Kryptographie

und

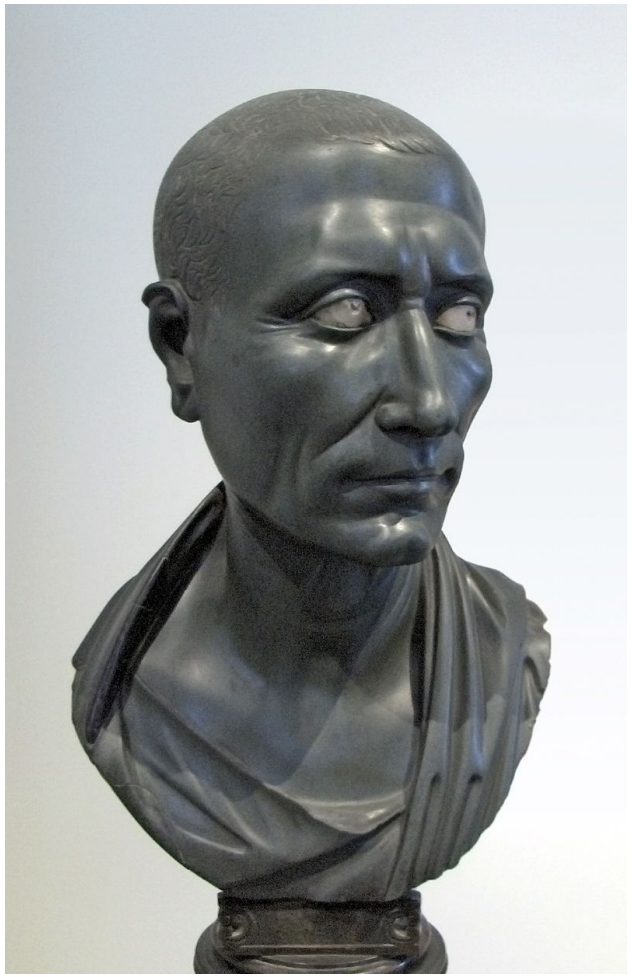
Kryptoanalyse

Kryptographen

Entwickeln Verfahren,
Nachrichten zu verschlüsseln

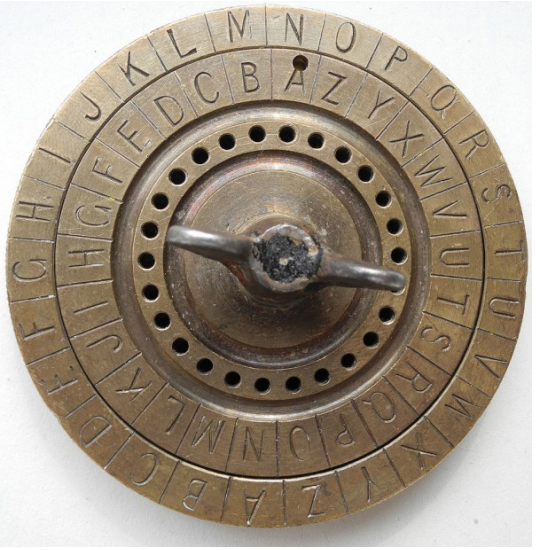
Ziel: Geheimhaltung
früher in Politik, Militär, Wirtschaft
heute für jedermann

