Vorlesungsskript

Einführung in die Kryptologie

Sommersemester 2022

Prof. Dr. Johannes Köbler
Humboldt-Universität zu Berlin
Lehrstuhl Komplexität und Kryptografie

24. April 2022

Inhaltsverzeichnis

1 Klassische Kryptoverfahren

1.1 Einführung

Kryptografische Verfahren schaffen Vertrauen in ungeschützten Umgebungen. Sie ermöglichen sichere Kommunikation über unsichere Kanäle und können verhindern, dass sich ein Kommunikationspartner unfair verhält. In unsicheren Umgebungen wie dem Internet können sie die aus direkter Interaktion gewohnte Sicherheit herstellen. Und auch die Interaktion in sicheren Umgebungen wird um Möglichkeiten erweitert, die ohne Kryptografie nicht denkbar wären.

In diesem Modul werden wir uns mit den mathematischen Grundlagen von kryptografischen Verfahren beschäftigen, wobei (symmetrische und asymmetrische) Verschlüsselungsverfahren im Vordergrund stehen. Im Mastermodul Kryptologie werden wir dann auch kryptografische Verfahren und Protokolle für andere Schutzziele betrachten wie z.B. Hashverfahren und digitale Signaturen sowie Pseudozufallsgeneratoren.

Kryptosysteme (Verschlüsselungsverfahren) dienen der Geheimhaltung von Nachrichten bzw. Daten. Hierzu gibt es auch andere Methoden wie z.B.

Physikalische Maßnahmen: Tresor etc.

Organisatorische Maßnahmen: einsamer Waldspaziergang etc.

Steganografische Maßnahmen: unsichtbare Tinte etc.

Andererseits können durch kryptografische Verfahren weitere **Schutzziele** realisiert werden.

- *Vertraulichkeit*
  - Geheimhaltung
  - Anonymität (z.B. Mobiltelefon)
  - Unbeobachtbarkeit (von Transaktionen)
- *Integrität*
  - von Nachrichten und Daten
- *Zurechenbarkeit*
  - Authentikation
  - Unabstreitbarkeit
  - Identifizierung
- *Verfügbarkeit*
  - von Daten
  - von Rechenressourcen
  - von Informationsdienstleistungen

In das Umfeld der Kryptografie fallen auch die folgenden Begriffe.

Kryptografie: Lehre von der Geheimhaltung von Informationen durch Verschlüsselung. Im weiteren Sinne: Wissenschaft von der Übermittlung, Speicherung und Verarbeitung von Daten in einer von potentiellen Gegnern bedrohten Umgebung.

Kryptoanalysis: Erforschung der Methoden eines unbefugten Angriffs gegen ein Kryptoverfahren (Zweck: Vereitelung der mit seinem Einsatz verfolgten Ziele)

Kryptoanalyse: Analyse eines Kryptoverfahrens zum Zweck der Bewertung seiner kryptografischen Stärken bzw. Schwächen.

Kryptologie: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptografischen Verfahren (umfasst Kryptografie und Kryptoanalyse).

1.2 Kryptosysteme

Es ist wichtig, Kryptosysteme von Codesystemen zu unterscheiden.

Codesysteme

- operieren auf semantischen Einheiten,
- starre Festlegung, welche Zeichenfolge wie zu ersetzen ist.

Beispiel 1 (Ausschnitt aus einem Codebuch der deutschen Luftwaffe)**.**

xve	***Bis auf weiteres Wettermeldung gemäß Funkbefehl testen***
yde	***Frage***
sLk	***Befehl***
fin	***beendet***
eom	***eigene Maschinen***

◁

Kryptosysteme

- operieren auf syntaktischen Einheiten
- flexibler Mechanismus durch Schlüsselvereinbarung

Definition 2. *Ein* ***Alphabet*** $A = \{a_0, \ldots, a_{m-1}\}$ *ist eine geordnete endliche Menge von* ***Zeichen*** a_i*. Eine Folge* $x = x_1 \ldots x_n \in A^n$ *heißt* ***Wort*** *(der* ***Länge*** n*). Die Menge aller Wörter über dem Alphabet* A *ist* $A^* = \bigcup_{n \geq 0} A^n$*.*

Beispiel 3. *Das* ***lateinische Alphabet*** A_{lat} *enthält die 26 Zeichen* `A,...,Z`*. Bei klassischen Verfahren wurde in Klartexten meist auf den Gebrauch von Interpunktions- und Leerzeichen sowie auf Groß- und Kleinschreibung verzichtet (*$\rightsquigarrow$ *Verringerung der Redundanz im Klartext).* ◁

Definition 4. *Ein* ***Kryptosystem*** *wird durch folgende Komponenten beschrieben:*

- A*, das* ***Klartextalphabet****,*
- B*, das* ***Kryptotextalphabet****,*
- K*, der* ***Schlüsselraum*** *(key space),*
- $M \subseteq A^*$*, der* ***Klartextraum*** *(message space),*
- $C \subseteq B^*$*, der* ***Kryptotextraum*** *(ciphertext space),*
- $E : K \times M \to C$*, die* ***Verschlüsselungsfunktion*** *(encryption function),*

