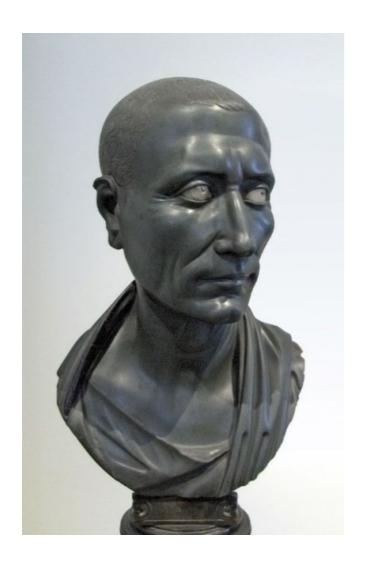
Kryptographie und Kryptoanalyse

Entwickeln Verfahren, Nachrichten zu verschlüsseln

Ziel: Geheimhaltung früher in Politik, Militär, Wirtschaft heute für jedermann



Gaius Julius Caesar 100 – 44 v. Chr

Alphabet-Verschiebung





Karl der Große 747 – 814 n. Chr

ABCDEFGHIJKLM

Kryptografie.de

3TEMBYHYYYXX

NOPQRSTUVWXYZ

Kryptoanalytiker

Entwickeln Verfahren, Verschlüsselung zu durchbrechen

Ziel: geheime Botschaften lesen



Abu Ya'qūb al-Kindī 801 – 873 n. Chr

Häufigkeitsanalyse

المساورة عاد والدور وصف والمكاوما المستواعدة مراولة الورم والمراد المراد من المارات و الدور وصف والمكاوم الموريا المهار المارات والمراد والموريا الموريا المو

Häufigkeitsanalyse

Grundlage: Häufigkeit von Buchstaben in Texten

2 N 9,78 % 3 I 7,55 % 4 S 7,27 % 5 R 7,00 % 6 A 6,51 % 7 T 6,15 % 8 D 5,08 % 9 H 4,76 % 10 U 4,35 %	1	ш	17,40 %
4 S 7,27 % 5 R 7,00 % 6 A 6,51 % 7 T 6,15 % 8 D 5,08 % 9 H 4,76 %	2	N	9,78 %
5 R 7,00 % 6 A 6,51 % 7 T 6,15 % 8 D 5,08 % 9 H 4,76 %	3	—	7,55 %
6 A 6,51 % 7 T 6,15 % 8 D 5,08 % 9 H 4,76 %	4	Ø	7,27 %
7 T 6,15 % 8 D 5,08 % 9 H 4,76 %	5	R	7,00 %
8 D 5,08 % 9 H 4,76 %	6	Α	6,51 %
9 H 4,76 %	7	۲	6,15 %
- 1,1211	8	О	5,08 %
10 U 4,35 %	9	Η	4,76 %
	10	U	4,35 %

11	L	3,44 %
12	O	3,06 %
13	G	3,01 %
14	M	2,53 %
15	0	2,51 %
16	В	1,89 %
17	W	1,89 %
18	F	1,66 %
19	K	1,21 %
20	Z	1,13 %

21	Р	0,79 %
22	>	0,67 %
23	J	0,27 %
24	Y	0,04 %
25	X	0,03 %
26	Ø	0,02 %

Durchschnittliche Häufigkeiten

→ Abweichungen, besonders in kurzen Texten

Weiter nach den Aufgaben

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

27 93 15 48 03 79 01 34 78 55 66 77 10 54 53 86 97 08 85 62 28 72 83 94 05 16

219	31548U3,	(90134/85)	500//10545380	9/08850228/28394	02.10
380	426 59 14 9	90 12 45 89	88216564	19 96 73 39	
49	37 70 25	23 56 00	99327675	30 07 84 50	
60	8136	67 11	43 87	41 18 95 61	
71	9247	22	98	52 29 06	
82	58	33	09	63 40 17	
	69	44	20	74 51	
	80		31		
	91		42		
	02				
	13				
	24				
	35				
	46				
	57				
	68				

Homophone: Mehrere Geheimzeichen pro Buchstabe

Beispiel: Zahlen von 00 bis 99 als Geheimzeichen

E mit 17% Häufigkeit → 17 Zahlen

N mit 9% Häufigkeit → 9 Zahlen, usw.

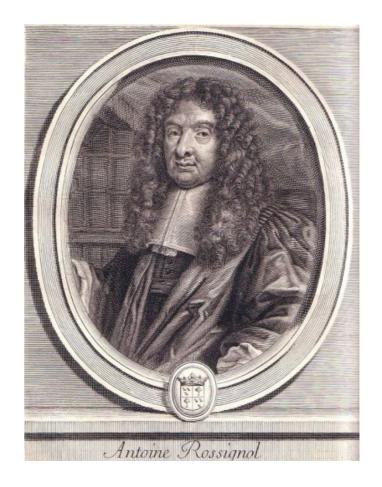
Verschlüssle E mit einer der 17 Zahlen (zufällig)

→ Jede Zahl erscheint (fast) gleich oft.

Historisch belegt um 1400 n. Chr.

Große Chiffre von Louis XIV (1638 – 1715) Erdacht von Antoine und Bonaventure Rossignol







Große Chiffre

587 Zahlen für

- Buchstaben
- Silben
- Hindernisse wie "nichts" oder "letztes löschen"

Erst 1893 geknackt (Étienne Brazeries)

Autor / Quellen

Autor:

Christian Pothmann (cpothmann.de)
 Freigegeben unter CC BY-NC-SA 4.0, Januar 2022



Grafiken:

- Caesar: en.wikipedia.org, gemeinfrei
- Alberti-Scheibe: de.wikipedia.org, gemeinfrei
- Karl der Große: de.wikipedia.org, gemeinfrei
- Chiffre Karls des Großen: © O. Kuhlemann, kryptographie.de
- al-Kindī: commons.wikimedia.org, gemeinfrei
- Handschrift al-Kindīs: en.wikipedia.org, gemeinfrei
- Louis XIV: en.wikipedia.org, gemeinfrei
- Antoine Rossignol: de.wikipedia.org, gemeinfrei
- Große Chiffre: de.wikipedia.org, gemeinfrei