dass A das Geheimnis kennt (und somit als Besitzer des Geheimnis authentifiziert ist).

In diesem Fall heißt das Protokoll ein zero-knowledge Protokoll oder ein zero-knowledge Beweis.

3.19 Beispiel (Die magische Tür)

Abbildung 6: FIXME: Skizze einer magischen Tür

Die magische Tür ist nur mit Passwort zu öffnen.

Ziel: A soll gegenüber B beweisen, dass er das Passwort kennt.

1) A betritt den Vorraum und schließt die Außentür.

2) A geht zufällig durch Tür 1 oder 2 und schließt sie.

3) B betritt den Vorraum und ruft zufällig “Tür 1” oder “Tür 2”.

4) Ist A zufällig hinter der richtigen Tür, so kommt er hinaus.

5) Ist A hinter der falschen Tür, so geht er durch die magische Tür und kommt auf der richtigen Seite heraus.

6) Die Schritte 1-5 werden n-mal wiederholt, solange bis $\frac{1}{2^n}$ kleiner als die gewünschte Fehlerwahrscheinlichkeit ist.

Beweis (der zero-knowledge Eigenschaft): B kann alle Informationen, die er während des Ablaufs erhält mit einer Videokamera aufzeichnen. Wenn ein Simulator $\tilde{B}$ ohne Kenntnis des Passwortes einen Videofilm herstellen kann, der mit dem von B identisch ist, so besitzt das Protokoll die zero-knowledge Eigenschaft. Dazu braucht $\tilde{B}$ eine Testperson $\tilde{A}$. Dann versucht $\tilde{B}$ die Aufforderung “Tür 1” oder “Tür 2” von B zu erraten.

Ist $\tilde{A}$ zufällig im richtigen Raum, wird die Szene aufgenommen, andernfalls nicht. Nach ca. $2n$ Versuchen besitzt $\tilde{B}$ das gewünschte Video.

3.20 Beispiel (Das Feige-Fiat-Shamir Protokoll)

Die Korrektheit beruht darauf, dass es für $n \gg 0$ schwer ist in $(\mathbb{Z}/_{n\mathbb{Z}})^\times$ Quadratwurzeln zu finden.

Verfahren:

1) Schlüsselerzeugung: A wählt zwei große Primzahlen p und q und berechnet $pq = n$. n ist öffentlich, p und q geheim.

2) A wählt $s \in \{1, \ldots, n-1\}$ zufällig und berechnet $v = s^2 \pmod n$. v ist öffentlich, sist geheim.

3) Anwendung: A wählt zufällig $r \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$ und sendet $x = r^2 \pmod n$ an B.

4) B wählt $\varepsilon \in \{0,1\}$ und sendest es an A.

5) Ist $\varepsilon = 0$, so sendet A die Zahl $y = r$ an B. Ist $\varepsilon = 1$, so sendet A die Zahl $y = rs \pmod n$ an B.

6) Im Fall $\varepsilon = 0$ prüft B, ob $y^2 = x \pmod n$ gilt. Im Fall $\varepsilon = 1$ prüft B, ob $y^2 = xv \pmod n$ gilt.

7) Das Verfahren wird wiederholt, bis B sicher ist, dass A das Geheimnis s kennt.

Korrektheit:

a) Wenn A das Geheimnis s kennt, so gilt:

$$y^2 = (rs^\varepsilon)^2 = r^2 s^{2\varepsilon} = r^2 v^\varepsilon = xv^\varepsilon \pmod n$$

b) Wenn $\tilde{A}$ das Geheimnis s nicht kennt, so kann er höchstens eine der beiden Fragen beantworten. Wenn er beide mit y_0 bzw. y_1 beantwortet, so gilt

$$y_0^2 = x \pmod n \quad \text{und} \quad y_1^2 = xv \pmod n$$

und damit folgt $\left(\frac{y_1}{y_0}\right)^2 = v \pmod n$. Daher ist $\frac{y_1}{y_0} \in \{-s, s\}$ ist $\tilde{A}$ bekannt.

c) $\tilde{A}$ kann mit 50% Erfolgswahrscheinlichkeit betrügen, denn wenn die Frage ε richtig vermutet, kann er $x = r^2 v^{-\varepsilon} \pmod n$ berechnen und $y = r$ senden. Die Überprüfung von B ergibt dann

$$xv^{\varepsilon} = r^2 = y^2$$

Zero-knowledge Eigenschaft: Ein Simulator $\tilde{A}$ kann das Verfahren wie folgt nachstellen:

1) $\tilde{A}$ wählt $\tilde{\varepsilon} \in \{0,1\}$ und berechnet $x = r^2 v^{-\tilde{\varepsilon}} \pmod n$ und sendet x an B.

2) B antwortet mit $\varepsilon \in \{0,1\}$.

