

Wanted!



Abbildung 1: Wer ist das?

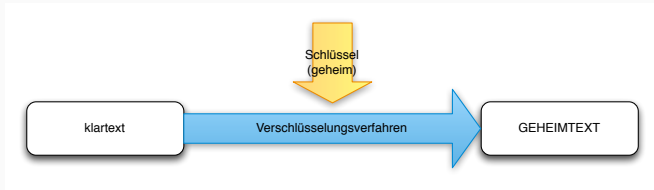
- Internetüberwachung durch amerikanische und britische Geheimdienste
  - “Anzapfen” von Kabeln
  - “Kooperation” mit großen IT-Dienstleistern/-unternehmen
- Enthüllt durch Ex-CIA-Mitarbeiter **Edward Snowden**
  - Lebt seither im Exil in Russland

- Politisch:
  - Nahezu keine
- Persönlich:
  - Will man sich vor Überwachung schützen?
  - Kann man sich vor Überwachung schützen?

- Wie lassen sich Informationen vor unbefugtem Zugriff schützen?
  - “Verstecken” → Steganographie
  - “Unlesbar machen” → Verschlüsselung

# Verschlüsselung

---



**Abbildung 2:** Allgemeiner Ablauf einer Verschlüsselung. Konvention: Klartext in Kleinbuchstaben, Geheimtext in Großbuchstaben

- Der **klartext** wird mittels eines geheimen **Schlüssels** zum **GEHEIMTEXT** **verschlüsselt**
- Aus dem **GEHEIMTEXT** kann man den **klartext** mittels des geheimen Schlüssels wieder **entschlüsseln**

- Die Sicherheit eines Verschlüsselungsverfahrens darf **nicht** auf der Geheimhaltung des Algorithmus basieren, sondern ausschließlich auf der Geheimhaltung des Schlüssels
- Wieso?
  - Algorithmen sind schwer geheim zu halten
  - Algorithmen sind schwer austauschbar
  - Algorithmen sollen überprüft werden können
  - ...

**Kryptologie** Überbegriff für

**Kryptographie** Erforschung von Verfahren zur  
Verschlüsselung bzw. allgemein zum Schutz  
von Daten

**Kryptoanalyse** Erforschung von Methoden zum “Knacken”  
von Verschlüsselungen

- Das unbefugte “Knacken” einer Verschlüsselung bezeichnet man auch als **Entziffern** (im Gegensatz zum rechtmäßigen Entschlüsseln)



- Das Bedürfnis nach “sicherer” Kommunikation ist schon sehr alt:
  - Skytale (um 500 v. Chr.)



- Cäsar-Verschlüsselung

- Grundidee:
  - Lege eine bestimmte Zahl zur Verschiebung fest
  - “Verschiebe” dann jeden Buchstaben des Klartexts um diese Zahl im Alphabet weiter
- Cäsar wählte angeblich eine Verschiebung um 3
  - Aus “hallo” wird “KDOOR”
- Die Entschlüsselung erfolgt durch eine Verschiebung um die gleiche Zahl in die umgekehrte Richtung

- **Monoalphabetisches** Verfahren
  - Es gibt genau ein Alphabet für den Geheimtext, nämlich das verschobene “Originalalphabet”
- **Monographisches** Verfahren
  - Die Verschlüsselung erfolgt zeichenweise
- **Substitutionsverfahren**
  - Zeichen aus dem Klartext werden durch andere Zeichen ersetzt

- Verschlüsse eine kurze (!) Nachricht mittels Cäsar-Verschlüsselung
  - Tausche die Nachricht mit einem Mitschüler
  - Entschlüsselt die so erhaltene Nachricht (der Schlüssel muss bekannt sein!)
- Hilfestellung:
  - 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

- Das Verfahren ist nicht sonderlich sicher
- Welche Möglichkeiten hat man, einen cäsar-verschlüsselten Geheimtext zu “knacken”?
  - Durchprobieren aller Schlüssel (**Brute Force**)
  - Suchen von “auffälligen” Wörtern
  - Häufigkeitsanalyse

- Schreibe ein Programm, das alle möglichen Verschiebungen zu einem gegebenen String erzeugt und anzeigt
  - Konvertiere den String zunächst vollständig in Groß- oder Kleinbuchstaben
- Verwende das Programm, um eine abgefangene<sup>1</sup> Botschaft eines Mitschülers zu entziffern (also zu “knacken”)

---

<sup>1</sup>Bitte nur gewaltfrei abfangen...

- Mit Variablen vom Typ `char` kann man rechnen:
  - `(char)('A'+1)` ergibt bspw. das Zeichen `'B'` usw.
- Die Methode `Math.floorMod(int dividend, int divisor)` könnte hilfreich sein:
  - Für positive Zahlen äquivalent zu `dividend % divisor`, für negative jedoch unterschiedlich
  - Beispiel: `Math.floorMod(-2, 20)` ergibt 18 (`-2 % 20` ergibt hingegen -2)

- Beobachtung: Buchstaben treten (in einer bestimmten Sprache) mit sehr unterschiedlicher Häufigkeit auf
- Beispiel (Deutsch):
  - Häufigster Buchstabe: "e" (ca. 17,4%)
  - Zweithäufigster Buchstabe: "n"
- Idee:
  - Untersuche die Buchstabenhäufigkeiten im Geheimtext
  - Schließe daraus auf die Verschiebung



## Aufgabe 3

- Entziffere den folgenden Geheimtext mittels Häufigkeitsanalyse:

KHZ LUAZJOSBLZZLSU NLOLPTLY ALEAL PZA LPUL UPJOA PTTLY NHUG  
LPUMHJOL HBMNHIL ILP JHLZHY NLOA LZ QLKVJO YLSHAPC NBA

- Häufigkeitsverteilung (Deutsch):

a	b	c	d	e	f	g	h	i	j	k	l	m
6,51	1,89	3,06	5,08	17,40	1,66	3,01	4,76	7,55	0,27	1,21	3,44	2,53

n	o	p	q	r	s	t	u	v	w	x	y	z
9,78	2,51	0,79	0,02	7,00	7,27	6,15	4,35	0,67	1,89	0,03	0,04	1,13

- **Jede** monoalphabetische Verschlüsselung ist anfällig für Angriffe mittels Häufigkeitsanalyse
  - Grund: Ein bestimmter Buchstabe aus dem Klartext wird immer zum gleichen Buchstaben im Geheimtext
- Die Häufigkeitsanalyse wurde im arabischen Raum entdeckt
  - Erste Erwähnung: 9. Jahrhundert nach Christus (!) durch Abu al-Kindi
- Es entstand die Notwendigkeit für bessere Verschlüsselungsverfahren

- Schreibe ein Programm, das die Häufigkeit eines jeden Buchstabens in einem String ermittelt und ausgibt
- Entziffere den folgenden Geheimtext mit Hilfe dieses Programms:

IXF MYJ XDFY IYKYSNYHWFYJ WHPI MGPI YHSNXD EYLUYLYUYS TSM STS  
WGDDYS WYHSY LYHWFYJ XTPI SXPI NYHSYN EHDDYS DYUYS

- Vorsicht: Der Text ist nicht cäsar-verschlüsselt