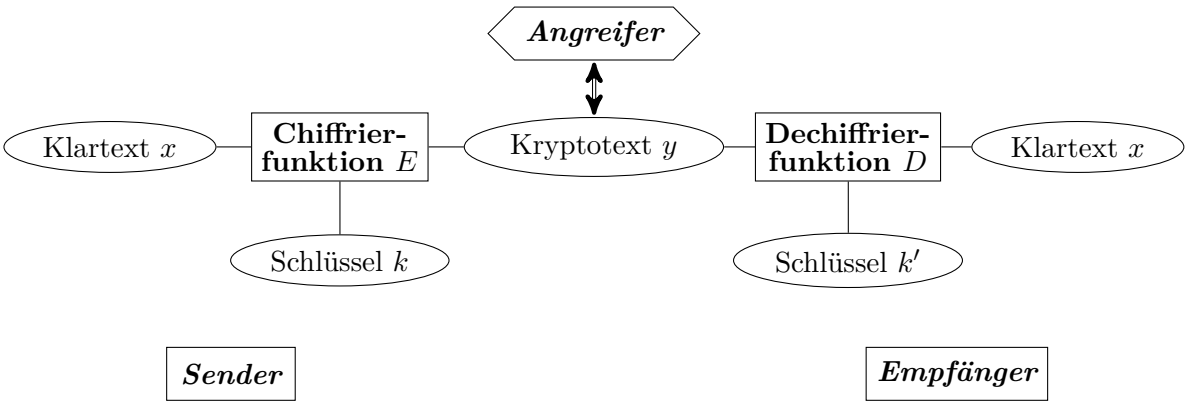

Abbildung 1.1: Schematische Darstellung der Funktionsweise eines Kryptosystems

- $D : K \times C \to M$, *die* ***Entschlüsselungsfunktion*** *(decryption function) und*
- $S \subseteq K \times K$, *eine Menge von Schlüsselpaaren* (k, k') *mit der Eigenschaft, dass für jeden Klartext* $x \in M$ *folgende Beziehung gilt:*

$$D(k', E(k, x)) = x \tag{1.1}$$

Bei symmetrischen Kryptosystemen ist $S = \{(k, k) \mid k \in K\}$, weshalb wir in diesem Fall auf die Angabe von S verzichten können. Zu jedem Schlüssel $k \in K$ korrespondiert also eine **Chiffrierfunktion** $E_k : x \mapsto E(k, x)$ und eine **Dechiffrierfunktion** $D_k : y \mapsto D(k, y)$. Die Gesamtheit dieser Abbildungen wird auch **Chiffre** (englisch *cipher*) genannt. (Daneben wird der Begriff „Chiffre“ auch als Bezeichnung für einzelne Kryptotextzeichen oder kleinere Kryptotextsequenzen verwendet.)

Lemma 5. *Für jedes Paar* $(k, k') \in S$ *ist die Chiffrierfunktion* E_k *injektiv.*

Beweis. Angenommen, für zwei Klartexte x_1 und x_2 gilt $E(k, x_1) = E(k, x_2)$. Dann folgt

$$x_1 \overset{(1.1)}{=} D(k', \underbrace{E(k, x_1)}_{E(k,x_2)}) = D(k', E(k, x_2)) \overset{(1.1)}{=} x_2$$

□

1.3 Die additive Chiffre

Die Moduloarithmetik erlaubt es uns, das Klartextalphabet mit einer Addition und Multiplikation auszustatten.

Definition 6 (**teilt-Relation, modulare Kongruenz**). *Seien* a, b, m *ganze Zahlen mit* $m \geq 1$. *Die Zahl* a ***teilt*** b *(kurz:* $a|b$*), falls ein* $d \in \mathbb{Z}$ *existiert mit* $b = ad$. *Teilt* m *die Differenz* $a - b$, *so schreiben wir hierfür*

$$a \equiv_m b \text{ oder } a \equiv b \pmod{m}$$

(in Worten: a *ist* ***kongruent*** *zu* b *modulo* m*). Weiterhin bezeichne*

$$a \bmod m = \min\{a - dm \geq 0 \mid d \in \mathbb{Z}\}$$

Tabelle 1.1: Werte der additiven Chiffrierfunktion ROT13 (Schlüssel $k = 13$).

x	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
$E(13, x)$	*n o p q r s t u v w x y z a b c d e f g h i j k l m*

den bei der Ganzzahldivision von a durch m auftretenden ***Rest****, also diejenige ganze Zahl $r \in \{0, \ldots, m-1\}$, für die eine ganze Zahl $d \in \mathbb{Z}$ existiert mit $a = dm + r$. Sowohl r als auch d sind hierbei eindeutig bestimmt (siehe Übungen) und die Zahl d wird auch mit a* div *m bezeichnet.*

Die auf $\mathbb{Z}$ definierten Operationen

$$a \oplus_m b := (a + b) \bmod m \text{ und } a \odot_m b := ab \bmod m$$

sind abgeschlossen auf $\mathbb{Z}_m = \{0, \ldots, m-1\}$ und bilden auf dieser Menge einen kommutativen Ring mit Einselement, den sogenannten **Restklassenring** modulo m. Für $a \oplus_m -b$ schreiben wir auch $a \ominus_m b$. Wenn aus dem Kontext klar ist, dass $a, b \in \mathbb{Z}_m$ sind, schreiben wir anstelle von $a \oplus_m b$, $a \ominus_m b$ und $a \odot_m b$ auch einfach $a + b$, $a - b$ bzw. ab. Durch Identifikation der Zeichen a_i eines Alphabets $A = \{a_0, \ldots, a_{m-1}\}$ mit ihren Indizes können wir die auf $\mathbb{Z}_m$ definierten Rechenoperationen auf Buchstaben übertragen.

Definition 7 (**Buchstabenrechnung**). *Sei $A = \{a_0, \ldots, a_{m-1}\}$ ein Alphabet. Für Indizes $i, j \in \{0, \ldots, m-1\}$ und eine ganze Zahl $z \in \mathbb{Z}$ ist*

$$\begin{array}{lll} a_i + a_j = a_{i+j}, & a_i - a_j = a_{i-j}, & a_i a_j = \quad a_{ij}, \\ a_i + z \ = a_{i+z}, & a_i - z \ = a_{i-z}, & z a_j \ = a_{zj \bmod m}. \end{array}$$

Mit Hilfe dieser Notation lässt sich die additive Chiffre , die auch als Verschiebechiffre oder Caesar-Chiffre bezeichnet wird, leicht beschreiben.