3) Ist $\varepsilon = \tilde{\varepsilon}$, so sendet $\tilde{A}$ die Nachricht $y = r$ an B. Die Überprüfung durch B ist dann erfolgreich.

4) Ist $\varepsilon \neq \tilde{\varepsilon}$ so werden die Nachrichten des Simulators gelöscht und das Verfahren wiederholt.

Fazit: Sowohl im Originalprotokoll als auch in der Simulation werde zufällige Tripel (x, ε, y) erzeugt mit $xv^{\varepsilon} = y \pmod n$ und abgespeichert. Die beiden Protokolle sind für Außenstehende nicht zu unterscheiden.

F. Secret Sharing

Ziel: Eine geheime Information soll auf mehrere Parteien aufgeteilt werden, so dass keine mir seinem Teil etwas anfangen kann.

Beispiel: Ein Banktresor, der nur von drei Direktoren gleichzeitig geöffnet werden kann.

Problem: Einer der beteiligten "verliert" seinen Schlüssel oder stirbt.

3.21 Definition

Ein (n,t)-secret-sharing Protokoll (oder ein threshold-Verfahren) ist ein Protokoll bei dem ein Geheimnis s in eine Anzahl von n Teilgeheimnissen $s_1, \ldots, s_n$ aufgeteilt wird, so dass für eine Schwelle von t gilt:

a) Aus je t oder mehr Teilgeheimnissen kann s rekonstruiert werden.

b) Aus weniger als t Teilgeheimnissen kann man s nicht berechnen oder nur mir einer geringen Wahrscheinlichkeit erraten.

3.22 Beispiel (Ein$(n,2)$-secret-sharing Protokoll)

1) Man wählt eine zufällige Gerade in $\mathbb{Q}^2$, die die y-Achse in $(0,d)$ schneidet. Dabei sei $d \in \mathbb{Q}_+$ das Geheimnis.

2) Jedem der n Teilnehmer wird ein zufällig gewählter Punkt s der Gerade mitgeteilt.

Abbildung 7: FIXME: Skizze

Kein Teilnehmer kann nur aus seinem s_i die Gerade (bzw. d) ermitteln, aber je zwei Teilnehmer können es.

3.23 Beispiel (Ein (n,n)-secret-sharing Protokoll)

1) Man wählt einen genügend großen Körper $\mathbb{F}_q = \mathbb{Z}/_{p\mathbb{Z}}$ oder $\mathbb{Q}$. Nenne ihn K.

2) Das Geheimnis sei $s \in K$. Wähle ein Polynom

$$f = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1 x + s \in K[x]$$

mit zufällig gewählten $a_1, \ldots, a_{m-1} \in K$.

3) Jedem der n Teilnehmer wird ein Punkt $(b_i, f(b_i)) \in K^2$ mit $b_i \in K$ zufällig mitgeteilt.

4) Treffen sich $\geq m$ Teilnehmer, so können sie das Polynom mit Lagrange-Interpolation wiederherstellen:

$$f(x) = \sum_{i=1}^{m} \frac{\prod_{j \neq i} (x - b_j)}{\prod_{j \neq i} (b_i - b_j)} f(b_i)$$

5) Weniger als m Teilnehmer können das Polynom nicht rekonstruieren, sondern höchstens mit einer Wahrscheinlichkeit $< \frac{1}{\#k}$ erraten.

3.24 Beispiel (Kompliziertes secret-sharing Protokoll)

Man kann mit Hilfe komplizierterer geometrischer Objekte auch kompliziertere secret-sharing Aufgaben lösen, z.B. soll sich ein Firmentresor nur öffnen lassen, wenn folgende Personen anwesend sind:

- zwei Direktoren
- drei Vizepräsidenten
- ein Direktor
- zwei Vizedirektoren

Verfahren:
1) Wähle einen genügend großen Körper $K = \mathbb{Z}/_{p\mathbb{Z}}$ oder $K = \mathbb{Q}$.
2) Im Raum K^3 wähle einen Punkt $(0,0,s)$ auf der z-Achse. Das Geheimnis sei s.
3) Wähle zufällig eine Ebene E durch s, die die z-Achse nicht enthält. Gleichung: $a_1x + a_2y + z = s$.
4) Wähle in E eine Gerade G durch den Punkt $(0,0,s)$.
5) Wähle auf G Punkte $D_1, D_2, \ldots$, die den Direktoren zugeteilt werden.
6) Wähle in E einen Kreis C durch den Punkt $(0,0,s)$.
7) Wähle auf C Punkte $V_1, V_2, \ldots$, die den Vizedirektoren zugeteilt werden. Dabei muß jeweils $\overline{V_iV_j} \cap G \neq D_k$ für alle i, j, k sein.
Dann sind die gewünschten Bedingungen erfüllt, denn:
a) Je zwei Direktoren können die Gerade G berechnen und damit $\{(0,0,s)\} = G \cap z$-Achse.
b) Je drei Vizedirektoren können den Kreis C berechnen und damit $\{(0,0,s)\} = C \cap z$-Achse bzw. können Sie einfach E berechnen.
c) Je ein Direktor und zwei Vizedirektor können die Ebene E berechnen und damit $\{(0,0,s)\} = E \cap z$-Achse.
Anwendung: Z.B. sind die amerikanischen Nuklearwaffen mit einem secret-sharing Protokoll gesichert. Nur wenn die "richtigen" Personen ihre Teilgeheimnisse kombinieren, entsteht das echte Geheimnis. Dieses wird dann mit einer Einwegfunktion verschlüsselt und mit einer gespeicherten Funktion verglichen.

