Modul 114

Thema 10/11

Verschlüsselung – Geschichte und Grundsätzliches

Agenda

Thema	Inhalte
1	Zahlensysteme BIN - DEZ - HEX
2	Arithmetische und logische Grundoperationen im Binärsystem
3	Die Logik und den Prozessor verstehen
4	Grosse Zahlen in kleinen Variablen ablegen
5	Fehler in der Datenübertragung finden und korrigieren
6	Speicherplatz als rares Gut - Dateien und ihr Platzbedarf
7	Speicherplatz als rares Gut - Kompression
8	Speicherplatz als rares Gut - Reduktion
9	Vektorgrafiken - Eine Alternative zu den Pixeln
10	Verschlüsselung - Geschichte und Grundsätzliches
11	Verschlüsselung – Moderne Verfahren

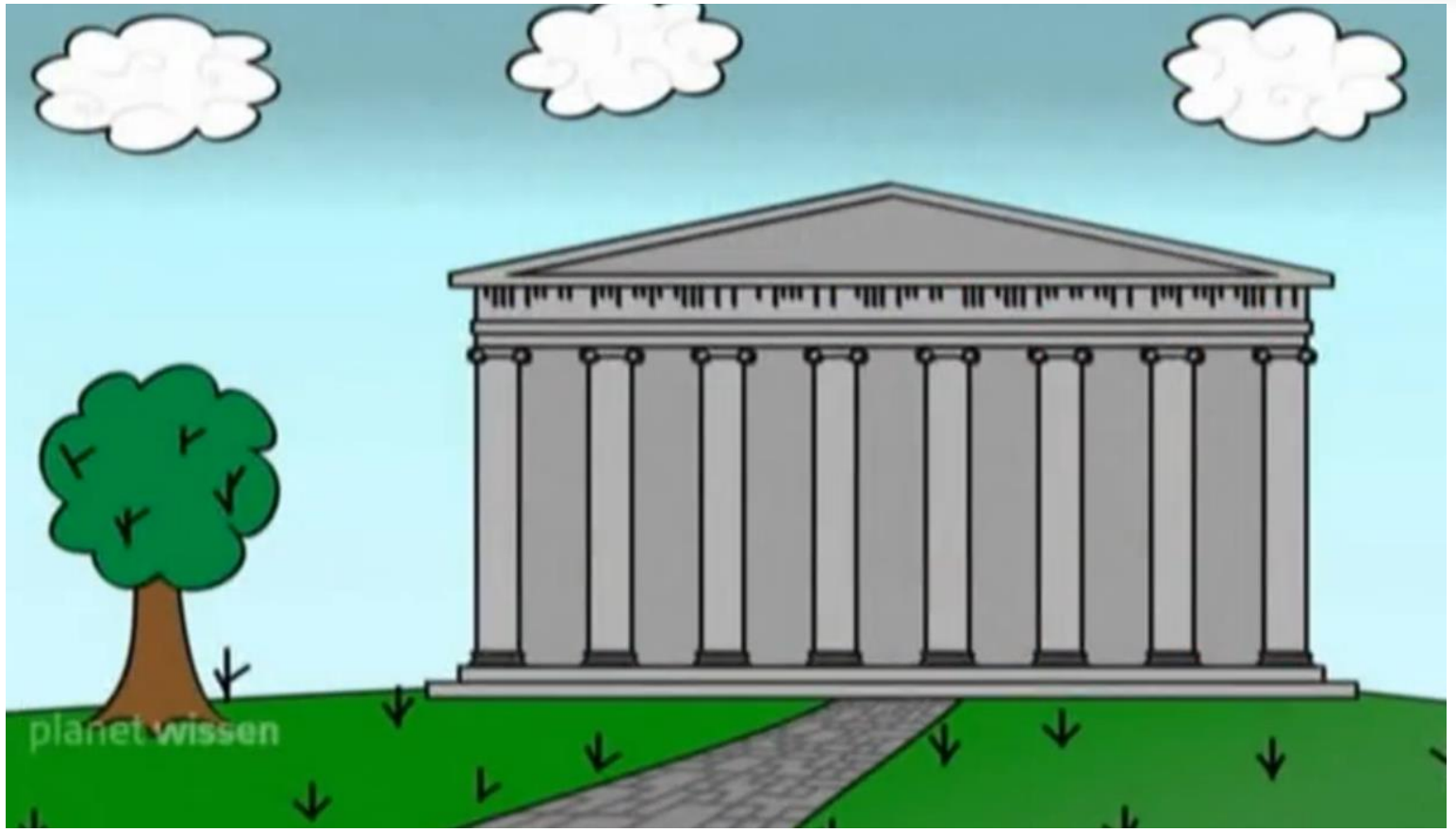
Tagesziele

Ich kann...