Definition 8. *Bei der* ***additiven Chiffre*** *ist $A = B = M = C$ ein beliebiges Alphabet mit $m := \|A\|$ und $K = \{0, \ldots, m-1\}$. Für $k \in K$, $x \in M$ und $y \in C$ gilt*

$$E(k, x) = x + k \quad \textit{und} \quad D(k, y) = y - k.$$

Im Fall des lateinischen Alphabets führt der Schlüssel $k = 13$ auf eine interessante Chiffrierfunktion, die in UNIX-Umgebungen auch unter der Bezeichnung ROT13 bekannt ist (siehe Tabelle 1.1). Natürlich kann mit dieser Chiffrierfunktion nicht ernsthaft die Vertraulichkeit von Nachrichten gewahrt werden. Vielmehr soll durch sie ein unbeabsichtigtes Mitlesen – etwa von Rätsellösungen – verhindert werden.

ROT13 ist eine ***involutorische*** (also zu sich selbst inverse) Abbildung, d.h. für alle $x \in A$ gilt

$$\text{ROT13}(\text{ROT13}(x)) = x.$$

Da ROT13 zudem keinen Buchstaben auf sich selbst abbildet, ist sie sogar ***echt involutorisch***.

1.4 Die affine Chiffre

Die Buchstabenrechnung legt folgende Modifikation der Caesar-Chiffre nahe. Anstatt auf jedes Klartextzeichen den Schlüsselwert k zu addieren, können wir die Klartextzeichen auch mit k multiplizieren. Allerdings erhalten wir hierbei nicht für jeden Wert von k eine injektive Chiffrierfunktion. So bildet etwa die Funktion $g : A_{lat} \to A_{lat}$ mit $g(x) = 2x$ sowohl `A` als auch `N` auf das Zeichen $g(\mathtt{A}) = g(\mathtt{N}) = \mathtt{a}$ ab. Um eine hinreichende und notwendige Bedingung für die Zulässigkeit eines Schlüsselwerts k formulieren zu können, führen wir folgende Begriffe ein.

Definition 9 (ggT, kgV, teilerfremd). *Seien $a, b \in \mathbb{Z}$. Für $(a, b) \neq (0, 0)$ ist*

$$\mathrm{ggT}(a, b) = \max\{d \in \mathbb{Z} \mid d \text{ teilt die beiden Zahlen } a \text{ und } b\}$$

*der **größte gemeinsame Teiler** von a und b und für $a \neq 0, b \neq 0$ ist*

$$\mathrm{kgV}(a, b) = \min\{d \in \mathbb{Z} \mid d \geq 1 \text{ und die beiden Zahlen } a \text{ und } b \text{ teilen } d\}$$

*das **kleinste gemeinsame Vielfache** von a und b. Ist $\mathrm{ggT}(a, b) = 1$, so nennt man a und b **teilerfremd** oder man sagt, a ist **relativ prim** zu b.*

Lemma 10. *Seien $a, b, c \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a + bc)$ und somit $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a \bmod b)$, falls $b \geq 1$ ist.*

Beweis. Jeder Teiler d von a und b ist auch ein Teiler von b und $a + bc$ und umgekehrt. □

Euklidischer Algorithmus: Der größte gemeinsame Teiler zweier Zahlen a und b lässt sich wie folgt bestimmen.

O. B. d. A. sei $a > b > 0$. Bestimme die natürlichen Zahlen (durch Divsision mit Rest*):

$$r_0 = a > r_1 = b > r_2 > \cdots > r_s > r_{s+1} = 0 \text{ und } d_2, d_3, \ldots d_{s+1}$$

mit

$$r_{i-1} = d_{i+1} r_i + r_{i+1} \text{für } i = 1, \ldots, s.$$

Hierzu sind s Divisionsschritte erforderlich. Wegen

$$\mathrm{ggT}(r_{i-1}, r_i) = \mathrm{ggT}(r_i, \underbrace{r_{i-1} - d_{i+1} r_i}_{r_{i+1}})$$

folgt $\mathrm{ggT}(a, b) = \mathrm{ggT}(r_s, r_{s+1}) = r_s$.

Beispiel 11. *Für $a = 693$ und $b = 147$ erhalten wir*

i	r_{i-1}	$=$	$d_{i+1}\cdot$	r_i	$+ r_{i+1}$
1	693	$=$	4	$\cdot 147$	$+ 105$
2	147	$=$	1	$\cdot 105$	$+ 42$
3	105	$=$	2	$\cdot 42$	$+ 21$
4	42	$=$	2	$\cdot \mathbf{21}$	$+ 0$

und damit $\mathrm{ggT}(693, 147) = r_4 = 21$. ◁

*Also: $d_{i+1} = r_{i-1} \operatorname{div} r_i$ und $r_{i+1} = r_{i-1} \bmod r_i$.

Der euklidische Algorithmus lässt sich sowohl iterativ als auch rekursiv implementieren.

Prozedur $\texttt{Euklid}_{\texttt{it}}(a, b)$

```
1 repeat
2     r := a mod b
3     a := b
4     b := r
5 until r = 0
6 return(a)
```

Prozedur $\texttt{Euklid}_{\texttt{rek}}(a, b)$

```
1 if b = 0 then
2     return(a)
3 else
4     return(Euklid_rek(b, a mod b))
```

Zur Abschätzung von s verwenden wir die Folge der Fibonacci-Zahlen F_n.

$$F_n = \begin{cases} 0, & \text{falls } n = 0 \\ 1, & \text{falls } n = 1 \\ F_{n-1} + F_{n-2}, & \text{falls } n \geq 2 \end{cases}$$

Durch Induktion über $i = s+1, s, \ldots, 0$ folgt $r_i \geq F_{s+1-i}$ und somit $a = r_0 \geq F_{s+1}$. Weiterhin lässt sich durch Induktion über $n \geq 0$ zeigen, dass $F_{n+1} \geq \phi^{n-1}$ ist, wobei $\phi = (1+\sqrt{5})/2$ der ***goldene Schnitt*** ist. Der Induktionsanfang ($n = 0$ oder 1) ist klar, da $F_2 = F_1 = 1 = \phi^0 \geq \phi^{-1}$ ist. Unter der Induktionsannahme $F_{i+1} \geq \phi^{i-1}$ für $i \leq n-1$ folgt wegen $\phi^2 = \phi + 1$

$$F_{n+1} = F_n + F_{n-1} \geq \phi^{n-2} + \phi^{n-3} = \phi^{n-3}(\phi + 1) = \phi^{n-1}.$$

Somit ist $a \geq \phi^{s-1}$, d. h. $s \leq 1 + \lfloor \log_\phi a \rfloor$.