G. Kryptoanalyse von Protokollen

3.25 Beispiel

Die in einem Protokoll verwendeten Verfahren sind immer nur so sicher, wie ihre Implementation erlaubt. Z.B. konnten 1995 zwei Studenten die SSL-Verschlüsselung des Netscape-Browsers wie folgt knacken:

- Das Protokoll verwendete einen Pseudozufallsgenerator
- Zur Initialisierung wurden die Systemzeit und zwei Prozess-IDs des Clients verwendet.
- Die Prozess-IDs sind bei einem multi-user System abfragbar.
- Die Systemzeit beim Start der Verbindung läßt sich mit einer gewissen Spannbreite abschätzen.

Daher müssen statt 10^{18} verschiedene SSL-Schlüssel nur wenige tausend durchprobiert werden.

3.26 Beispiel (Die Impersonations-Attacke)

Ein Betrüger $\tilde{A}$ versucht sich als Person A auszugeben, z.B. ist dies möglich, wenn eine TTP verwendet wird, die öffentliche Schlüssel verwendet, so dass jeder entsprechende Nachrichten generieren kann.
Abhilfe: Jedem Teilnehmer soll von der TTP am Anfang eine eindeutige geheime Information zugeordnet werden.

3.27 Beispiel (Replay-Attacke)

Der Betrüger schleust die Nachricht, die bereits einmal gesendet wurde, erneut in das System ein. Z.B. könnte ein Händler einen Überweisungsauftrag einfach mehrmals in der Bank einreichen.
Abhilfe: Alle nachrichten müssen mit einem Zeitstempel versehen sein. Gibt es keine synchronisierten Uhren, so soll man "Einmalwerte" verwenden. Besonders Passwortverfahren sind anfällig gegenüber Replay-Attacken. Passwörter sollten nur endliche Lebensdauer haben.

3.28 Beispiel (Denial-of-service-Attacke)

Wie bei der Replay-Attacke werden Datenpackte wiederholt in das System eingespeist. Der Empfänger erkennt zwar nach einiger Zeit ihre Ungültigkeit, inzwischen kann er aber nicht mehr seine eigentliche Aufgabe nachkommen, z.B. könnte das System abstürzen.

Abhilfe:

- leicht verifizierbare Zeitstempel einbauen.
- Eine Wiederholung einer gewissen Aktion ist erst nach einer bestimmten Zeit erlaubt (“time out”), z.B. beim Abruf von Informationen.

3.29 Beispiel (Die Man-in-the-middle-Attacke)

Der Angreifer fängt die Nachrichten der Partei *A* ab und sendet seine eigenen Nachrichten an *B*. Ebenso verfährt er in umgekehrter Richtung, z.B. beim Diffie-Hellman Schlüsselaustausch bemerken die beiden Kommunikationspartner dies nicht, weil sie glauben, mit dem jeweils anderen einen Schlüssel vereinbart zu haben.

Abhilfe:

- Varianten der sogenannten Interlock-Protokolle verwenden
- Austausch von Schlüsseln auf zwei oder mehr Wegen.
- Verwendung von Schlüsselzertifikaten

3.30 Beispiel (Der Schachgroßmeister-Angriff)

Wenn ein Schachgroßmeister simultan abwechselnd mit Weiß und Schwarz spielt, kann er in beiden Partien jeweils die Züge der Gegner kopieren und damit mindestens einen Sieg oder zwei Remis erzielen.

No-Key-Protokolle:

1) *A* legt die Nachricht *s* in eine Kiste und verschließt diese mit einem Vorhängeschloss, zu dem nur *A* einen Schlüssel besitzt. *A* schickt die Kiste an *B*.

2) *B* hängt sein eigenes Vorhängeschloss an die Kiste und schickt diese zurück an *A*.

3) *A* entfernt sein Vorhängeschloss und schickt die Kiste zurück an *B*.

4) *B* entfernt sein Schloss, öffnet die Kiste und liest *s*.

Kryptographisches Beispiel: Bei einem no-key Protokoll schiebt sich der Angreifer *X* zwischen *A* und *B*, ohne dass dies bemerkt wird. *C* gibt sich *A* gegenüber als *B* aus und kommuniziert mit *A*. *X* empfängt die Kiste von *A* und hängt sein Schloss daran, schickt die Kiste zurück an *A*, *A* entfernt das Schloss und *X* kann die Nachricht dann lesen.

