

Kryptographie und Kryptoanalyse

Kryptographen

Entwickeln Verfahren,
Nachrichten zu verschlüsseln

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

Kryptographen



Gaius Julius Caesar

100 – 44 v. Chr

Alphabet-Verschiebung



Kryptographen



Karl der Große 747 – 814 n. Chr

Ɑ Ɱ Ɐ Ɒ ⱱ Ⱳ ⱳ ⱴ Ⱶ ⱶ ⱷ ⱸ ⱹ ⱺ ⱻ
A B C D E F G H I J K L M
Kryptografie.de
ⱼ ⱋ ⱌ ⱍ ⱎ ⱏ ⱐ ⱑ ⱒ ⱓ ⱔ ⱕ ⱖ ⱗ ⱘ ⱙ ⱚ
N O P Q R S T U V W X Y Z

Kryptoanalytiker

Entwickeln Verfahren,
Verschlüsselung zu durchbrechen

Ziel: geheime Botschaften lesen

Kryptographien

Abu Ya'qūb al-Kindī

801 – 873 n. Chr

Häufigkeitsanalyse

[illegible][illegible]

Häufigkeitsanalyse

Grundlage: Häufigkeit von Buchstaben in Texten

1	E	17,40 %
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 %

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

21	P	0,79 %
22	V	0,67 %
23	J	0,27 %
24	Y	0,04 %
25	X	0,03 %
26	Q	0,02 %

Durchschnittliche Häufigkeiten

→ Abweichungen, besonders in kurzen Texten

Erschweren der Häufigkeitsanalyse

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
38	04	26	59	14	90	12	45	89			88	21	65	64			19	96	73	39					
49		37	70	25		23	56	00			99	32	76	75			30	07	84	50					
60			81	36			67	11				43	87				41	18	95	61					
71			92	47				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																					

Erschweren der Häufigkeitsanalyse

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.

Verschlüsse E mit einer der 17 Zahlen (zufällig)
→ Jede Zahl erscheint (fast) gleich oft.

Historisch belegt um 1400 n. Chr.

Erschweren der Häufigkeitsanalyse

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



Erschweren der Häufigkeitsanalyse

M	O	P	Q	R	S	T	V	X	Y	Z	&
811	117 238	219	407	511	355	340	141 163	205	518	820	279 448
702	359 500	338	595	733	527	618	284 164	436	639		615 827
genera, l. u. a.	35		lieu, x.	668		Ob.	19	presque	801		
gens	55		limites	708		obei	39	preter, dre, tion	30		
ger	575	95	liure	728		objet, s.	69	pretexte	841		
ges	115		le Roy de	758		obliger, ation	89	priv.	881		
gla	155		le Prince, de	798		observ, er, ation	129	principal, u. a.	52		
gle	215		le Duc de	838		obstacle, s.	179	prisonnier, s.	132		
gli	275		le Marquis de	858		obtenir	220	pro.	162		
glo, ire	335		le Baron de	898		oc, cation	249	prochain	202		
gna	375		le Sieur de	49		ocup, er	289	profit, er	262		
gne	435		loin	79		of.	349	projet, s.	282		
gni	485		lon	119		office, ier, s.	429	propos, ition	382		
gno	505		lors	189		offre, s.	449	provision, s.	422		
gouvern, or, ment	16		luy	259		oient	499	prouv	462		
gra, æ	405		Ma	868	298	oir	529	pru	462		
grand	525		me	779	339	oia	559	publi, er, c.	512		
gre	585		mi	279	379	oit	629	puis, sance	572		
gri	625		mo	439	479	ol	669	Qu	612		
gro	665		mu	489	519	om	729	qua	672		
gua	695		magasin, s.	519	559	on, s.	779	qualite	722		
gue	735		main, s.	549	589	ont	789	quand	742		
guerre	825		mais	579	619	op, pose, ition	819	quantite	762		
gui, de, s.	895		maitre, s.	609	649	or	849	quarente	782		
Pa	26		mal, ade, s. je, s.	639	679	ordinaire, s.	879	quart, ier, s.	822		
be	56		mand, er	679	719	ordonn, er	20	quatre	842		
bi	156		maniere, s.	719	759	ordre, s.	60	que	862		
bo	216		manque, r	759	799	or, s, t	100	quel, le, s.	882		
bu	266		marcbe, s.	799	839	os, t	130	question, s.	23		
baut	326		marqu, e, r	839	879	ou, r	160	qui	50	53	
babi, t, le, tant	486		marecha, f. u. a.	879	919	ouvr.	210	qu'il	73		
keur, e, s.	656		mauvais	919	959	La	240	quinze	153		
bier	796		meilleur	959	999		270	quo, n	390	153	

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. Kuhleemann, 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