Vorlesungsskript

Kryptologie 1

Wintersemester 07/08

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

19. Oktober 2007

Inhaltsverzeichnis

1 Klassische Verfahren

1.1 Einführung

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.

Steganographische Maßnahmen: unsichtbare Tinte etc.

Andererseits können durch kryptographische 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 Kryptographie fallen auch die folgenden Begriffe.

Kryptographie: Lehre von der Geheimhaltung von Informationen durch die Verschlüsselung von Daten. 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 kryptographischen Stärken bzw. Schwächen.

Kryptologie: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptographischen Verfahren (umfasst Kryptographie 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 1.1 (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 1.2 (**Alphabet**)

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

Beispiel 1.3 Das ***lateinische Alphabet*** A_{lat} enthält die 26 Buchstaben `A,...,Z`. Bei der Abfassung von Klartexten wurde meist auf den Gebrauch von Interpunktions- und Leerzeichen sowie auf Groß- und Kleinschreibung verzichtet ($\rightsquigarrow$ Verringerung der Redundanz im Klartext).

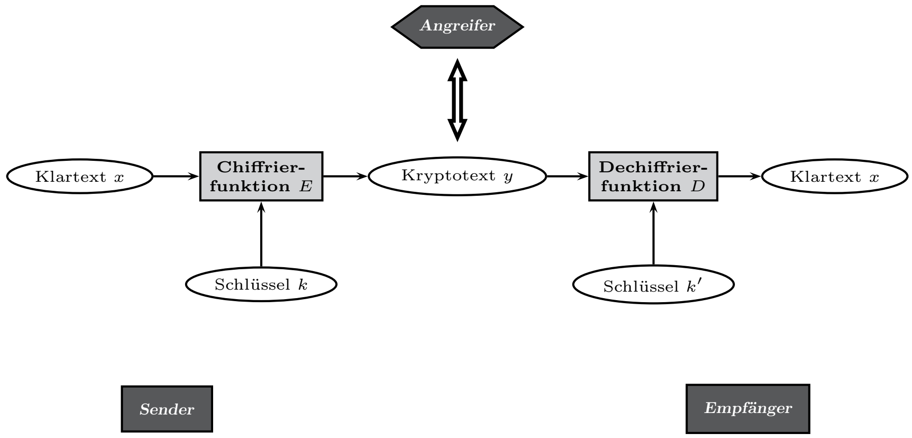
Definition 1.4 (**Kryptosystem**)

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

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

  gilt. Bei symmetrischen Kryptosystemen ist $S = \{(k, k) \mid k \in K\}$, weshalb wir 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 1.5 *Für jedes Paar $(k,k') \in S$ ist die Chiffrierfunktion E_k injektiv.*

Beweis Angenommen, für zwei unterschiedliche Klartexte $x_1 \neq x_2$ ist $E(k,x_1) = E(k,x_2)$. Dann folgt

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

im Widerspruch zu (1.1). ∎

1.3 Die affine Chiffre

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

Definition 1.6 (**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

$$a \equiv_m b$$

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

$$a \bmod m$$

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 $a = dm + r$.

Die auf $\mathbb{Z}$ definierten Operationen

$$a \oplus_m b := (a + b) \bmod m$$

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 $a \ominus_m b$.

Definition 1.7 (**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

$$\begin{array}{lll} a_i + a_j = a_{i \oplus_m j}, & a_i - a_j = a_{i \ominus_m j}, & a_i a_j = a_{i \odot_m j}, \\ a_i + z \;= a_{i \oplus_m z}, & a_i - z \;= a_{i \ominus_m z}, & z a_j \;= a_{z \odot_m j}. \end{array}$$

Wir rechnen also mit Buchstaben, indem wir sie mit ihren Indizes identifizieren und die Rechnung modulo m ausführen. Mit Hilfe dieser Notation lässt sich die Verschiebechiffre, die auch als additive Chiffre bezeichnet wird, leicht beschreiben.

Definition 1.8 (**additive Chiffre**)

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

$$E(k, x) = x + k \;\text{ und }\; D(c, y) = y - k.$$

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. Natürlich kann mit dieser Substitution nicht ernsthaft die Vertraulichkeit von Nachrichten geschützt werden. Vielmehr

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*

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

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

Da ROT13 zudem keinen Buchstaben auf sich selbst abbildet, ist sie sogar eine echt involutorische Abbildung.

Die Buchstabenrechnung legt folgende Modifikation der Caesar-Chiffre nahe: Anstatt auf jeden Klartextbuchstaben den Schlüsselwert k zu addieren, können wir die Klartextbuchstaben 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 den Buchstaben $g(\mathtt{A}) = g(\mathtt{N}) = \mathtt{A}$ ab. Um die vom Schlüsselwert k zu erfüllende Bedingung angeben zu können, führen wir folgende Begriffe ein.

Definition 1.9 (**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. 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***.

Euklidscher 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):

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

mit

$$r_{i-1} = d_{i+1} r_i + r_{i+1} \quad \text{für} \quad i = 1, \ldots, n.^*$$

Hierzu sind n 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 $\mathrm{ggT}(a, b) = \mathrm{ggT}(r_n, r_{n+1}) = r_n$.