Abhilfe: no-key Protokolle müssen signiert werden.

3.31 Beispiel (“Unfaire Attacken”)

a) Der Timing-Angriff beruht darauf, dass Entschlüsselungen je nach Beschaffenheit des Schlüssels unterschiedlich lange dauern können, z.B. bei RSA.

b) Der Elektromagnetische Angriff misst die Strahlungen, die ein Kryptochip während seiner Arbeit aussendet. Aus dem elektromagnetischen Muster kann manauf die verwendeten Rechenschritte schließen.

c) Beim Zerstörungs-Angriff wird auf elektronischem oder mechanischem Weg versuch, einen Kryptochip zu fehlerhaftem Verhalten zu bringen und aus seiner Reaktion auf den gespeicherten Schlüssel zu schließen.

4 Elliptische Kryptosysteme

A. Mathematische Grundlagen

Im folgenden sei K ein Körper. Die Zahl $\text{char}(K) = \begin{cases} p & \text{falls } \min\left\{ i \mid \underbrace{1+\ldots+1}_{i\text{mal}} = 0 \right\} = p < \infty \\ 0 & \text{sonst} \end{cases}$ heißt die Charakteristik von K.

4.1 Definition

Gegeben sei eine Gleichung der Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}$$

mit $a_1, a_2, \ldots, a_6 \in K$. Die Menge der Punkte $(x,y) \in K^2$ die diese Gleichung erfüllen heißt eine kubische Kurve über K.

4.2 Satz

Gilt $\text{char}(K) \neq \{2,3\}$ so gibt es eine Koordinatentransformation $x \mapsto \alpha_1 x + \alpha_2 y + \alpha_3$ und $y \mapsto \beta_1 + \beta_2 y + \beta_3$ die die Gleichung (FIXME 1) in folgende Gestalt überführt:

$$y^2 = x^3 + ax + b$$

mit $a, b \in K$.

Beweis: Vergleiche Übungsaufgabe. □

Im folgenden gelte stets $\text{char}(K) \notin \{2,3\}$.

4.3 Definition

Eine kubische Kurve $y^2 = x^3 + ax + b$ heißt eine elliptische Kurve, wenn das Polynom $x^3 + ax + b$ keine mehrfache Nullstellen hat. Eine elliptische Kurve wird auch mit $E(K)$ bezeichnet.

4.4 Bemerkung

a) Ist $E(K)$ eine elliptische Kurve über K und $L \supseteq K$ ein Erweiterungskörper, so definiert die Gleichung $y^2 = x^3 + ax + b$ ein elliptische Kurve $E(L)$, die $E(K)$ enthält.

b) Die Diskriminante eines Polynoms $f = (x - x_1) \cdot \ldots \cdot (x - x_n)$ ist definiert als

$$\text{discr}(f) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

in unserem Fall $x^3 + ax + b = (x - x_1)(x - x_2)(x - x_3)$ ergibt sich genau dann eine elliptische Kurve, wenn die Diskriminante $-4a^3 - 27b^2$ nicht verschwindet.

c) Über $K = \mathbb{C}$ ist eine kubische Kurve genau dann elliptisch, wenn sie nicht singulär ist.

Abbildung 8: FIXME: Singularitäten kubischer Kurven

4.5 Satz

Sei $E(K) = y^2 + ax^3 + b$ eine elliptische Kurve über K. Dann bilde $\overline{E}(K) = E(K) \cup \{O\}$, wobei O der sogenannte unendlich ferne Punkt ist. Desweiteren seien $P_1, P_2 \in E(K)$ vorgegeben.

I) Wir definieren den Punkt $P_3 = P_1 + P_2$ wie folgt:

1) Ist $P_1 = O$, so sei $P_3 = P_2$.

2) Ist $P_1 \neq O$ und $P_2 = O$, so sei $P_3 = P_1$.

3) Ist $P_1 = (x_1, y_1) \in E(K)$ und $P_2 = (x_2, y_2) \in E(K)$ mit $x_1 \neq x_2$, so sei $P_3 = (x_3, y_3)$ gegeben durch

$$x_3 = \frac{(y_2 - y_1)^2}{x_2 - x_1} - x_1 - x_2 \quad \text{und} \quad y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3)$$

4) Ist $P_1 = (x_1, y_1) \in E(K)$ und $P_2 = (x_2, y_2) \in E(K)$ und gilt $y_1 \neq y_2$, so ist $P_3 = O$.

5) Ist $P_1 = P_2 = (x_1, y_1) \in E(K)$, so sei $P_3 = (x_3, y_3)$ gegeben durch

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \quad \text{und} \quad y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$

II) Wir definieren einen Punkt $P_4 = -P_1$ wie folgt:

1) Ist $P_1 = O$, so sei $P_4 = O$.