Satz 12. *Seien $a > b > 0$ ganze Zahlen und sei n die Länge von a in Binärdarstellung. Dann führt der euklidische Algorithmus $O(n)$ Divisionsschritte zur Berechnung von* $\mathrm{ggT}(a, b)$ *durch. Dies führt auf eine Zeitkomplexität von $O(n^3)$, da jede Ganzzahldivision in Zeit $O(n^2)$ durchführbar ist.*

Erweiterter euklidischer bzw. **Berlekamp-Algorithmus:** Der euklidische Algorithmus kann so modifiziert werden, dass er eine lineare Darstellung

$$\mathrm{ggT}(a, b) = \lambda a + \mu b \text{ mit } \lambda, \mu \in \mathbb{Z}$$

des ggT liefert (Zeitkomplexität ebenfalls $O(n^3)$). Hierzu werden neben r_i und d_i weitere Zahlen

$$p_i = p_{i-2} - d_i p_{i-1} \text{ (mit } p_0 = 1 \text{ und } p_1 = 0)$$

und

$$q_i = q_{i-2} - d_i q_{i-1} \text{ (mit } q_0 = 0 \text{ und } q_1 = 1$$

für $i = 0, \ldots, s$ bestimmt. Dann gilt für $i = 0$ und $i = 1$,

$$ap_i + bq_i = r_i,$$

und wegen

$$\begin{aligned} ap_{i+1} + bq_{i+1} &= a(p_{i-1} - d_{i+1}p_i) + b(q_{i-1} - d_{i+1}q_i) \\ &= ap_{i-1} + bq_{i-1} - d_{i+1}(ap_i + bq_i) \\ &= (r_{i-1} - d_{i+1}r_i) \\ &= r_{i+1} \end{aligned}$$

folgt induktiv über $i = 2, \ldots, s$, dass diese Gleichung auch für $i = s$ gilt:

$$ap_s + bq_s = r_s = \mathrm{ggT}(a, b).$$

Korollar 13 (Lemma von Bezout)**.** *Der größte gemeinsame Teiler von a und b ist in der Form*

$$\mathrm{ggT}(a, b) = \lambda a + \mu b \text{ mit } \lambda, \mu \in \mathbb{Z}$$

darstellbar.

Beispiel 14. *Für $a = 693$ und $b = 147$ erhalten wir wegen*

i	r_{i-1}	$=$	$d_{i+1}\cdot$	r_i	$+$	r_{i+1}	p_i	q_i
0							1	0
1	693	$=$	4	$\cdot 147$	$+$	105	0	1
2	147	$=$	1	$\cdot 105$	$+$	42	1	-4
3	105	$=$	2	$\cdot$ 42	$+$	21	-1	5
4	42	$=$	2	$\cdot$ **21**	$+$	0	**3**	$\mathbf{-14}$

$p_i \cdot 693 +$	$q_i \cdot 147 =$	r_i
$1 \cdot 693 +$	$0 \cdot 147 =$	693
$0 \cdot 693 +$	$1 \cdot 147 =$	147
$1 \cdot 693 -$	$4 \cdot 147 =$	105
$-1 \cdot 693 +$	$5 \cdot 147 =$	42
$3 \cdot 693 -$	$14 \cdot 147 =$	21

die lineare Darstellung $3 \cdot 693 - 14 \cdot 147 = 21$. ◁

Aus der linearen Darstellbarkeit des größten gemeinsamen Teilers ergeben sich eine Reihe von nützlichen Schlussfolgerungen.

Korollar 15. *Der größte gemeinsame Teiler von a und b wird von allen gemeinsamen Teilern von a und b geteilt,*

$$x|a \ \wedge \ x|b \quad \Rightarrow \quad x|\,\mathrm{ggT}(a, b).$$

Beweis. Seien $\mu, \lambda \in \mathbb{Z}$ mit $\mu a + \lambda b = \mathrm{ggT}(a, b)$. Falls x sowohl a als auch b teilt, dann teilt x auch die Produkte μa und λb und somit auch deren Summe. □

Korollar 16. $\mathrm{ggT}(a, b) = \min\{\lambda a + \mu b \geq 1 \mid \lambda, \mu \in \mathbb{Z}\}$.

Beweis. Sei $M = \{\lambda a + \mu b \geq 1 \mid \lambda, \mu \in \mathbb{Z}\}$, $m = \min M$ und $g = \mathrm{ggT}(a, b)$. Dann folgt $g \geq m$, da g in der Menge M enthalten ist, und $g \leq m$, da g jede Zahl in M teilt. □

Korollar 17. *Zwei Zahlen a und b sind genau dann zu einer Zahl $m \in \mathbb{Z}$ teilerfremd, wenn ihr Produkt ab teilerfremd zu m ist,*

$$\mathrm{ggT}(a, m) = \mathrm{ggT}(b, m) = 1 \quad \Leftrightarrow \quad \mathrm{ggT}(ab, m) = 1.$$

Beweis. Da a und b teilerfremd zu m sind, existieren Zahlen $\mu, \lambda, \mu', \lambda' \in \mathbb{Z}$ mit $\mu a + \lambda m = \mu' b + \lambda' m = 1$. Somit ergibt sich aus der Darstellung

$$1 = (\mu a + \lambda m)(\mu' b + \lambda' m) = \underbrace{\mu\mu'}_{\mu''} ab + \underbrace{(\mu a \lambda' + \mu' b \lambda + \lambda \lambda' m)}_{\lambda''} m$$

und Korollar 16, dass auch ab teilerfremd zu m ist.