Beispiel 1.10

Für $a = 693$ und $b = 147$ erhalten wir z. B.

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

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

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

Algorithmus 1.11 $\textsc{Euklid}_{it}(a, b)$

repeat
  $r \leftarrow a \bmod b$
  $a \leftarrow b$
  $b \leftarrow r$
until $r = 0$
return a

Algorithmus 1.12 $\textsc{Euklid}_{rek}(a, b)$

if $b = 0$ **then**
  return a
else
  return $\textsc{Euklid}(b,\ a \bmod b)$
end

Zur Abschätzung von n 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 $i = n, n-1, \ldots, 0$ folgt $r_i \geq f_{n+1-i}$; also $a \geq f_{n+1}$. Wegen $f_n \geq \Re^n$ (wobei $\Re = \frac{1+\sqrt{5}}{2}$; Beweis durch Induktion) ist dann $a \geq \Re^n$, d. h. $n \leq \log_{\Re} a$.

---

[*]Also: $d_i = r_{i-2}$ div r_{i-1} und $r_i = r_{i-2} \bmod r_{i-1}$.

Theorem 1.13 *Der Euklidsche Algorithmus führt zur Berechnung von* $\mathrm{ggT}(a,b)$ *(unter der Annahme* $a > b > 0$*) höchstens* $\lfloor \log_R a \rfloor + 1$ *Divisionsschritte durch. Dies führt auf eine Zeitkomplexität von* $O(n^3)$*, wobei* n *die Länge der Eingabe in Binärdarstellung bezeichnet und wir* $O(n^2)$ *Rechenschritte für eine einzelne Ganzzahldivision ansetzen.*

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

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

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

$$p_i = p_{i-2} - d_i p_{i-1}, \quad \text{wobei} \quad p_0 = 1 \quad \text{und} \quad p_1 = 0,$$

und

$$q_i = q_{i-2} - d_i q_{i-1}, \quad \text{wobei} \quad q_0 = 0 \quad \text{und} \quad q_1 = 1,$$

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

$$ap_i + bq_i = r_i,$$

und durch Induktion über i,

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

zeigt man, dass dies auch für $i = 2, \ldots, n$ gilt.

Korollar 1.14 (Lemma von Bezout) *Der größte gemeinsame Teiler von* a *und* b *ist in der Form*

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

darstellbar.

Beispiel 1.15 Für $a = 693$ und $b = 147$ erhalten wir z. B. mit

i	r_{i-1}	$=$	$d_{i+1} \cdot$	r_i	$+\ r_{i+1}$	$p_i \cdot 693\ +$	$q_i \cdot 147$	$=$	r_i
0						$1 \cdot 693\ +$	$0 \cdot 147$	$=$	693
1	693	$=$	4	$\cdot 147\ +$	105	$0 \cdot 693\ +$	$1 \cdot 147$	$=$	147
2	147	$=$	1	$\cdot 105\ +$	42	$1 \cdot 693\ +$	$(-4) \cdot 147$	$=$	105
3	105	$=$	2	$\cdot\ 42\ +$	21	$(-1) \cdot 693\ +$	$5 \cdot 147$	$=$	42
4	42	$=$	2	$\cdot\ \mathbf{21}\ +$	0	$\mathbf{3} \cdot 693\ +$	$(\mathbf{-14}) \cdot 147$	$=$	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 1.16

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

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

Korollar 1.17 *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 Sei $g = \mathrm{ggT}(a,b)$. Dann existieren Zahlen $\mu, \lambda \in \mathbb{Z}$ mit $\mu a + \lambda b = g$. Da x nach Voraussetzung sowohl a als auch b teilt, teilt x auch die Zahlen μa und λb und somit auch deren Summe $\mu a + \lambda b = g$. ■

Korollar 1.18 (Lemma von Euklid) *Teilt a das Produkt bc und sind a, b teilerfremd, so ist a auch Teiler von c,*

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

Beweis Wegen $\mathrm{ggT}(a,b) = 1$ existieren Zahlen $\mu, \lambda \in \mathbb{Z}$ mit $\mu a + \lambda b = 1$. Da a nach Voraussetzung das Produkt bc teilt, muss a auch $c\mu a + c\lambda b = c$ teilen. ■

Korollar 1.19 *Wenn sowohl a als auch b zu einer Zahl $m \in \mathbb{Z}$ teilerfremd sind, so ist auch das Produkt ab teilerfremd zu m,*

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

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

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

dass auch ab teilerfremd zu m ist. ■

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

Satz 1.20 *Sei $m \geq 1$. 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 $x \not\equiv_m x'$. Gilt umgekehrt $\mathrm{ggT}(b, m) = 1$, so folgt aus den Kongruenzen

$$bx_1 \equiv_m y$$

und

$$bx_2 \equiv_m y$$

sofort $m|(bx_1 - y)$ und $m|(bx_2 - y)$, 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 $x_1 \equiv_m x_2$. Dies zeigt, dass die Abbildung $f : \mathbb{Z}_m \to \mathbb{Z}_m$ mit $f(x) = bx \bmod m$ injektiv ist. Da jedoch Definitions- und Wertebereich von f identisch sind, muss f dann auch surjektiv sein. Dies impliziert, dass die Kongruenz $bx \equiv_m y$ für jedes $y \in \mathbb{Z}_m$ lösbar ist. ■

Korollar 1.21 *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. Die invertierbaren Elemente von $\mathbb{Z}_m$ werden in der Menge*

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

zusammengefasst.