2) Ist $P_1 = (x_1, y_1) \in E(K)$, so sei $P_4 = (x_1, -y_1)$.

Mit dieser Definition gilt:

a) Die Punkte $P_3 = P_1 + P_2$ und $P_4 = -P_1$ liegen wieder in $\overline{E}(K)$.

b) Die Menge $\overline{E}(K)$ wird mit diesen Definitionen zu einer abelschen Gruppe.

Beweis:

Zu (a): Die Fälle $I.1$, $I.2$, $I.4$, $II.1$ und $II.2$ sind klar. Die Fälle $I.3$ und $I.5$ können leicht mit CoCoA nachgeprüft werden.

Zu (b): Das Element O ist offensichtlich ein neutrales Element für $\left(\overline{E}(K), +\right)$. Nach $I.4$ gilt: $P_1 + (-P_1) = O$ für alle $P_1 \in \overline{E}(K)$. Das Kommutativgesetz $P_1 + P_2 = P_2 + P_1$ für $P_1, P_2 \in \overline{E}(K)$ ist klar. Das Assoziativgesetz wird in der Übungsaufgabe mit CoCoA gezeigt. □

4.6 Bemerkung (Geometrische Interpretation der Addition auf $\overline{E}(\mathbb{R})$)

Sei $K = \mathbb{R}$. Als Punkt O nehmen wir den unendlich fernen Punkt in Richtung der y-Achse. Für $P_1, P_2 \in E(\mathbb{R})$ kann man $P_1 + P_2$ und $-P_1$ wie folgt interpretieren:

Abbildung 9: FIXME: Rechenoperationen für Punkte auf einer (idealisierten) elliptischen Kurve

1) Die Operation $P_1 \mapsto -P_1$ ist die Spiegelung an der x-Achse.

2) Die Summe $P_1 + P_2$ ist dadurch definiert, dass $-P_1 - P_2$ der dritte Schnittpunkt (neben P_1 und P_2) der Geraden $\overline{P_1 P_2}$ mit $E(K)$ ist, d.h. es gilt $P_1 + P_2 + (-P_1 - P_2) = O$.

4.7 Bemerkung

Ist K ein Körper mit $\mathrm{char}(K) \in \{2, 3\}$, so kann man auf $\overline{E}(K)$ ebenfalls eine Gruppenstruktur definieren (vgl. Koblitz, Aspects ..., Chapter 6, §1.6).

4.8 Satz (Klassifikation endlicher Körper)

a) Die Charakteristik p eines Körpers ist Null oder eine Primzahl.

b) Ist K endlich, so ist $\mathrm{char}(K) = p$ prim.

c) Umgekehrt ist p prim, so ist $\mathbb{F}_p = \mathbb{Z}/_{p\mathbb{Z}}$ ein Körper mit p Elementen.

d) Ist K endlich und $\mathrm{char}(K) = p$, so gilt $\#K = p^e$ mit $e > 0$.

e) Für jede Primzahl p und jedes $e > 0$ gibt es genau einen Körper K mit $\#K = p^e = q$. Bezeichnung: $\mathbb{F}_q$.

f) Ist $f \in \mathbb{F}_p[x]$ ein irreduzibles Polynomvom Grad e, so gilt

$$\mathbb{F}_q = \mathbb{F}_p[x]/(f) = \mathbb{F}_p \oplus \mathbb{F}_q \bar{x} \oplus \ldots \oplus \mathbb{F}_p \bar{x}^{e-1}$$

Beweis:

Zu (a): Wäre $p = \mathrm{char}(K) < \infty$ nicht prim, so gäbe es $a, b \in \{2, \ldots, p-1\}$ mit $ab = q$ und

$$\underbrace{(1 + \ldots + 1)}_{a \text{ mal}, \neq 0} \cdot \underbrace{(1 + \ldots + 1)}_{b \text{ mal}, \neq 0} = 0$$

Dies ist ein Widerspruch dazu, dass $\underbrace{(1+\ldots+1)}_{a \text{ mal}, \neq 0}$ ein Einheit ist.

Zu (b): Klar.

Zu (c): Klar.

Zu (d): Die Abbildung $\begin{array}{ccc} \mathbb{F}_p & \to & K \\ \overline{a} & \mapsto & \underbrace{(1+\ldots+1)}_{a \text{ mal}} \end{array}$ ist injektiver Homomorphismus, d.h. es liegt eine Körpererweiterung vor. Betrachte K hiermit als $\mathbb{F}_p$-Vektorraum. Dann gilt $e = \dim_{\mathbb{F}_p}(K) < \infty$ und daher $K \cong \mathbb{F}_p^r$ (Kongruenz als $\mathbb{F}_p$-Vektorraum) und daher $\#K = p^e$.

Zu (e): vgl. Algebra.

