

# Geheime Schriften und Codeknackerei

Jürgen Hermes

Sprachliche Informationsverarbeitung  
Institut für Linguistik  
Universität zu Köln

19. 3. 2012



# Skytale, Sparta ca. 500 v. Chr.



Abbildung: Skytale. Quelle: [www.wikimedia.org](http://www.wikimedia.org)



# Kryptologie

- ▶ Verbergen vs. Aufdecken
- ▶ Verfahren vs. Schlüssel
- ▶ Verschlüsseln vs. Verstecken



# Verstecke ohne Wörter - Semagramme

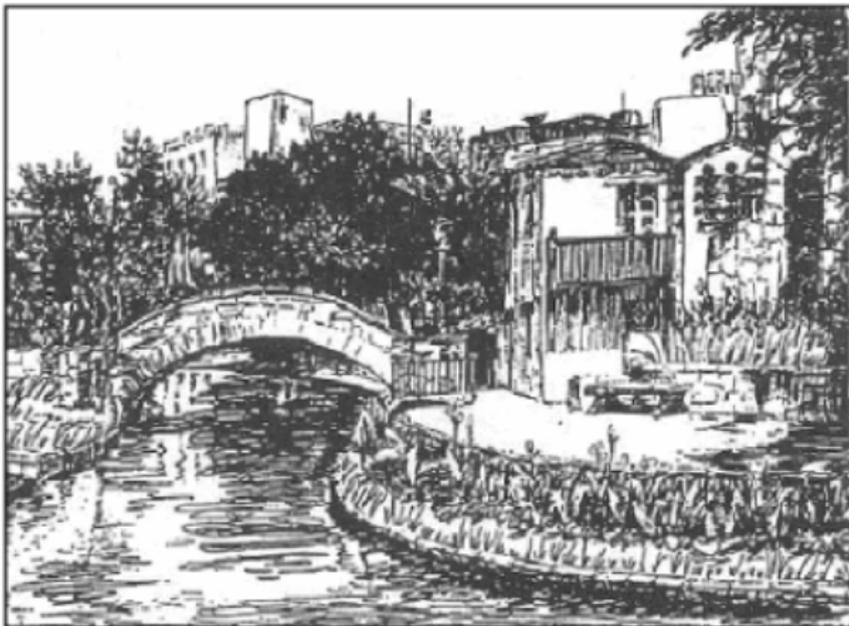


Abbildung: Semagramm. Quelle: [www.gat-blankenburg.de](http://www.gat-blankenburg.de)



# Verstecke in Wörtern - Akrostichon

Einfach zu verwenden und schnell bewerkstelligt,  
nur eben auch keine besonders sichere Methode:  
das, was hier einzig und ausschließlich für das  
erste Wort demonstriert wird, kann auch für das letzte  
Wort jeder Zeile festgelegt werden. Jeder kann das  
lesen, wenn er bzw. sie nur ein wenig sucht.



# Verstecke in Wörtern - Akrostichon

**Einfach** zu verwenden und schnell bewerkstelligt,  
**nur** eben auch keine besonders sichere Methode:  
**das**, was hier einzig und ausschließlich für das  
**erste** Wort demonstriert wird, kann auch für das letzte  
**Wort** jeder Zeile festgelegt werden. Jeder kann das  
**lesen**, wenn er bzw. sie nur ein wenig sucht.



# Vestecke in Wörtern - Cardan-Gitter

Sir John regards you well and spekes again that  
all as rightly 'raile him is yours now and ever.  
May he 'tore for past d'lays with many charms.

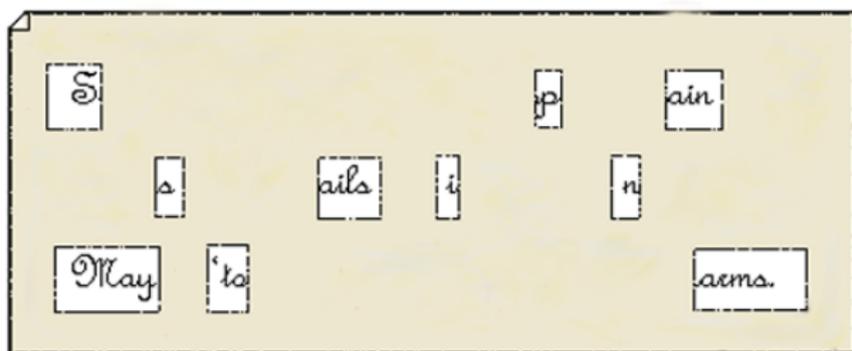


Abbildung: Cardan-Gitter. Quelle: [www.wikimedia.org](http://www.wikimedia.org)