- den Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung erklären.
- den Begriff «Steganographie» erklären.
- exemplarisch monoalphabetische Chiffren dechiffrieren.

Einstiegsaufgabe

Aufgabe zum Einstieg



Lösung


J D I XFJTT EBTT JDI OJDIVT XFJTT


ICH WEISS DASS ICH NICHTS WEISS

Grundsätzliches

Drei Schutzziele bezüglich Informationsübertragung

Ziel: Information sicher übertragen

«Sicher» heisst in diesem Sinne:

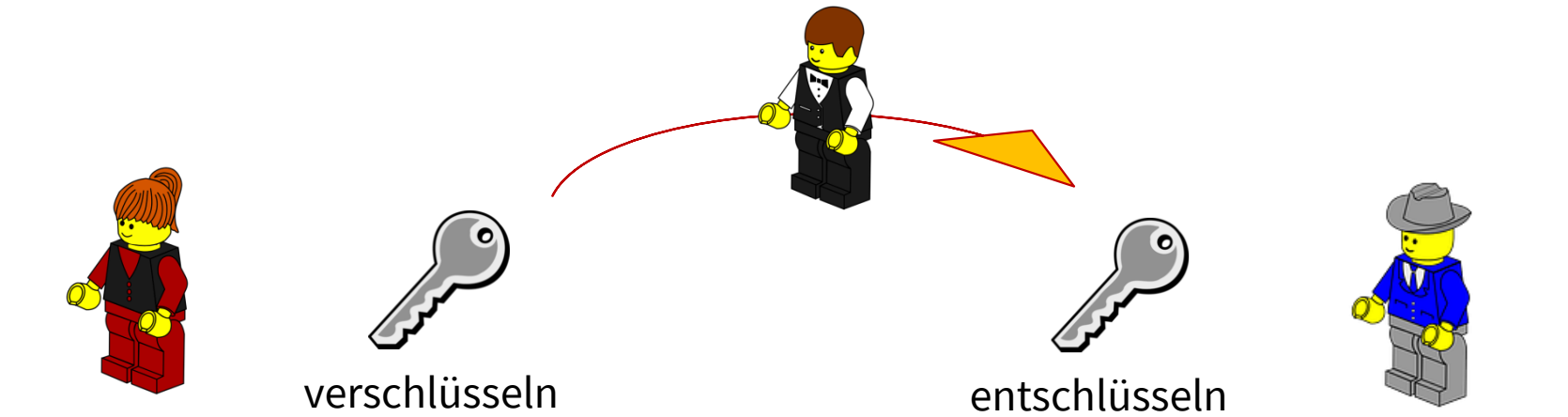
- Vertraulichkeit (Confidentiality)
  Inhalte können von unbefugten nicht eingesehen werden
  (sichere Verschlüsselung)

- Integrität (Integrity)
  Die Inhalte sind unverfälscht und vollständig
  (gute Hash-Funktion)

- Authentizität (Authenticity)
  Sender und Empfänger einander klar bekannt sein
  (gute digitale Signatur-Funktion)