Gilt umgekehrt $\mathrm{ggT}(ab, m) = 1$, so existieren Zahlen $\mu, \lambda \in \mathbb{Z}$ mit $\mu ab + \lambda m = 1$. Mit Korollar 16 folgt sofort $\mathrm{ggT}(a, m) = \mathrm{ggT}(b, m) = 1$. □

Korollar 18 (Lemma von Euklid)**.** *Sind a und b teilerfremd und teilt a das Produkt bc, so teilt a auch c,*

$$\mathrm{ggT}(a,b) = 1 \ \wedge \ a|bc \quad \Rightarrow \quad a|c.$$

Beweis. Wegen $\mathrm{ggT}(a,b) = 1$ existieren Zahlen $\mu, \lambda \in \mathbb{Z}$ mit $\mu a + \lambda b = 1$. Falls a das Produkt bc teilt, muss a auch die Zahl $\mu ac + \lambda bc = c$ teilen. □

Damit nun eine Abbildung $g : A \to A$ der Form $g(x) = bx$ auf einem Alphabet A injektiv (oder gleichbedeutend, surjektiv) ist, muss es zu jedem Zeichen $y \in A$ genau einen Zeichen $x \in A$ mit $bx = y$ geben. Wie der folgende Satz zeigt, ist dies genau dann der Fall, wenn b und m teilerfremd sind.

Satz 19. *Seien b, y, m ganze Zahlen mit $m \geq 1$. Die lineare Kongruenzgleichung $bx \equiv_m y$ besitzt genau dann eine eindeutige Lösung $x \in \{0, \ldots, m-1\}$, wenn $\mathrm{ggT}(b,m) = 1$ ist.*

Beweis. Angenommen, $\mathrm{ggT}(b,m) = g > 1$. Dann ist mit x auch $x' = x + m/g$ eine Lösung von $bx \equiv_m y$ mit $x \not\equiv_m x'$. Folglich ist die Kongruenz $bx \equiv_m y$ nicht eindeutig lösbar.
Gilt umgekehrt $\mathrm{ggT}(b,m) = 1$, so folgt aus den Kongruenzen

$$bx_1 \equiv_m y$$

und

$$bx_2 \equiv_m y$$

sofort $b(x_1 - x_2) \equiv_m 0$, also $m|b(x_1 - x_2)$. Wegen $\mathrm{ggT}(b,m) = 1$ folgt mit dem Lemma von Euklid $m|(x_1 - x_2)$, also $x_1 \equiv_m x_2$. Folglich hat die Kongruenz $bx \equiv_m y$ für jedes $y \in \mathbb{Z}_m$ höchstens eine Lösung $x \in \{0, \ldots, m-1\}$. Zudem folgt, dass die Abbildung $f : \mathbb{Z}_m \to \mathbb{Z}_m$ mit $f(x) = bx \bmod m$ injektiv ist. Da aber der Definitions- und der Wertebereich von f die gleiche Mächtigkeit haben, muss f dann auch surjektiv sein. Somit hat die Kongruenz $bx \equiv_m y$ für jedes $y \in \mathbb{Z}_m$ sogar genau eine Lösung $x \in \{0, \ldots, m-1\}$. □

Korollar 20. *Im Fall $\mathrm{ggT}(b,m) = 1$ hat die Kongruenz $bx \equiv_m 1$ genau eine Lösung, die das **multiplikative Inverse** von b modulo m genannt und mit $b^{-1} \bmod m$ (oder einfach mit b^{-1}) bezeichnet wird.*

Korollar 17 zeigt, dass die Menge

$$\mathbb{Z}_m^* = \{b \in \mathbb{Z}_m \mid \mathrm{ggT}(b,m) = 1\}$$

aller invertierbaren Elemente von $\mathbb{Z}_m$ unter der Operation $\odot_m$ abgeschlossen ist. Mit Korollar 20 folgt daher, dass $(\mathbb{Z}_m^*, \odot_m, 1)$ eine multiplikative Gruppe bildet. Allgemeiner zeigt man, dass die Multiplikation eines beliebigen Rings $(R, +, \cdot, 0, 1)$ mit Eins auf der Menge $R^* = \{a \in R \mid \exists b \in R : ab = 1 = ba\}$ aller **Einheiten** von R eine Gruppe bildet (siehe Übungen). Diese Gruppe $(R^*, \cdot, 1)$ wird als **Einheitengruppe** von R bezeichnet.
Das multiplikative Inverse von b modulo m ergibt sich aus der linearen Darstellung $\lambda b + \mu m = \mathrm{ggT}(b,m) = 1$ zu $b^{-1} = \lambda \bmod m$. Die folgende Tabelle gibt für jedes $b \in \mathbb{Z}_{26}^*$ das multiplikative Inverse b^{-1} an.

b	1	3	5	7	9	11	15	17	19	21	23	25
b^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Bei Kenntnis von b^{-1} kann die Kongruenz $bx \equiv_m y$ leicht zu $x = yb^{-1} \bmod m$ gelöst werden.
Nun lässt sich die additive Chiffre leicht zur affinen Chiffre erweitern.