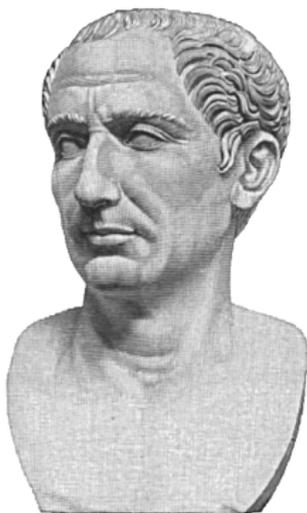


# Anagramme: Ein kombinatorisches Problem

INFORMATION - INFAM ION ROT - INFAM ION TOR - INFAM  
 ION ORT - INFAM RIO TON - INFAM RIO NOT - FIRMA ION  
 NOT - FAIR OMNI TON - FAIR OMNI NOT - TARIF IN MONO -  
 FIAT IN MORON - FORMAT IN ION - FAN IM RIO TON - FAN  
 IM RIO NOT - FAN OMNI TRIO - FAN MIT ORION - FORTAN  
 IM ION - TRAF OMNI IN - TRAF OMNI ION - MAI FRONT  
 ION - MAI ORF IN TON - MAI ORF IN NOT - MAIN INFO ROT  
 - MAIN INFO TOR - MAIN INFO ORT - MAIN TORF ION -  
 MAIN FORT ION - MAIN OFT IRON - NAOMI IN TORF -  
 NAOMI IN FORT - NINA MIR FOTO - NATION IM ORF - IRAN  
 OFT OMNI - TINA INFO ROM - MAN OFT IN RIO - OTMAR  
 INFO IN - AN INFO IM ROT - AN INFO IM TOR - AN TORF IM  
 ION - AN FORT IM ION - ARNO INFO MIT - ARNO OFT MINI -  
 ARNO OFT IM IN - NOTAR INFO IM - NATO INFO MIR ...



# Caesar-Verschlüsselung



**Abbildung:** Gaius Julius Caesar (100-44 v. Chr.). Quelle: [wikimedia.org](https://commons.wikimedia.org/wiki/File:Gaius_Julius_Caesar_Bust.jpg)



# Analyse der Häufigkeiten - Buchstaben

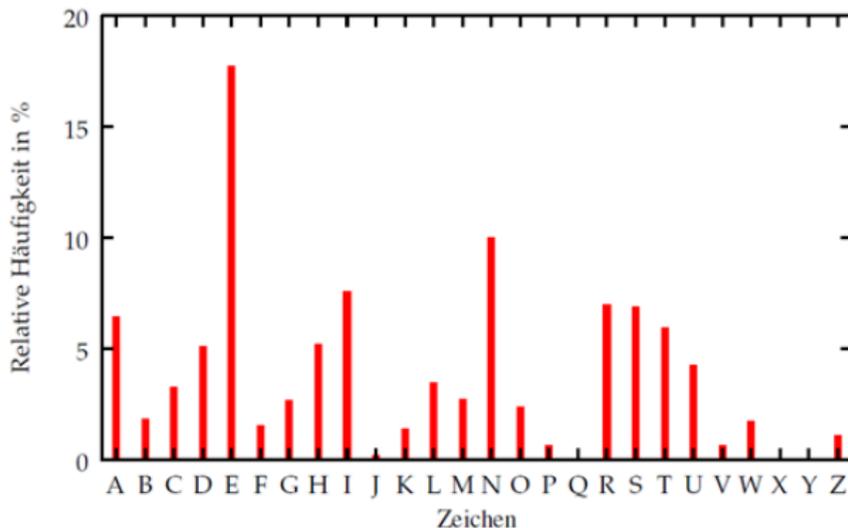


Abbildung: Typische Häufigkeiten von Buchstaben (deutsche Texte)