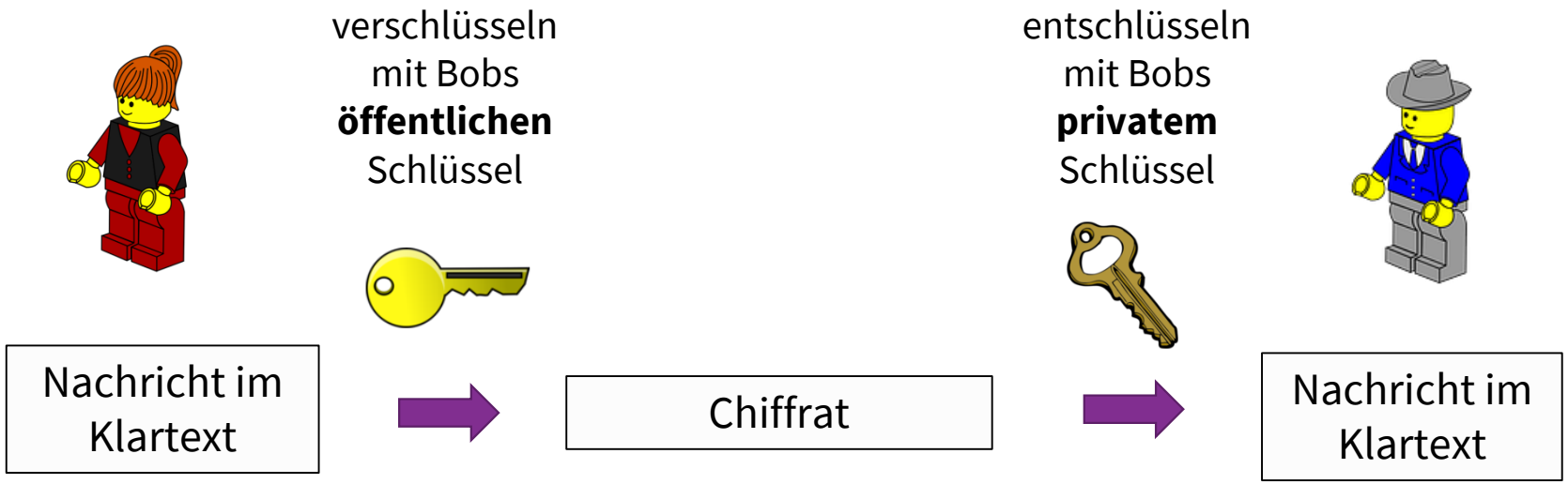
Symmetrische Verfahren

Vorteil: Schnell
Nachteil: Schlüssel muss letztlich unverschlüsselt übermittelt werden