Korollar 1.19 zeigt, dass $\mathbb{Z}_m^*$ unter der Operation $\odot_m$ abgeschlossen ist, und mit Korollar 1.21 folgt, dass $(\mathbb{Z}_m^*, \odot_m)$ eine multiplikative Gruppe bildet.

Das multiplikative Inverse von b modulo m ergibt sich aus der linearen Darstellung $\lambda b + \mu m = \mathrm{ggT}(b, m) = 1$ zu $b^{-1} = \lambda \bmod m$. Bei Kenntnis von b^{-1} kann die Kongruenz $bx \equiv_m y$ leicht zu $x = yb^{-1} \bmod m$ gelöst werden. Die folgende Tabelle zeigt die multiplikativen Inversen b^{-1} für alle $b \in \mathbb{Z}_{26}^*$.

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

Nun lässt sich die additive Chiffre leicht zur affinen Chiffre erweitern.

Definition 1.22 (**affine Chiffre**)

Bei der ***affinen Chiffre*** ist $A = B = M = C$ ein beliebiges Alphabet mit $m := \|A\| > 1$ 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 eine involutorische Chiffrierfunktion $x \mapsto E(b, c; x) = c - x$ (**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
$-x-1$	*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 1.23 (affine Chiffre)

Sei $A = \{\mathtt{A}, \ldots, \mathtt{Z}\} = B$, also $m = 26$. Weiter sei $k = (9, 2)$, also $b = 9$ und $c = 2$. Um den Klartextbuchstaben $x = \mathtt{F}$ zu verschlüsseln, berechnen wir

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

da der Index von F gleich 5, der von *V* gleich 21 und $9 \cdot 5 + 2 = 47 \equiv_{26} 21$ ist. Um einen Kryptotextbuchstaben 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 $b^{-1} = q_2 = 3$ ergibt. Damit erhalten wir für den Kryptotextbuchstaben $y = \mathtt{V}$ den ursprünglichen Klartextbuchstaben

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

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

Eine wichtige Rolle spielt die Funktion

$$\varphi : \mathbb{N} \to \mathbb{N} \quad \text{mit} \quad \varphi(m) = \|\mathbb{Z}_m^*\| = \|\{a \mid 0 \leq a \leq m-1,\ \mathrm{ggT}(a, m) = 1\}\|,$$

die sogenannte *Eulersche φ-Funktion.*

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

Wegen

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

folgt sofort

$$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1).$$

Um hieraus für beliebige Zahlen $m \in \mathbb{N}$ eine Formel für $\varphi(m)$ zu erhalten, genügt es, $\varphi(ab)$ im Fall $\mathrm{ggT}(a, b) = 1$ in Abhängigkeit von $\varphi(a)$ und $\varphi(b)$ 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 1.24

Sei $m = 3$ und $l = 7$. Dann erhalten wir die Funktion $f : \mathbb{Z}_{21} \to \mathbb{Z}_3 \times \mathbb{Z}_7$ mit

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

10	**11**	12	**13**	14	15	**16**	**17**	18	**19**	**20**
(**1**, **3**)	(**2**, **4**)	(0, **5**)	(**1**, **6**)	(**2**, 0)	(0, **1**)	(**1**, **2**)	(**2**, **3**)	(0, **4**)	(**1**, **5**)	(**2**, **6**)

Die **fett** gedruckten Werte gehören zu $\mathbb{Z}_{21}^*$, $\mathbb{Z}_3^*$ bzw. $\mathbb{Z}_7^*$. Man beachte, dass ein x-Wert genau dann in $\mathbb{Z}_{21}^*$ ist, wenn beide Komponenten von $f(x)$ zu $\mathbb{Z}_3^*$ bzw. $\mathbb{Z}_7^*$ gehören. $\triangleleft$

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

f^{-1}	0	1	2	3	4	5	6
0	0	15	9	3	18	12	6
1	7	1	16	10	4	19	13
2	14	8	2	17	11	5	20

Wegen

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

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

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

Theorem 1.25 *Die Eulersche φ-Funktion ist multiplikativ, d. h. für teilerfremde Zahlen m und l gilt $\varphi(ml) = \varphi(m)\varphi(l)$.*

Korollar 1.26 *Sei $m = \prod_{i=1}^{k} p_i^{e_i}$ die Primfaktorzerlegung von m. Dann gilt*

$$\varphi(m) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1).$$

Beweis Es gilt

$$\varphi(\textstyle\prod_{i=1}^{k} p_i^{e_i}) = \prod_{i=1}^{k} \varphi(p_i^{e_i}) = \prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1}) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1).$$

■