Kryptographen



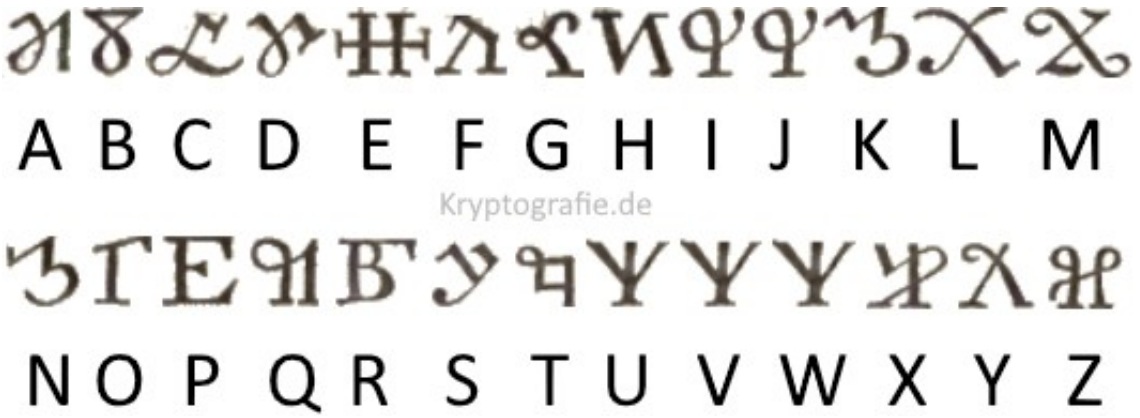
Gaius Julius Caesar
100 – 44 v. Chr

Alphabet-Verschiebung



Kryptographen

Karl der Große
747 – 814 n. Chr



Kryptoanalytiker

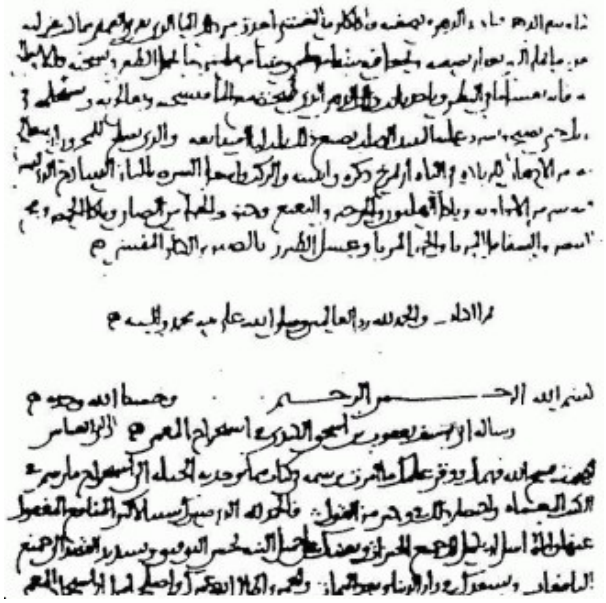
Entwickeln Verfahren,
Verschlüsselung zu durchbrechen

Ziel: geheime Botschaften lesen

Kryptographen

Abu Ya'qūb al-Kindī
801 – 873 n. Chr

Häufigkeitsanalyse



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

Weiter nach den Aufgaben

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.