Zu (f): Zeige, dass $\mathbb{F}_p[x]/(f) = K$ ein Körper mit $q = p^e$ Elementen ist. Durch Division mit Rest durch f folgt, dass $\left\{1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{e-1}\right\}$ eine $\mathbb{F}_p$-Vektorraumbasis von K ist. Gilt $\overline{g}\overline{h} = 0$ für $g, h \in \mathbb{F}_p[x] \setminus \mathbb{F}_p$ so folgt $gh \in (f)$, also f teilt $gh \Rightarrow f$ teilt g oder h. Daher $\overline{g} = 0$ oder $\overline{h} = 0$.

Also ist K ein Integritätsring. Damit ist die Multiplikation $\mu_{\overline{g}} : K \to K$ injektiv und $\mathbb{F}_p$-linear, also bijektiv. Daher ist $\overline{g}$ eine Einheit in K für $\overline{g} \neq 0$. □

4.9 Theorem (Hesse - Anzahl der Punkte von $E\left(\mathbb{F}_q\right)$)

Sei p prim. $q = p^e$, $e > 0$. $\overline{E}(\mathbb{F}_q) : y^2 = x^3 + ax + b$ elliptische Kurve.

a) $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$.

b) Sei $r \geq 1$ und wir betrachten $E(\mathbb{F}_{q^r})$. Dann gilt:

$$\#E(\mathbb{F}_{q^r}) = q^r - 1 - \alpha^r - \overline{\alpha}^r$$

wobei α und $\overline{\alpha}$ die komplexen Lösungen der quadratischen Gleichung

$$x^2 - (q + 1 - \#E(\mathbb{F}_q))\, x + q = 0$$

sind.

4.10 Bemerkung

a) Es gibt effiziente Algorithmen zur Berechnung von $\#E(\mathbb{F}_q)$ die bis ca. $q \approx 10^{500}$ durchführbar sind.

b) Hasse's Theorem besagt $\#E(\mathbb{F}_q) \cong q$.

B. Algorithmische Grundlagen

Auch hier sei K Körper mit $\mathrm{char}(K) \notin \{2, 3\}$.

Frage: Wie berechnet man Punkte von $E(K)$?

4.11 Satz (Berechnung von Punkten von $E\left(\mathbb{F}_q\right)$)

Sei $p > 2$ ungerade Primzahl und $q = p^e$ mit $e > 0$. Betrachte die folgenden Instruktionen:

1) Wähle ein zufälliges Element $x \in \mathbb{F}_q$ und berechne $f(x) = x^3 + ax + b$. OE gelte $f(x) \neq 0$, ansonsten wählen wir ein anderes x.

2) Berechne $f(x)^{\frac{q-1}{2}} \in \{-1, 1\}$ und prüfe, ob das Resultat Eins ist (Ist dies der Fall, so ist $f(x)$ ein Quadrat in $\mathbb{F}_q$). Ist dies nicht der Fall, so beginne wieder mit Schritt Eins.

3) Gilt $q \equiv 3 \pmod 4$, so berechne $y = f(x)^{\frac{q-1}{4}}$, gib das Paar (x, y) als Resultat aus und stoppe.

4) Gilt $q \equiv 1 \pmod 4$ schreibe $q - 1 = 2^s t$ mit $s \geq 2$ und einer ungeraden Zahl $t > 0$.

5) Wähle ein zufälliges Element $u \in \mathbb{F}_q$ und berechne $u^{\frac{q-1}{2}} \in \{-1, 1\}$. Wiederhole dies solange, bis $u^{\frac{q-1}{2}} = -1$ gilt. Berechne dann $v = u^t$.

6) Bestimme $y_1 = f(x)^{\frac{t+1}{2}}$.

7) Für $i = 2,3,\ldots,s$ berechne $f(x)^{t2^{s-i}}$ und definiere $l_0, l_1, \ldots, l_{s-2} \in \{0,1\}$ induktiv durch

$$f(x)^{t2^{s-1}} = v^{l_0 2^{s-i+1} + l_1 2^{s-i+2} + \ldots + l_{i-2} 2^{s-1}}$$

8) Bilde $l = l_0 + 2l_1 + \ldots + 2^{s-2} l_{s-2}$ und $y = y_1 v^{-l}$.
9) Gib das Paar (x,y) als Ergebnis aus und stoppe.
Dies ist ein probabilistischer Algorithmus, der einem Punkt (x,y) auf $(x,y) \in E(\mathbb{F}_q)$ berechnet.