Definition 21. *Bei der* ***affinen Chiffre*** *ist $A = B = M = C$ ein beliebiges Alphabet mit $m := \|A\|$ und $K = \mathbb{Z}_m^* \times \mathbb{Z}_m$. Für $k = (b, c) \in K$, $x \in M$ und $y \in C$ gilt*

$$E(k, x) = bx + c \quad \text{und} \quad D(k, y) = b^{-1}(y - c).$$

In diesem Fall liefert die Schlüsselkomponente $b = -1$ für jeden Wert von $c \in \mathbb{Z}_m$ eine involutorische Chiffrierfunktion $x \mapsto E_{(-1,c)}(x) = c - x$ (**verschobenes komplementäres Alphabet**). Wählen wir für c ebenfalls den Wert -1, so ergibt sich die Chiffrierfunktion $x \mapsto -x - 1$, die auch als **revertiertes Alphabet** bekannt ist. Offenbar ist diese Funktion genau dann echt involutorisch, wenn m gerade ist.

x	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
$-x$	*a z y x w v u t s r q p o n m l k j i h g f e d c b*
$-x-1$	*z y x w v u t s r q p o n m l k j i h g f e d c b a*

Als nächstes illustrieren wir die Ver- und Entschlüsselung mit der affinen Chiffre an einem kleinen Beispiel.

Beispiel 22 (affine Chiffre)**.** *Sei $A = \{\mathsf{A}, \ldots, \mathsf{Z}\} = B$, also $m = 26$. Weiter sei $k = (9, 2)$, also $b = 9$ und $c = 2$. Um das Klartextzeichen $x = \mathsf{F}$ zu verschlüsseln, berechnen wir*

$$E(k, x) = bx + c = 9\mathsf{F} + 2 = \mathsf{v},$$

da der Index von F *gleich 5, der von* v *gleich 21 und $9 \cdot 5 + 2 = 47 \equiv_{26} 21$ ist. Um ein Kryptotextzeichen wieder entschlüsseln zu können, benötigen wir das multiplikative Inverse von $b = 9$, das sich wegen*

i	r_{i-1}	$=$	$d_{i+1} \cdot r_i$	$+$	r_{i+1}	$p_i \cdot 26 +$	$q_i \cdot 9 =$	r_i
0						$1 \cdot 26 +$	$0 \cdot 9 =$	26
1	26	$=$	$2 \cdot 9$	$+$	8	$0 \cdot 26 +$	$1 \cdot 9 =$	9
2	9	$=$	$1 \cdot 8$	$+$	1	$1 \cdot 26 +$	$(-2) \cdot 9 =$	8
3	8	$=$	$8 \cdot \mathbf{1}$	$+$	0	$(-1) \cdot 26 +$	$\mathbf{3} \cdot 9 =$	1

zu $b^{-1} = q_3 = 3$ ergibt. Damit erhalten wir für das Kryptotextzeichen $y =$ v *das ursprüngliche Klartextzeichen*

$$D(k, y) = b^{-1}(y - c) = 3(\mathsf{v} - 2) = \mathsf{F}$$

zurück, da $3 \cdot 19 = 57 \equiv_{26} 5$ ist. ◁

1.5 Die Eulersche Phi-Funktion

Zur Berechnung der Schlüsselzahl bei der multiplikativen und affinen Chiffre benötigen wir die Funktion

$$\varphi : \mathbb{N} \to \mathbb{N} \quad \text{mit } \varphi(m) = \|\mathbb{Z}_m^*\| = \|\{a \in \mathbb{Z}_m \mid \mathrm{ggT}(a, m) = 1\}\|,$$

die sogenannte ***Eulersche φ-Funktion***. Die folgende Tabelle zeigt die Werte $\varphi(m)$ für $m = 1, \ldots, 10$ (für die Menge $\{1, \ldots, n\}$, $n \in \mathbb{N}$, schreiben wir auch kurz $[n]$).

m	1	2	3	4	5	6	7	8	9	10
$\mathbb{Z}_m^*$	$\{0\}$	$\{1\}$	$[2]$	$\{1,3\}$	$[4]$	$\{1,5\}$	$[6]$	$\{1,3,5,7\}$	$\{1,2,4,5,7,8\}$	$\{1,3,7,9\}$
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4

Für primes p gilt offensichtlich $\varphi(p) = p - 1$, da $\mathbb{Z}_p^* = [p-1]$ ist. Wegen

$$\mathbb{Z}_{p^k} - \mathbb{Z}_{p^k}^* = \{0, p, 2p, \ldots, (p^{k-1} - 1)p\}$$

folgt zudem

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) \text{ für } k \geq 1.$$

Um hieraus für beliebige Zahlen $n \in \mathbb{N}$ eine Formel für $\varphi(n)$ zu erhalten, genügt es, $\varphi(ml)$ im Fall $\mathrm{ggT}(m, l) = 1$ in Abhängigkeit von $\varphi(m)$ und $\varphi(l)$ zu bestimmen. Hierzu betrachten wir die Abbildung $f : \mathbb{Z}_{ml} \to \mathbb{Z}_m \times \mathbb{Z}_l$ mit

$$f(x) = (x \bmod m, x \bmod l).$$

Beispiel 23. *Sei $m = 5$ und $l = 6$. Dann erhalten wir die Funktion $f : \mathbb{Z}_{30} \to \mathbb{Z}_5 \times \mathbb{Z}_6$ mit*

x	0	**1**	2	3	4	5	6	**7**	8	9
$f(x)$	$(0,0)$	$(\mathbf{1},\mathbf{1})$	$(\mathbf{2},2)$	$(\mathbf{3},3)$	$(\mathbf{4},4)$	$(0,\mathbf{5})$	$(\mathbf{1},0)$	$(\mathbf{2},\mathbf{1})$	$(\mathbf{3},2)$	$(\mathbf{4},3)$

x	10	**11**	12	**13**	14	15	16	**17**	18	**19**
$f(x)$	$(0,4)$	$(\mathbf{1},\mathbf{5})$	$(\mathbf{2},0)$	$(\mathbf{3},\mathbf{1})$	$(\mathbf{4},2)$	$(0,3)$	$(\mathbf{1},4)$	$(\mathbf{2},\mathbf{5})$	$(\mathbf{3},0)$	$(\mathbf{4},\mathbf{1})$

x	20	21	22	**23**	24	25	26	27	28	**29**
$f(x)$	$(0,2)$	$(\mathbf{1},3)$	$(\mathbf{2},4)$	$(\mathbf{3},\mathbf{5})$	$(\mathbf{4},0)$	$(0,\mathbf{1})$	$(\mathbf{1},2)$	$(\mathbf{2},3)$	$(\mathbf{3},4)$	$(\mathbf{4},\mathbf{5})$