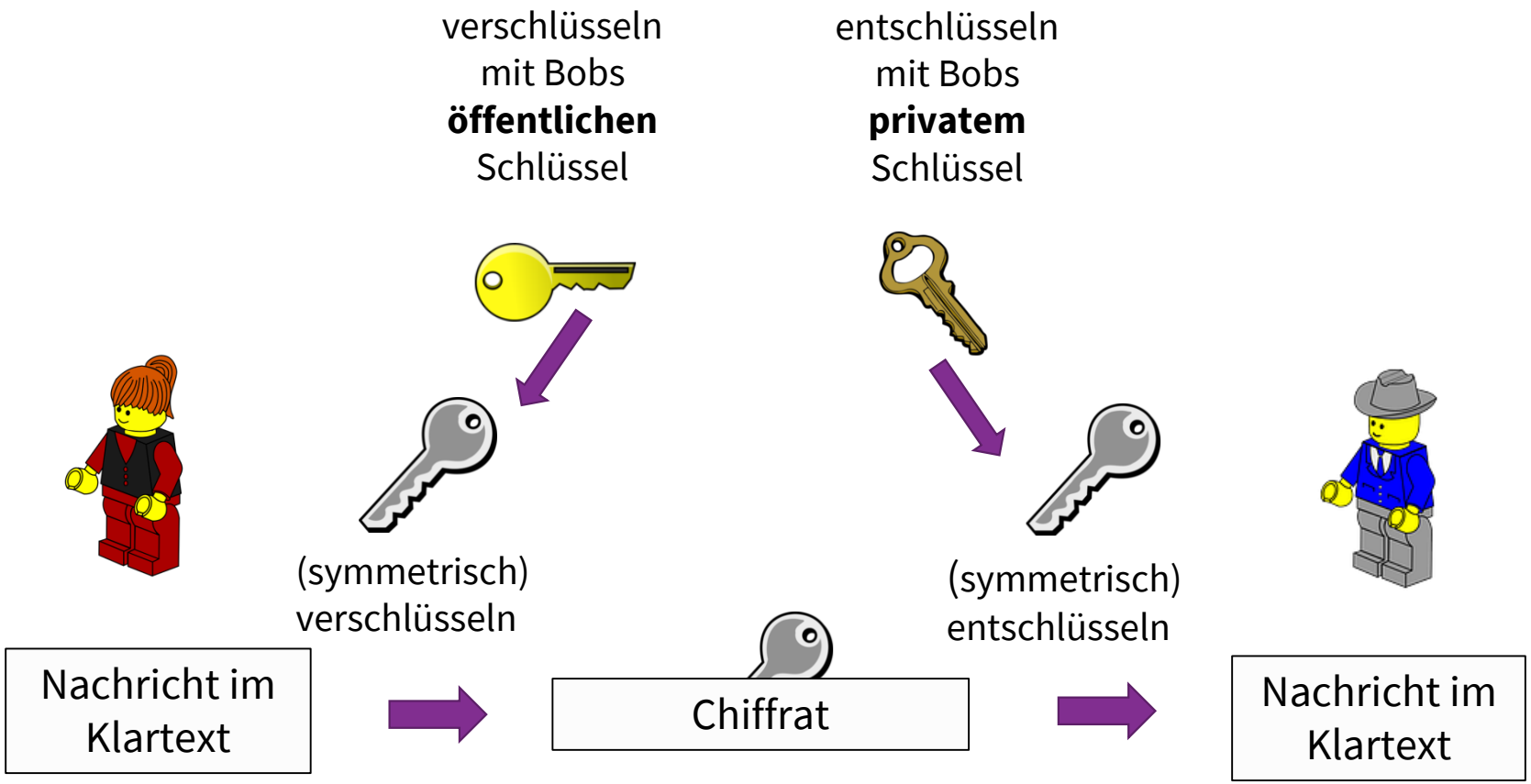


Asymmetrische Verfahren

Vorteil: Kein Schlüsselaustausch nötig
Nachteil: relativ langsam



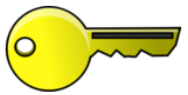
Hybride Verfahren



Digitale Signatur

signieren mit Alice's **privatem** Schlüssel

überprüfen der Signatur mit Alice's **öffentlichen** Schlüssel



Zu signierendes Dokument

Zu signierendes Dokument

Signatur

Nachricht im Klartext

Steganographie

Nachrichten im Text

Die Nachricht wird nicht primär verschlüsselt, sondern versteckt.

- Text in Text
- Bilder in Bildern
- First Letter Messages
- Bitströme in Dateien

Beispiel:
Aus dem Buch «Digital Fortress» von Dan Brown

128-10-6-39-10-128-6-193-98-25-68-85-112-126-78

Lösung: Jeweils der erste Buchstabe des entsprechenden Kapitels im englischen Original. Ergibt: **«we are watching you».**

Nachrichten in Bildern

- Bitmap-Bilder bestehen aus vielen Bytes, welche die Farbintensität angeben

00000078	EB D8 CB E3 D7 D7 DE DB
00000080	CD E5 D2 DE E9 CD D3 F0
00000088	C9 DD EE D0 D2 EE D0 CA
00000090	E1 D0 D4 E2 D4 CC EF CD
00000098	E0 E7 CD CD EE CD CC EB
000000A0	D2 C9 E0 D7 CF E6 D0 DC

- Eine Änderung der am wenigsten signifikanten Bits lässt sich im Bild kaum erkennen.
- Um z.B. den Wert 119 (Binär 01110111) zu verstecken können etwa die Offsets 80 bis 87 «modifiziert» werden.

00000080	CE E5 D3 DF EA CD D3 F1

- 11001110 11100101 11010011 11011111 11101010 11001101 11010011 11110001

Fazit zur Steganographie

- Zählt zwar zu den Geheimschriften, nicht aber zur Kryptographie

- Meistens sehr aufwändiges Prozedere

- Leicht zu «knacken» falls die Nachricht nicht noch zusätzlich verschlüsselt ist.

