

Vorlesungsskript  
Einführung in die Kryptologie  
Wintersemester 2011/12

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

*19. Oktober 2011*

# Inhaltsverzeichnis

<b>1</b>	<b>Klassische Verfahren</b>	<b>1</b>
1.1	Einführung . . . . .	1
1.2	Kryptosysteme . . . . .	1
1.3	Die affine Chiffre . . . . .	3



# 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).

---

<b>xve</b>	<i>Bis auf weiteres Wettermeldung gemäß Funkbefehl testen</i>
<b>yde</b>	<i>Frage</i>
<b>sLk</b>	<i>Befehl</i>
<b>fin</b>	<i>beendet</i>
<b>eom</b>	<i>eigene Maschinen</i>

---

◁

## Kryptosysteme

- operieren auf syntaktischen Einheiten,
- flexibler Mechanismus durch Schlüsselvereinbarung

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

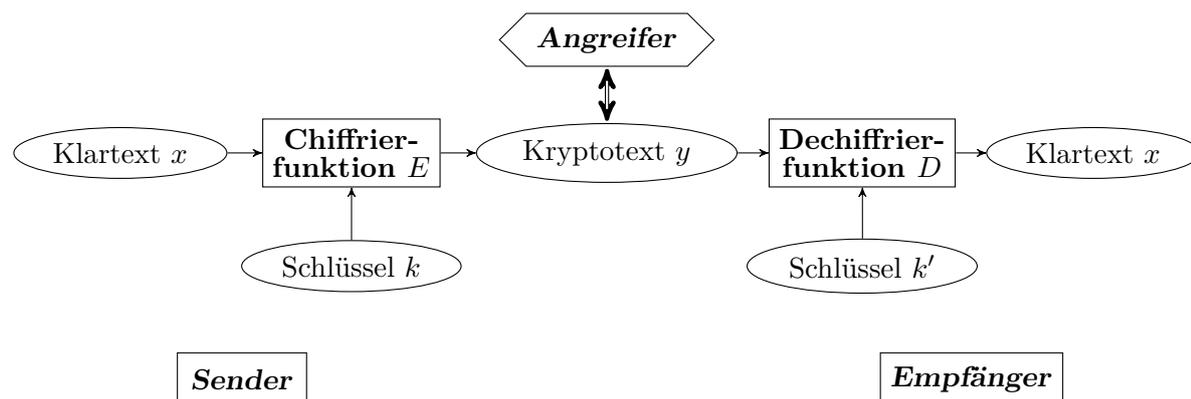
**Beispiel 3.** Das **lateinische Alphabet**  $A_{lat}$  enthält die 26 Buchstaben **A, ..., Z**. Bei der Abfassung von Klartexten wurde meist auf den Gebrauch von Interpunktions- und Leerzeichen sowie auf Groß- und Kleinschreibung verzichtet ( $\leadsto$  Verringerung der Redundanz im Klartext). ◁

**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),
- $E : K \times M \rightarrow C$ , die **Verschlüsselungsfunktion** (encryption function),
- $D : K \times C \rightarrow M$ , 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

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

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  $r \in \{0, \dots, m-1\}$ , 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  $\mathbb{Z}_m = \{0, \dots, m-1\}$  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  $A = \{a_0, \dots, a_{m-1}\}$  ein Alphabet. Für Indizes  $i, j \in \{0, \dots, m-1\}$  und eine ganze Zahl  $z \in \mathbb{Z}$  ist

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

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  $K = \{1, \dots, m-1\}$ . Für  $k \in K$ ,  $x \in M$  und  $y \in C$  gilt

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

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 1.3). 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

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

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  $g : A_{\text{lat}} \rightarrow A_{\text{lat}}$  mit  $g(x) = 2x$  sowohl **A** als auch **N** auf den Buchstaben  $g(\mathbf{A}) = g(\mathbf{N}) = \mathbf{A}$  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

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

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

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

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

**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 Division mit Rest):

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

mit

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

Hierzu sind  $n$  Divisionsschritte erforderlich. Wegen

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

folgt  $\text{ggT}(a, b) = \text{ggT}(r_n, r_{n+1}) = r_n$ .

---

\*Also:  $d_i = r_{i-2} \text{ div } r_{i-1}$  und  $r_i = r_{i-2} \text{ mod } r_{i-1}$ .