Vorlesungsskript

Einführung in die Kryptologie

Wintersemester 2015/16

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

15. Oktober 2015

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.

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 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 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 (**Alphabet**)**.** *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 $A^* = \bigcup_{n \geq 0} A^n$.*

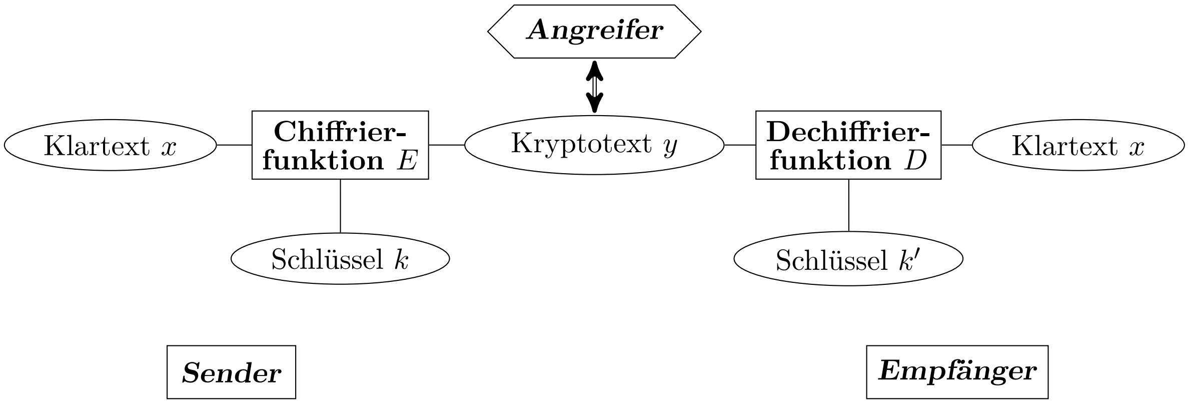
Beispiel 3. *Das **lateinische Alphabet** A_{lat} enthält die 26 Buchstaben `A,...,Z`. Bei der Abfassung von Klartexten wurde meist auf den Gebrauch von Interpunktions- und Leerzeichen sowie auf Groß- und Kleinschreibung verzichtet ($\rightsquigarrow$ Verringerung der Redundanz im Klartext).* ◁

Definition 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 $x \in M$ 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 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 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*

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

*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

$$a \odot_m b := ab \bmod m.$$

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*

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 $a \ominus_m b$.

Durch Identifikation der Buchstaben a_i 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*

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

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

Definition 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*

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

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 (siehe Tabelle 1.1). Natürlich kann mit dieser Substitution nicht ernsthaft die Vertraulichkeit von Nachrichten geschützt 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

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

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

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

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

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

*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. □

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):

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

mit

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

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	· 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.

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

```
repeat
   r := a mod b
   a := b
   b := r
until r = 0
return a
```

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

```
if b = 0 then
   return a
else
   return Euklid_rek(b, a mod b)
```

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

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

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

Durch Induktion über $i = s, s-1, \ldots, 0$ folgt $r_i \geq F_{s+1-i}$; also $a = r_0 \geq F_{s+1}$. 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. *Der Euklidsche Algorithmus führt $O(n)$ Divisionsschritte zur Berechnung von* $\mathrm{ggT}(a,b)$ *durch, wobei n die Länge der Eingabe $a > b > 0$ in Binärdarstellung bezeichnet. Dies führt auf eine Zeitkomplexität von $O(n^3)$, da jede Ganzzahldivision in Zeit $O(n^2)$ durchführbar ist.*

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 $i = 2, \ldots, s$ gilt. Insbesondere gilt also

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

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

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

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

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 16. *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 17 (Lemma von Euklid)**.** *Teilt a das Produkt bc und sind a, b teilerfremd, so teilt a auch 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 $\mu a + \lambda b = 1$. Falls a das Produkt bc teilt, muss a auch die Zahl $c\mu a + c\lambda b = c$ teilen. □

Korollar 18. *Wenn a und b zu einer Zahl $m \in \mathbb{Z}$ teilerfremd sind, so ist auch das Produkt ab teilerfremd zu m,*

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