Beweis: Nach dem kleinen Fermatschen Satz gilt $f(x)^{q-1} = 1$ in $\mathbb{F}_q$. Da $\mathbb{F}_q$ ein Körper ist, folgt $f(x)^{\frac{q-1}{2}} \in \{-1,1\}$. Sei $g \in \mathbb{F}_q^\times$ ein Erzeuger dieser zyklischen Gruppe und sei $f(x) = g^j$ mit $j \in \{0,\ldots,q-2\}$. Damit folgt:

$$f(x)^{\frac{q-1}{2}} = g^{j\frac{(q-1)}{2}} = (-1)^j$$

Dies zeigt: $f(x)^{\frac{q-1}{2}} = 1 \Leftrightarrow j$ gerade $\Leftrightarrow f(x) = g^j$ ist ein Quadrat.

Im Fall $q \equiv 3 \pmod 4$ gilt dann für $y = f(x)^{\frac{q+1}{4}}$ dass $y^2 = f(x) f(x)^{\frac{q-1}{2}} = f(x) = x^3 + ax + b$ und daher $(x,y) \in E(\mathbb{F}_q)$.

Betrachte nun den Fall $q \equiv 1 \pmod 4$. Wegen $u^{\frac{q-1}{2}} = -1$ ist u kein Quadrat in $\mathbb{F}_q$. Also folgt für $v = u^t$:

$$\begin{aligned} v^{2^s} &= u^{t2^s} = u^{q-1} = 1 \\ \text{und} \quad v^{2^{s-1}} &= u^{ts^{s-1}} = u^{\frac{q-1}{2}} = -1 \end{aligned}$$

Also ist v eine primitive 2^s-te Einheitswurzel in $\mathbb{F}_q$.
Im Schritt 6 erfüllt y_1 die Gleichung $y_1^2 = f(x)^{t+1} = f(x) f(x)^t$, wobei $f(x)$ ein Quadrat ist. Für $z = f(x)^t$ gilt

$$z^{2^{s-1}} = f(x)^{t2^{s-1}} = f(x)^{\frac{q-1}{2}} = 1$$

Also gilt: $z = v^{2l}$ mit $l \in \mathbb{N}$ und dann gilt für $y = y_1 v^{-l}$ die gewünschte Gleichung

$$y^2 = y_1^2 v^{-2l} = f(x) f(x)^t z^{-1} = f(x)$$

Wir müssen also noch zeigen, dass in den Schritten 7 und 9 ein $l \in \left\{0,\ldots,2^{s-1}-1\right\}$ berechnet wird mit der Eigenschaft $v^{2l} = z = f(x)^t$. Scheibe

$$l = l_0 + l_1 2 + \ldots + l_{s-1} 2^{s-2} \quad \text{mit } l_i \in \{0,1\}$$

Zeige, dass Schritt 7 diese l_i induktiv berechnet. Es gilt:

$$\begin{aligned} f(x)^t &= v^{2l} \\ \Rightarrow \quad f(x)^{t2^{s-2}} &= f(x)^{\frac{q-1}{4}} = v^{l2^{s-1}} = v^{l_0 2^{s-1}} \end{aligned}$$

Also folgt: $l_0 = 1 \Leftrightarrow f(x)^{\frac{q-1}{4}} = -1$.
Ebenso erhalten wir:

$$f(x)^{t2^{s-3}} = f(x)^{\frac{q-1}{8}} = v^{l2^{s-2}} = v^{l_0 2^{s-2} + l_1 2^{s-1}}$$

Dabei gilt:

$$\left[f(x)^{t2^{s-3}} v^{-l_0 2^{s-2}} \right]^2 = 1$$

und daher gilt $v^{l_1 2^{s-1}} \in \{-1,1\}$. Also folgt:

$$l_1 = 1 \quad \Leftrightarrow \quad f(x)^{\frac{q-1}{2}} = -v^{l_0 2^{s-2}}$$

Induktiv erhalten wir die Behauptung. □

4.12 Bemerkung

Braucht man nur irgendeine elliptische Kurve $E(K)$ mit einem Punkt $P \in E(K)$, so kann man einfach wie folgt verfahren: Sei $\mathrm{char}(k) > 3$. Wähle zufällige Elemente $y_0, x_0, a \in K$. Setze $b = y_0^2 - x_0^3 - ax_0$. Berechne $D = 4a^3 + 27b^2$. Wiederhole das Verfahren solange, bis $D \neq 0$ gilt. Dann verwende $E(K)$: $y^2 = x^3 + ax + b$ und $P = (x_0, y_0)$.

Aufgabe

Gegeben sei eine elliptische Kurve $E(K)$ und ein Punkt $P \in \overline{E}(K) = G$ (G ist die Gruppe der Punkte). Wie kann man $\mathrm{ord}_G(P)$ bestimmen, also

$$\mathrm{ord}_G(P) \quad = \quad \min\{i \geq 0 \mid iP = O\}$$

Die offensichtliche Methode, nämlich die Berechnung von $P, 2P, 3P, \ldots$ ist ineffizient.

4.13 Satz (Die Baby-Step-Giant-Step Methode von Shanks)

Gegeben sei eine endliche Abelsche Gruppe G und ein Element $g \in G$. Ferner sei eine Schranke $B \in \mathbb{N}$ mit $\mathrm{ord}_G(g) \leq B$ gegeben.