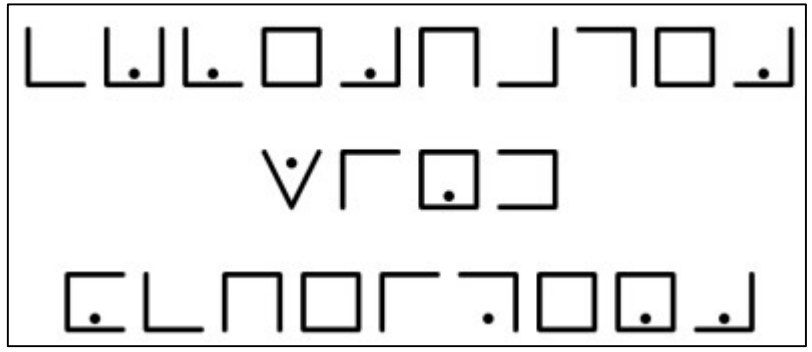
Monoalphabetische Chiffren

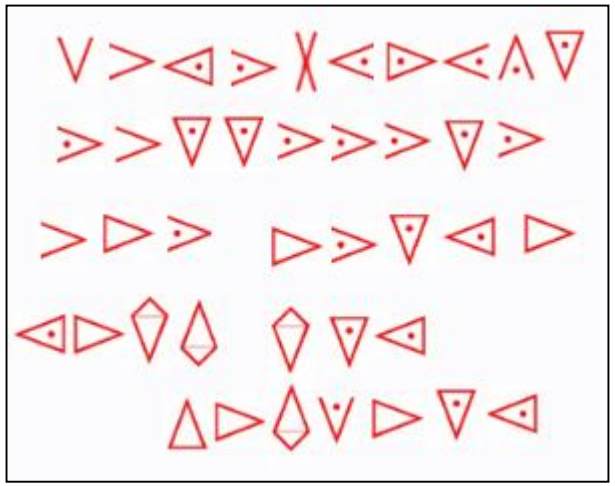
Grundsätzliches

- Ähnlich wie Codierung. Es braucht Nomenklaturen.

- Alle Zeichen werden jeweils immer wieder durch dieselben Zeichen ersetzt.

- Viele gängige «Geheimschriften» (Freimaurer, Tempelritter,…)





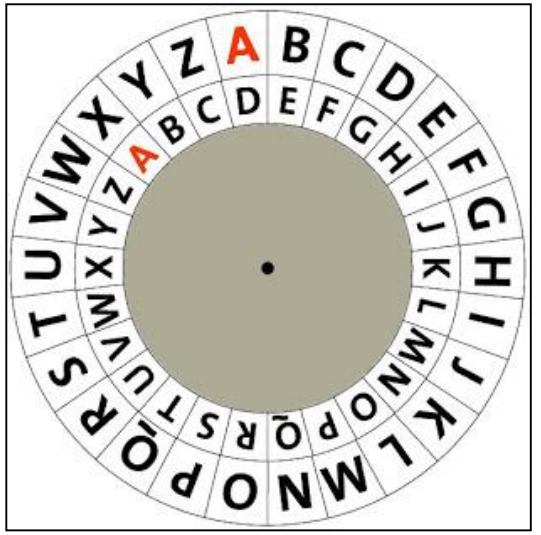
Caesar-Chiffre

- Ähnlich wie Codierung. Es braucht Nomenklaturen.
- Alle Zeichen werden jeweils immer wieder durch dieselben Zeichen ersetzt.
- Beispiel:

  DAS IST STRENG GEHEIM

  GDV LVW VWUHQJ JHKHLP

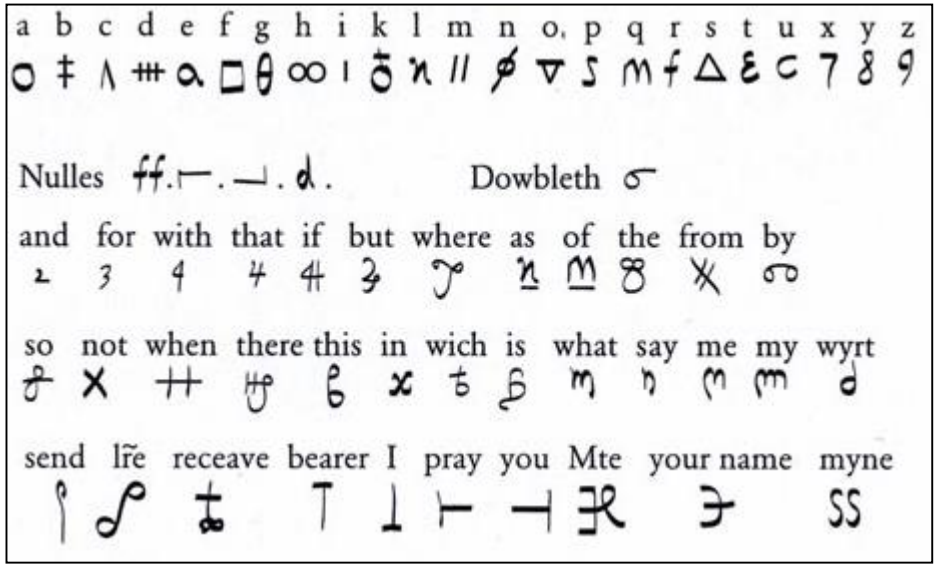
  (Verschlüsselt mit Schlüssel «3» oder «D»)



