1.1 Begriffe

Kryptologie umfasst

Kryptographie – Verschlüsselung von Nachrichten, sodass nur der berechtigte Empfänger diese entschlüsseln kann,

Kryptanalyse – Analyse verschlüsselter Nachrichten mit dem Ziel der unberechtigten Entschlüsselung,

Steganographie – Verstecken einer Nachricht, um deren Existenz (und nicht nur ihren Inhalt) geheim zu halten.

Die *Codierung* hingegen umfasst allgemeiner die Repräsentation von Nachrichten/Information. Eine Codierung kann dazu dienen, dem unberechtigten Empfänger das Lesen zu erschweren, kann aber auch anderen Zwecken dienen.

1.2 Literaturhinweise

- Friedrich L. Bauer: Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie
- Bruce Schneier: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C
- Johannes Buchmann: Einführung in die Kryptographie
- Simon Singh: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet

1.3 Einführendes Beispiel

```
QVRF VFG RVAR FGERAT TRURVZR ANPUEVPUG
```

Häufigkeitsverteilung der Buchstaben:

A	E	F	G	N	P	Q	R	T	U	V	Z
3	2	3	3	1	2	1	7	2	3	5	1

- weicht stark ab von der der Sprache, in der die Nachricht vermutlich verfasst wurde (Deutsch, evtl. Englisch)

⇒ Wir vermuten zunächst eine einfache Zeichenersetzung.

- Annahme: häufigster Buchstabe (R) im Original ein e:

```
QVeF VFG eVAe FGEeAT TeUeVZe ANPUEVPUG
```

- drittes Wort vermutlich eine, also V=i und A=n:

```
QieF iFG eine FGEenT TeUeiZe nNPUEiPUG
```

- zweites Wort vermutlich ist, also F=s und G=t:

```
Qies ist eine stEenT TeUeiZe nNPUEiPUt
```



```
Qies ist eine stEenT TeUeiZe nNPUEiPUt
```


- erstes und viertes Wort vermutlich dies und streng, also Q=d, E=r und T=g:

```
dies ist eine streng geUeiZe nNPUriPUt
```

- wir erkennen geheime, also U=h und Z=m:

```
dies ist eine streng geheime nNPhriPht
```

- schließlich mit N=a und P=c:

```
dies ist eine streng geheime nachricht
```

- Die Vorschrift zur Entschlüsselung lässt sich in einer Tabelle zusammenfassen:

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
n	?	?	?	r	s	t	?	?	?	?	?	?	a	?	c	d	e	?	g	h	i	?	?	?	m

- Beachte symmetrische Paare A=n und N=a, E=r und R=e sowie G=t und T=g.
- Fortsetzung dieser Symmetrie ergibt:

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
n	?	p	q	r	s	t	u	v	?	?	?	z	a	?	c	d	e	f	g	h	i	?	?	?	m

- schließlich naheliegende Ergänzung zu

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
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

- Damit können alle zukünftigen Nachrichten, die dasselbe Verschlüsselungsverfahren nutzen, entziffert werden.
- bekannt als ROT13
  - Verwendung, um unbeabsichtigtes Lesen zu verhindern – ähnlich wie kopfüber gesetzte Lösungen in Rätselheften

1.4 Formalisierung

- Der *Klartext* besteht aus Zeichen des *Klartextzeichenvorrats* V.
  - im Beispiel $V = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots, \mathtt{z}\}$
  - bei modernen digitalen Verfahren $V = \{0, 1\}$
- Der *Geheimtext* besteht aus Zeichen des *Geheimtextzeichenvorrats* W.
  - im Beispiel $W = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}\}$
  - bei modernen digitalen Verfahren $W = \{0, 1\}$
- häufig $V = W$; in dieser Vorlesung i.d.R. V und W wie oben zur einfachen Unterscheidung Klartext/Geheimtext
- V^* und W^* sind alle Folgen von Klartext- bzw. Geheimtextzeichen (*Klartextraum* und *Geheimtextraum*)
- *Chiffrierung* (Verschlüsselung) $\mathbf{X}$ ist eine i.d.R. linkstotale Relation $\mathbf{X} \subset V^* \times W^*$
  - häufig, aber nicht immer, auch funktional (rechtseindeutig) $\mathbf{X} : V^* \longrightarrow W^*$
  - andernfalls heißen die y, sodass $(x, y) \in \mathbf{X}$, *Homophone* von x
- *Dechiffrierung* (Entschlüsselung) $\mathbf{X}^{-1}$ ist die konverse Relation $\mathbf{X}^{-1} \subset W^* \times V^*$
  - eindeutig, wenn $\mathbf{X}$ injektiv (linkseindeutig)

$\Rightarrow$ Meistens ist die Chiffrierung eine injektive Funktion $\mathbf{X} : V^* \longrightarrow W^*$, die Dechiffrierung die zugehörige Umkehrfunktion $\mathbf{X}^{-1}$.

- Chiffrierung ist *involutorisch*, falls $\mathbf{X} = \mathbf{X}^{-1}$