*Man beachte, dass f eine Bijektion zwischen $\mathbb{Z}_{30}$ und $\mathbb{Z}_5 \times \mathbb{Z}_6$ ist. Zudem fällt auf, dass ein x-Wert genau dann in $\mathbb{Z}_{30}^*$ liegt, wenn der Funktionswert $f(x) = (y, z)$ zu $\mathbb{Z}_5^* \times \mathbb{Z}_6^*$ gehört (die Werte $x \in \mathbb{Z}_{30}^*$, $y \in \mathbb{Z}_5^*$ und $z \in \mathbb{Z}_6^*$ sind **fett** gedruckt). Folglich bildet f die Argumente in $\mathbb{Z}_{30}^*$ bijektiv auf die Werte in $\mathbb{Z}_5^* \times \mathbb{Z}_6^*$ ab. Für f^{-1} erhalten wir somit folgende Tabelle:*

f^{-1}	0	**1**	2	3	4	**5**
0	0	25	20	15	10	5
1	6	**1**	26	21	16	**11**
2	12	**7**	2	27	22	**17**
3	18	**13**	8	3	28	**23**
4	24	**19**	14	9	4	**29**

Die fett gedruckten Einträge bilden dann die Tabelle der Einschränkung $\hat{f}^{-1}$ von f^{-1} auf die Menge $\mathbb{Z}_5^* \times \mathbb{Z}_6^*$. Das Bild dieser Einschränkung ist genau die Menge $\mathbb{Z}_{30}^*$. ◁

Der chinesische Restsatz, den wir im nächsten Abschnitt beweisen, besagt, dass f im Fall $\mathrm{ggT}(m,\ell)=1$ bijektiv und damit invertierbar ist. Wegen

$$\begin{aligned}\mathrm{ggT}(x,m\ell)=1 &\Leftrightarrow \mathrm{ggT}(x,m)=\mathrm{ggT}(x,\ell)=1\\ &\Leftrightarrow \mathrm{ggT}(x \bmod m,m)=\mathrm{ggT}(x \bmod \ell,\ell)=1\end{aligned}$$

ist daher die Einschränkung $\hat{f}$ von f auf den Bereich $\mathbb{Z}_{m\ell}^*$ eine Bijektion zwischen $\mathbb{Z}_{m\ell}^*$ und $\mathbb{Z}_m^*\times\mathbb{Z}_\ell^*$, d.h. es gilt

$$\varphi(m\ell)=\|\mathbb{Z}_{m\ell}^*\|=\|\mathbb{Z}_m^*\times\mathbb{Z}_\ell^*\|=\|\mathbb{Z}_m^*\|\cdot\|\mathbb{Z}_\ell^*\|=\varphi(m)\varphi(\ell).$$

Satz 24. *Die Eulersche φ-Funktion ist multiplikativ, d. h. für teilerfremde Zahlen m und ℓ gilt $\varphi(m\ell)=\varphi(m)\varphi(\ell)$.*

Korollar 25. *Sei $m=\prod_{i=1}^{\ell}p_i^{k_i}$ die Primfaktorzerlegung von m. Dann gilt*

$$\varphi(m)=\prod_{i=1}^{\ell}p_i^{k_i-1}(p_i-1)=m\prod_{i=1}^{\ell}(p_i-1)/p_i.$$

Beweis. Es gilt $\varphi(\prod_{i=1}^{\ell}p_i^{k_i})=\prod_{i=1}^{\ell}\varphi(p_i^{k_i})=\prod_{i=1}^{\ell}(p_i^{k_i}-p_i^{k_i-1})=\prod_{i=1}^{\ell}p_i^{k_i-1}(p_i-1)$. □

1.6 Der chinesische Restsatz

Die beiden linearen Kongruenzen

$$\begin{aligned}x &\equiv_3 0\\ x &\equiv_6 1\end{aligned}$$

besitzen je eine Lösung, es gibt aber kein x, das beide Kongruenzen gleichzeitig erfüllt. Der nächste Satz zeigt, dass unter bestimmten Voraussetzungen gemeinsame Lösungen existieren, und wie sie berechnet werden können.

Satz 26 (Chinesischer Restsatz (CRS))**.** *Falls $m_1,\ldots,m_k$ paarweise teilerfremd sind, dann hat das System*

$$\begin{aligned}x &\equiv_{m_1} b_1\\ &\vdots\\ x &\equiv_{m_k} b_k\end{aligned}\tag{1.2}$$

für beliebige Zahlen $b_1,\ldots,b_k\in\mathbb{Z}$ genau eine Lösung modulo $m=\prod_{i=1}^{k}m_i$.

Beweis. Zu jeder Zahl $n_i=m/m_i$ existieren wegen $\mathrm{ggT}(n_i,m_i)=1$ Zahlen μ_i und λ_i mit

$$\mu_i n_i+\lambda_i m_i=\mathrm{ggT}(n_i,m_i)=1$$

Für $i=1,\ldots,k$ löst daher die Zahl $s_i=\mu_i n_i$ das System

$$x\equiv_{m_j}\begin{cases}0, & j\neq i \quad (a)\\ 1, & j=i \quad (b)\end{cases}\tag{1.3}$$

Folglich gelten für $s = \sum_{i=1}^{k} b_i s_i$ die Kongruenzen $s \overset{(1.3a)}{\equiv}_{m_j} b_j s_j \overset{(1.3b)}{\equiv}_{m_j} b_j$, d.h. s löst das System (1.2). Dies zeigt, dass die Funktion

$$f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \text{ mit } f(x) = (x \bmod m_1, \ldots, x \bmod m_k)$$

surjektiv ist. Da der Definitions- und der Wertebereich von f gleich groß sind, muss f auch injektiv sein und (1.2) ist eindeutig lösbar. □

Man beachte, dass der Beweis des chinesischen Restsatzes konstruktiv ist und die Lösung x unter Verwendung des erweiterten euklidischen Algorithmus' effizient berechnet werden kann.