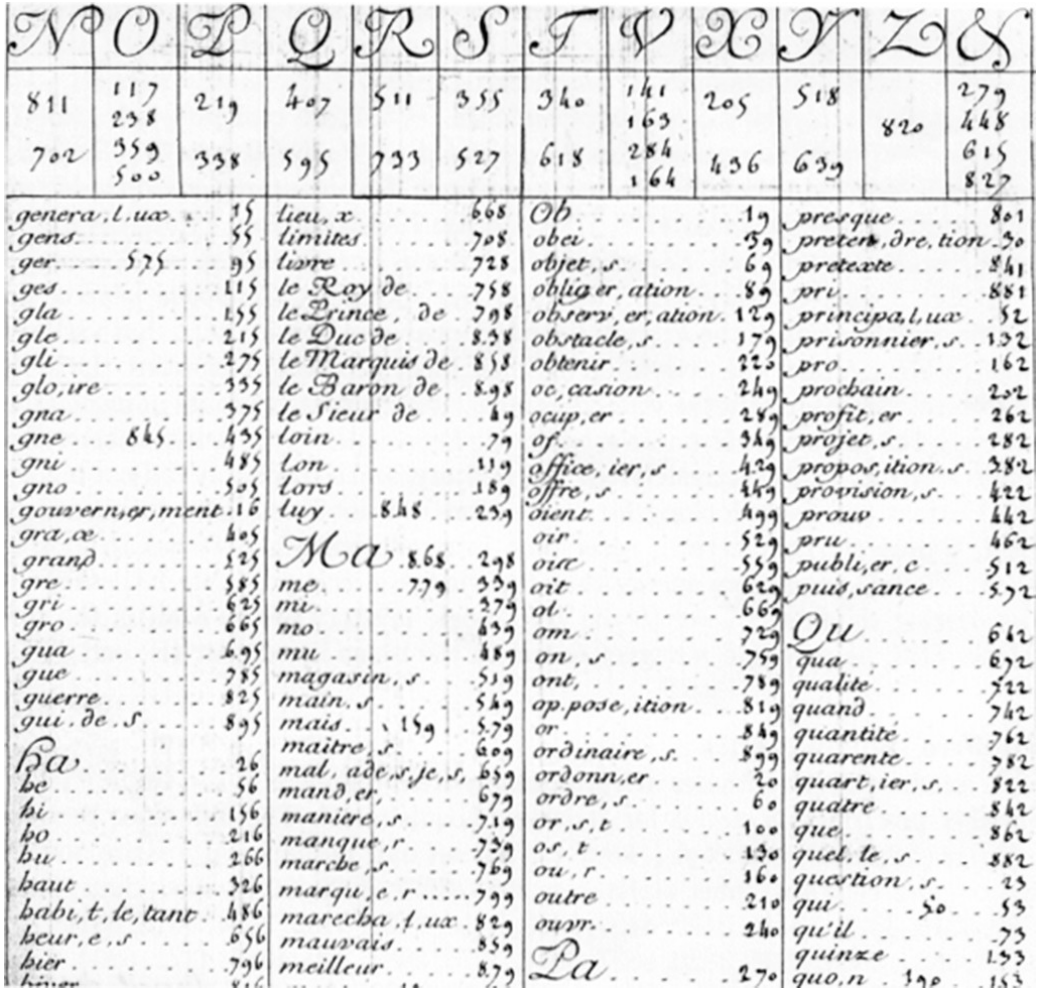
Verschlüssle E mit einer der 17 Zahlen (zufällig)
→ Jede Zahl erscheint (fast) gleich oft.

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



N	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,ux	15	lieu,x	668	Ob	19	presque	801
gens	55	limites	708	obei	59	preten,dre,tion	50
ger	575	95	livre	728	objet,s	69	pretexte	841
ges	115	le Roy de	758	oblig,er,ation	89	pri	881
gla	155	le Prince de	798	observ,er,ation	129	principa,l,ux	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,casion	249	prochain	202
gna	375	le Sieur de	49	ocup,er	289	profit,er	262
gne	845	435	loin	79	of	349	projet,s	282
gni	485	lon	119	office,ier,s	429	propos,ition,s	382
gno	505	lors	189	offre,s	469	provision,s	422
gouvern,er,ment	16	luy	848	259	oient	499	prouv	442
gra,æ	405				oir	529	pru	462
grand	525	Ma	868	298	oire	559	publi,er,c	512
gre	585	me	779	339	oit	629	puis,sance	572
gri	625	mi	379	ol	669		
gro	665	mo	839	om	729	Qu	662
gua	695	mu	889	on,s	759	qua	692
gue	785	magasin,s	519	ont,	789	qualite	722
guerre	825	main,s	549	op,pose,ition	819	quand	742
gui,de,s	895	mais	159	579	or	849	quantite	762
		maitre,s	609	ordinaire,s	899	quarente	782
ha	26	mal, ade,s,je,s,	659	ordonn,er	20	quart,ier,s	822
he	56	mand,er,	679	ordre,s	60	quatre	842
hi	156	maniere,s	719	or,s,t	100	que	862
ho	216	manque,r	739	os,t	130	quel,le,s	882
hu	266	marche,s	769	ou,r	160	question,s	23
haut	326	marqu,e,r	799	outre	210	qui	50 53
habi,t,le,tant	486	marecha,l,ux	829	ouvr	240	qu'il	73
heur,e,s	656	mauvais	859			quinze	153
hier	796	meilleur	879	La	270	quo,n	340 183

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