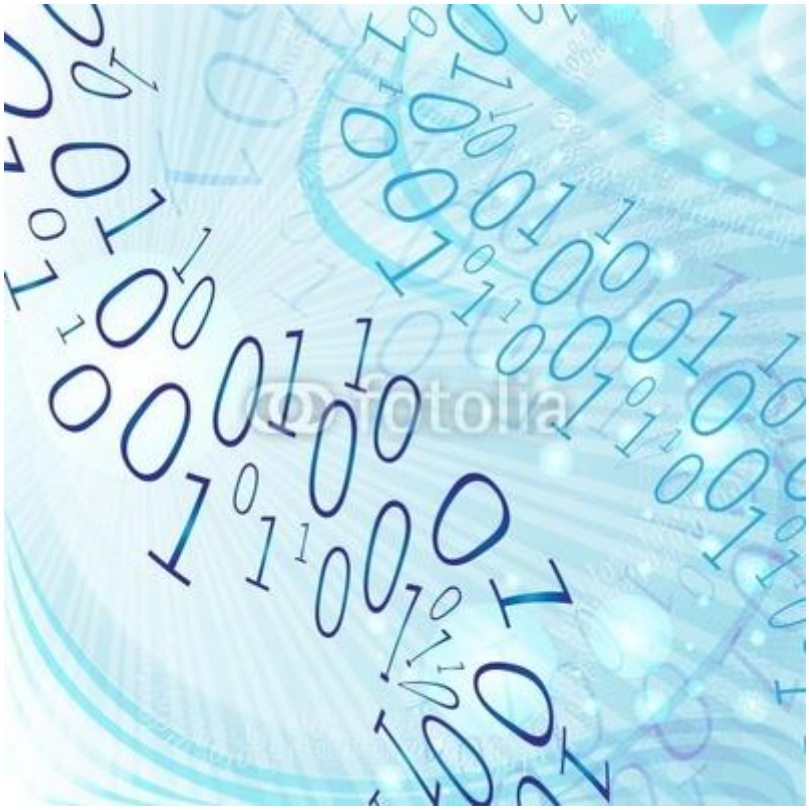
Kryptologie



Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich ausschließlich auf die Geheimhaltung des Schlüssels.

Kerckhoffs' Prinzip

Züricher Hochschule für angewandte Wissenschaften

FS2012 – Software Projekt 2

Gruppe 10 – Miro Ljubicic & Mathias Weigert

Inhaltsverzeichnis

Theoretische Grundlagen

Um Irritationen zu vermeiden erst einmal eine wichtige Definition. Wir werden in diesem Skript und auch im Programm immer wieder auf verschlüsselte Texte/Wörter zurück greifen müssen und auch auf die unverschlüsselte Bedeutung. Da es sich allgemein durchgesetzt hat, werden wir ebenfalls den unverschlüsselten Text immer klein schreiben und den chiffrierten Text immer gross.

Beispiel

```
grundlagen
QBEXNVKQOX
```

Monoalphabetische Chiffrierung

Caesar-Chiffre (Verschiebe-Chiffre)

Der Caesar-Chiffre ist eines der ältesten Verschlüsslungsverfahren. Es zeichnet sich dadurch aus, das man ein Buchstabe des Alphabetes als Schlüssel nimmt und das Alphabet dann um X Stellen verschiebt.

Dieser Chiffre ist extrem einfach und ohne grossen Aufwand zu entschlüsseln. Da nur 26 Schlüssel existieren (Anzahl der Buchstaben im Alphabet).

Beispiel

```
Yippie Ya Yeah Schweinebacke
KUBBUQ KM KQMT EOTIQUZQNMOWQ
```

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

Substitutions-Chiffre

Polyalphabetische Chiffrierung

Vigenère-Chiffre

Quellenangabe

📖 **KRYPTOLOGIE – ALGEBRAISCHE METHODEN UND ALGORITHMEN**
(Christian Karpfinger ¦ Hubert Kiechle)
📖