# Analyse der Häufigkeiten - Bigramme

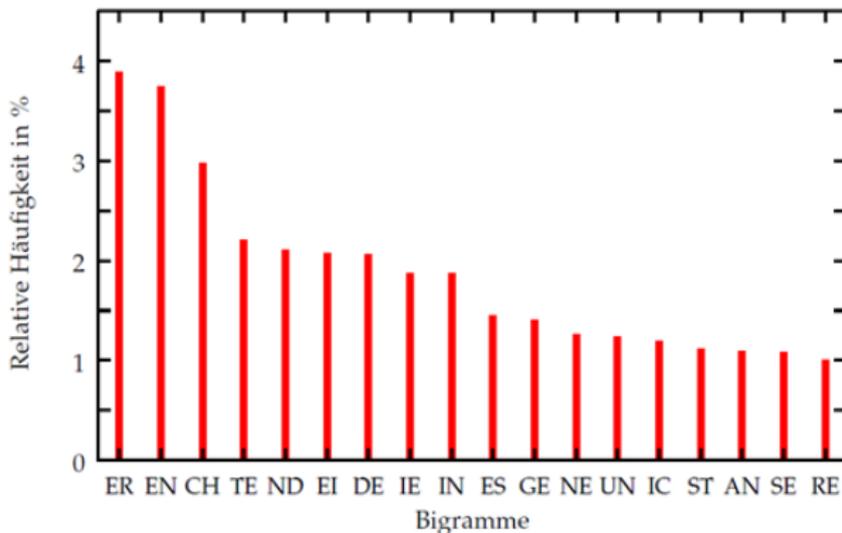


Abbildung: Typische Häufigkeiten von Bigrammen (deutsche Texte)



# Vigenère-Veschlüsselung



Abbildung: Blaise de Vigenère (1523-1596). Quelle: [wikimedia.org](https://commons.wikimedia.org/wiki/File:Blaise_de_Vigenere.jpg)



# Mechanische Erzeugung langer Schlüssel



**Abbildung:** Die deutsche Rotor-Schlüsselmaschine Enigma (20. Jahrhundert). Quelle: [wikimedia.org](https://www.wikimedia.org)



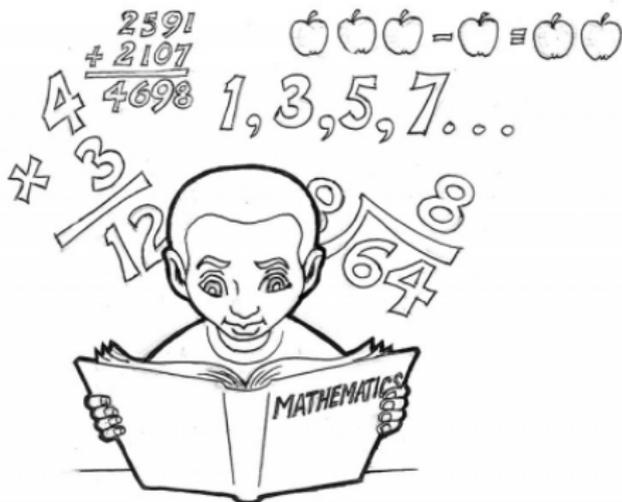
# Computationelle Erzeugung von Schlüsseln



Abbildung: Computer (seit 1941). Quelle: wikimedia.org



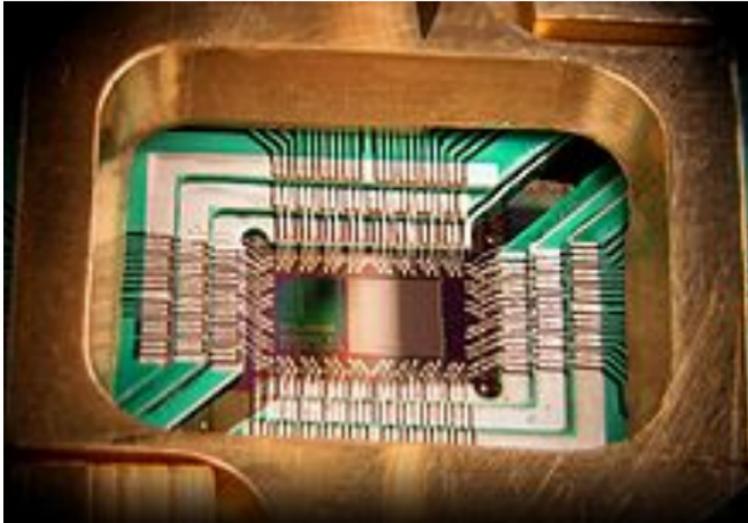
# Zukunft der Kryptologie - Software



**Abbildung:** Mathematik. Quelle: Divine Image Graphics,  
<http://www.schulbilder.org>



# Zukunft der Kryptologie - Hardware



**Abbildung:** Chip aus einem Quantencomputer. Quelle: D-Wave Systems Inc., wikimedia.org



# Ungelöste Geheimschriften



Abbildung: Das Voynich Manuskript (entdeckt 1912). Quelle: Yale University, Beinecke Rare Books and Manuscripts Library



# Ungelöste Geheimschriften

Foror vdrig rrand dflrand ofrorog  
Sror or ord r and rreg rrand dar  
rtror r and gorrer ofror ofrand  
r and rrothg rror rrothg rrothror  
ofror rror rror rtrror rreg?  
rrothg rrothg rrand ofror r and  
ror rrand rror rreg r rreg rrothg  
rtrror rror or ond ofthg rror r and  
ofror ofror rror rror rrothg r and  
ror rror rtrror rreg rrothg  
ror ond rror rror r and rreg  
r and rtrror rror rror