1) Berechne $\beta = \lfloor \sqrt{B} \rfloor$ und $1, g, g^2, \ldots, g^{\beta-1}$ und setze $g_1 = g^{-\beta}$.

2) Berechne g_1^α für $\alpha = 0, 1, \ldots, \beta - 1$ und prüfe jeweils ob $g_1^\alpha \in \{1, g, g^2, \ldots, g^{\beta-1}\}$ gilt. Sobald dies der Fall ist fahre mit Schritt 3 fort.

3) Es gelte: $g_1^\alpha = g^\gamma$ mit $\alpha \in \{1, \ldots, \beta\}$ und $\gamma \in \{0, \ldots, \beta - 1\}$. Faktorisiere $\alpha\beta + \gamma$ und finde den kleinsten Teiler $\delta \mid (\alpha\beta + \gamma)$ mit $g^\delta = 1$.

4) Gebe δ als Resultat aus und stoppe.

Dies ist ein Algorithmus, der $\mathrm{ord}_G(g)$ berechnet.

Beweis: Sei $n = \mathrm{ord}_G(g)$. Schreibe $n = \tilde{\alpha}\beta + \tilde{\gamma}$ mit $\tilde{\alpha} \in \{0, \ldots, \beta - 1\}$ und $\tilde{\gamma} \in \{0, \ldots, \beta - 1\}$. Dann gilt:

$$1 = g^n = g^{\tilde{\alpha}\beta + \tilde{\gamma}} \quad \Rightarrow \quad g_1^{\tilde{\alpha}} = g^{\tilde{\gamma}}$$

Also wird in Schritt 2 ein α mit $g_1^\alpha \in \{1, \ldots, g, \ldots, g^{\beta-1}\}$ gefunden und zwar $\alpha \leq \beta - 1$. Dann folgt $g_1^\alpha = g^\gamma$ und daher $g^{\alpha\beta+\gamma} = 1$. Daher $n \mid (\alpha\beta + \gamma)$ und damit haben wir n in Schritt 3 gefunden. □

4.14 Bemerkungen

a) Man kann diesen Algorithmus so modifizieren, dass er $\#G$ berechnet. Vergleiche H. Cohen, A course in computational number theory, Springer 1993, S. 241

b) Kennt man die Faktorisierung von $\#G$ (oder die "kleinen" Primfaktoren von $\#G$), so kann man leicht eine "gute" Schranke für $\mathrm{ord}_G(g)$ angeben.

c) Man kann die Algorithmen zur Berechnung von $\#G$ und $\mathrm{ord}_G(g)$ stark optimieren. Vergleiche H. Cohen, A course in computational number theory, Springer 1993, S. 404ff.

d) Angenommen wir brauchen nur irgendeine elliptische Kurve $E(K)$ und ein $P \in \overline{E}(K)$ mit bekannter Ordnung $\mathrm{ord}_{\overline{E}(K)}(P) = \#\overline{E}(K)$. Dann kann man wie folgt vorgehen:

1) Wähle eine elliptische Kurve $E(\mathbb{Q})$ und finde einen Punkt $P \in E(\mathbb{Q})$ mit $\mathrm{ord}_{\overline{E}(\mathbb{Q})}(P) = \infty$ (Es gibt nur endlich viele $P \in E(\mathbb{Q})$ mit $\mathrm{ord}_{\overline{E}(\mathbb{Q})}(P) < \infty$ und diese sind leicht berechenbar). Jeder Punkt $P \in E(\mathbb{Q})$ mit $P = (x_0, y_0)$ und $y_0 \notin \mathbb{Z}$ erfüllt $\mathrm{ord}_{\overline{E}(\mathbb{Q})}(P) = \infty$.

2) Bilde die Reduktion $E(\mathbb{F}_p) = E(\mathbb{Q})_{\bmod p}$ dieser Kurve, d.h.die kubische Kurve über $\mathbb{F}_p$ mit derselben Gleichung $y^2 = x^2 + \overline{a}x + \overline{b}$. Die Primzahl p darf Zähler und Nenner von a und b nicht teilen. Teilt p auch Zähler und Nenner von $D = 4a^3 + 27b^3$, dann ist $E(\mathbb{F}_p)$ wieder eine elliptische Kurve.

3) Berechne $\#E(\mathbb{F}_p)$ und wiederhole die Schritte 1 und 2 solange bis $\#E(\mathbb{F}_q)$ eine Primzahl ist. Die Wahrscheinlichkeit hierfür ist $\frac{1}{\log(p)}$. In diesem Fall erfüllt jeder Punkt $p \in E(\mathbb{F}_p)$ die Eigenschaft $\mathrm{ord}_{\overline{E}(\mathbb{F}_p)} = \#\overline{E}(\mathbb{F}_p)$.