Maria Stuarts Geheimschrift

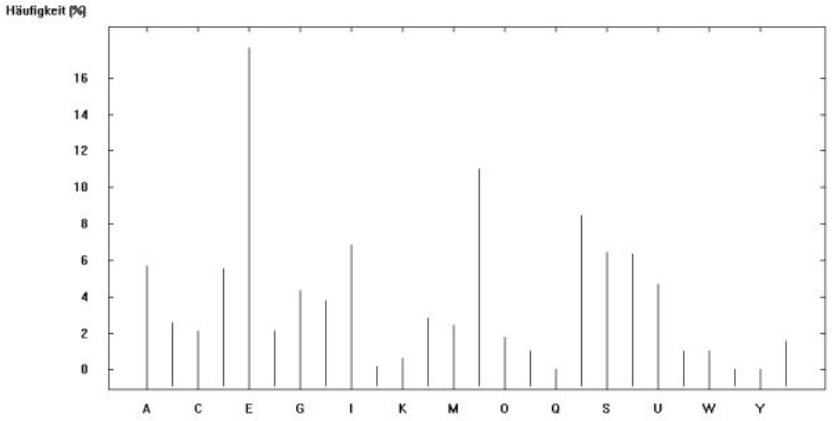
- Thronfolgekämpfe in Schottland
- 1569 wird Stuart wegen angeblichen Mordes zu 18 Jahren Haft verurteilt
- Beteiligt sich aus dem Gefängnis am Babbington-Kommplott
- 1586 wird ihre verschlüsselte Kommunikation kompromittiert, was sie schliesslich den Kopf kostete

Die gesamte Story findet sich im sehr lesenswerten Buch «Geheime Botschaften» von Steven Singh



Kryptoanalyse

- Buchstabenhäufigkeiten (ev. Häufigkeiten von Bi- und Trigrammen)
- Zipfsches Gesetz (Verteilung Häufigkeit-Rangfolge)



Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

Kryptoanalyse

Buchstabenkontext-Regeln, wie:

- A-Priori-Regeln (z.B. u nach q)
- Wahrscheinliche Nachbarn

Wahrscheinlichste rechts- & linksseitige Buchstaben:

1)	E_{rechts} := {R,N,I,S,M,L,D}	E_{links} := {D,I,T,R,B,G,S}
2)	N_{rechts} := {D,E,A,I,G,S,M}	N_{links} := {E,I,U,A,O,N,R}
3)	I_{rechts} := {E,N,C,T,S,G,M}	I_{links} := {E,D,S,N,T,M,R}
4)	S_{rechts} := {T,S,E,C,I,A,O}	S_{links} := {E,I,U,A,O,N,R}
5)	R_{rechts} := {E,A,D,I,S,T,O}	R_{links} := {E,O,H,A,P,G,F}
6)	A_{rechts} := {S,N,U,L,B,R,E}	A_{links} := {D,N,R,H,T,M}
7)	T_{rechts} := {E,I,A,D,H}	T_{links} := {S,I,E,N,R,H,A}
8)	H_{rechts} := {E,A,R,I,T,L,M}	H_{links} := {C,E,T}
9)	D_{rechts} := {E,A,I}	D_{links} := {N,E,R,T,S,H}
10)	U_{rechts} := {N,E,S,F,M,C,T}	U_{links} := {A,Z,N,R,M,F,T}

Fazit zu monoalphabet. Chiffren

- Ziemlich einfach zu knacken

- Haben sich in der Geschichte nicht bewährt

Übungsaufgaben

- **Das Gelernte können Sie mit Hilfe von AB 114-10 üben**

Ziel: Repetition und Vertiefung des Stoffes
SF: Einzelarbeit/Partnerarbeit
Zeit: 60 Minuten

Abschluss

- **Offene Punkte / Fragen**
- **Feedback**
- **Hausaufgaben**
  - Arbeitsblatt AB114-10 fertig lösen