Man verifiziert auch leicht, dass f ein Isomorphismus zwischen dem Ring $(\mathbb{Z}_m, \oplus_m, \odot_m)$ und dem direkten Produkt der Ringe $(\mathbb{Z}_{m_i}, \oplus_{m_i}, \odot_{m_i})$, $1 \le i \le k$, ist. Dies ist nicht nur für theoretische Überlegungen nützlich, sondern hat auch praktische Konsequenzen. Beispielsweise lässt sich dadurch die Laufzeit von bestimmten Berechnungen im Ring $\mathbb{Z}_m$ deutlich reduzieren, sofern die Primzahlzerlegung von m bekannt ist.

1.7 Die Hill-Chiffre

Die von Hill im Jahr 1929 publizierte Chiffre ist eine Erweiterung der multiplikativen Chiffre auf Buchstabenblöcke. Der Klartext wird also nicht zeichen- sondern blockweise verarbeitet. Die Blöcke haben eine feste Länge l und sowohl Klar- als auch Kryptotextraum bestehen aus allen Wörtern $x \in A^l$. Als Schlüssel dient eine $(l \times l)$-Matrix $k = (k_{ij})$ mit Koeffizienten in $\mathbb{Z}_m$. Diese transformiert einen Klartext $x = x_1 \ldots x_l \in A^l$ in den Kryptotext $y = y_1 \ldots y_l$ mit $y_i = x_1 k_{1i} + \cdots + x_l k_{li}$ für $i = 1, \ldots, l$:

$$(y_1 \ \cdots \ y_l) = (x_1 \ \cdots \ x_l) \begin{pmatrix} k_{11} & \ldots & k_{1l} \\ \vdots & \ddots & \vdots \\ k_{l1} & \ldots & k_{ll} \end{pmatrix}$$

Wir bezeichnen die Menge aller $(l \times l)$-Matrizen (k_{ij}) mit Koeffizienten $k_{ij} \in \mathbb{Z}_m$ mit $\mathbb{Z}_m^{l \times l}$. Als Schlüssel können nur invertierbare Matrizen k benutzt werden, da sonst der Chiffriervorgang nicht injektiv ist. Ob eine Matrix $k \in \mathbb{Z}_m^{l \times l}$ invertierbar ist, lässt sich an ihrer Determinante erkennen.

Definition 27 (Determinante). *Sei R ein kommutativer Ring mit Eins und sei $n \ge 1$. Eine Funktion $f : R^{n \times n} \to R$ heißt **Determinantenfunktion**, falls sie für jede Matrix $A = (a_{ij}) \in R^{n \times n}$ mit Zeilen $a_1, \ldots, a_n \in R^n$ folgende Eigenschaften erfüllt:*

- *f ist **multilinear**, d.h. für jeden Vektor $b \in R^n$ und jedes Element $r \in R$ gilt*

$$f \begin{pmatrix} a_1 \\ \vdots \\ r \cdot a_i + b \\ \vdots \\ a_n \end{pmatrix} = r \cdot f \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} + f \begin{pmatrix} a_1 \\ \vdots \\ b \\ \vdots \\ a_n \end{pmatrix}$$

- *f ist **alternierend**, d.h. im Fall $a_i = a_j$ für $i \ne j$ gilt $f(A) = 0$*
- *f ist **normiert**, d.h. $f(E) = 1$, wobei $I_n \in R^{n \times n}$ die Einheitsmatrix ist.*

Tatsächlich ist f durch diese drei Eigenschaften eindeutig festgelegt und wir bezeichnen $f(A)$ wie üblich mit $det(A)$.

Eine explizite Darstellung für die Determinantenfunktion liefert der laplacesche Entwicklungssatz. Für $1 \leq i, j \leq n$ sei A_{ij} die durch Streichen der i-ten Zeile und j-ten Spalte aus A hervorgehende Matrix. Dann ist $det(A) = a_{11}$, falls $n = 1$, und für $n \geq 2$ und $i \in [n]$ beliebig ist

$$det(A) = \sum_{j=1}^{n} a_{ij} \underbrace{(-1)^{i+j} det(A_{ij})}_{\tilde{a}_{ij}} = \sum_{j=1}^{n} a_{ji}\tilde{a}_{ji} \qquad \text{"Entwicklung nach der } i\text{-ten Zeile bzw. Spalte"}$$

Die Terme $\tilde{a}_{ij} = (-1)^{i+j} det(A_{ij})$ werden als **Kofaktoren** bezeichnet. Aus dieser Formel lässt sich zwar ein Algorithmus zur Berechnung der Determinante ableiten, allerdings hat dieser eine exponentielle Laufzeit. Mit dem Gaußschen Eliminationsverfahren lässt sich die Determinante jedoch effizient berechnen (siehe Übungen).

Für die Dechiffrierung eines mit dem Schlüssel k berechneten Kryptotextes wird die inverse Matrix k^{-1} benötigt. Invertierbare Matrizen werden auch als **regulär** bezeichnet. Eine Matrix $k \in \mathbb{Z}_m^{l \times l}$ ist genau dann regulär, wenn $\text{ggT}(det(k), m) = 1$ ist. In diesem Fall lässt sich k^{-1} mit dem Gauß-Jordan-Algorithmus effizient berechnen (siehe Übungen).