

MIT FLUGPOST
PAR AVION



*310 x 200
Wash. D.C.
3*

William F. FRIEDMANN

424 North George Mason Drive

ARLINGTON

300 Virginia USA.

**AEROGRAMM
AÉROGRAMME
AIR LETTER**

NICHTS EINSCHLIESSEN, SONST KEINE BEHANDLUNG ALS AEROGRAMM



ABSENDER:

Rudolf L. R. Ogerman
Andrea
SALZBURG, Rudolf Drebisstr, 17



Salzburg, am 1. Februar 1954

Mr. William F. F R I E D M A N N

424, North George Mason Drive

A R L I N G T O N

V i r g i n i a , U.S.A.

S E H R G E E H R T E R H E R R !

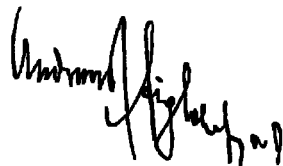
Auf meinen Brief an Sie vom 24. September 1953 bekam ich am 30. Oktober v. J. von Ihrem Sekretär, Mr. E. B. Young am 27. X. 1953 Nachricht, dass Sie bis Ende November verreist sind und erst nach Ihrer Heimkehr mir persönlich schreiben werden.

Bis heute traf diese Nachricht nicht hier ein und ist es nicht ausgeschlossen, dass Ihr Brief am Postwege verloren ging. Solcher Verlust wäre umso bedauerlicher, weil ich gerade dem Gutachten und der Bewertung eines so bedeutenden und anerkannten Fachmannes, wie Sie, sehr geschätzter Herr Friedmann sind, größte Wichtigkeit beimesse.

Ich bitte daher um bezügliche Nachricht, eventuell Wiederholung Ihrer etwa in Verlust geratenen Antwort an mich.

Mit fachkollegialem Grusse und der Versicherung besonderer Wertschätzung bin ich

I h r



DEAR MISTER FRIEDMANN ,

By virtue of practical industry acquainted with your illustrious name I read in J.Galland's book: Bibliography of Literature of cryptology - a long series of your works concerning this sphere of scientific branch, whose the fewest (I am sorry to say) are to be bought in book-trade.

Some years ago I had to translate into German for a friend the work entitled: 'L'indice des coincidences'. On this occasion I could study it thoroughly, whence it was possible to draw a conclusion upon the high spirit and the enormous importance of your other works.

After having got your address from my friend ,Mr.J.H. Waite (57 Strawbridge Av., Westmont, New Jersey) and aware, that you ,dear Colonell, know my book: 'Systeme des Chiffrirens' and that you are acquainted with my name (according your 'Codes and ciphers' in vol.V of the 'Encyclopaedia Britannica ', moreover firmly convinced, that your ample speciality makes possible to you- I want to ask you for the favour of giving me your precious special advice.

Because the publishing of my 'Systeme des Dechiffrierens' planned in the year 1926 was prevented on the strength of superior order ,I produced from sketches, schemes and notes and also by memory a manuscript brought up to the modern point of science , of which I submit following things :

- (1) the prospectus
- (2) the register
- (3) the list of supplements to 'Systeme des Chiffrierens'
- (4) the list of supplements to 'Systeme des Dechiffrirens'

I wish to realize these papers. The printing or an other publishing is impossible ,as in consideration of the contents 'officially' declared for 'secret' as on account of my special life-long liabilities. It remains only the acquisition of the manuscripts for exclusive possession on the part of a collector, an admirer

of the cryptography or by a great library, taking pride in the possession of this monumental work.

In thus manner the manuscripts could be made available for study to a circle of interested persons as well as to an individual person ,welcome by the possessor.

I beg you to inspect the foresaid documents and to consult me about the value of the manuscripts, in consideration of the circumstance, that they are a work of life during many years perfected and that an acquisition by a purchaser will incorporate in his collection an unique scarcity ,a single copy. which makes him as exclusive possessor.

Hoping, that you ,dear colleague, will fulfill my request, I am awaiting your words to that effect with keen attention and I assure you of my best respects ,with collegial regards

Yours sincerely

A handwritten signature in cursive script, appearing to read "Andrew H. Fisher, D." with a small flourish at the end.

P R O S P E K T

der

S Y S T E M E D E S D E C H I F F R I E R E N S

aus Erlebnissen und Erfahrungen in Kriegs- und Friedenszeiten dargestellt von

A n d r e a s F I G L

Hefrat i.R., Oberst a.D.

Der stürmische Ablauf der Menschheitsgeschichte während der letzten Jahrzehnte hat auf allen Gebieten des Wissens und Könnens raschere und grözere Fortschritte gebracht, als irgend eine frühere Epoche.

Alle Fernverkehrsmittel: Telegraph, Telephon, Funk, Fernschreiber sind auf neue hohe Entwicklungsstufen gebracht worden, um die gewaltig angewachsene amtliche, geschäftliche und private Korrespondenz zu bewältigen.

Der Zerfall alter, grosser Staatengebilde und die Entstehung zahlreicher neuer kleiner Staaten hat die Korrespondenzflut noch gesteigert, hat aber auch das Bedürfnis nach W a h r u n g der Staats-, Geschäfts- und sonstigen Interessen vermehrt, was wieder die Nachfrage nach S i c h e r u n g e n für diesen Verkehr vervielfältigte.

Solche Sicherungen i n n e r e r A r t suchte man in den G e h e i m s c h r i f t e n, welche zahlreiche und verschiedene Systeme zum Chiffrieren in jedem, auch dem höchsten Anspruche genügenden Ausmasze darboten.

Infolge dieses lebendigen Interesses nicht nur amtlicher Stellen, sondern auch weiter privater Kreise an diesem Wissensgebiete erschienen nach dem Weltkriege in vielen Kulturländern Werke über die Geheimschreiberei, die Kryptographie.

In Oesterreich wurde im Jahre 1926 das Werk des ersten und letzten Chefkryptographen der ehemaligen k.u.k. österreichisch-ungarischen Armee die

" S Y S T E M E D E S C H I F F R I E R E N S " +)

herausgegeben, in welchen--als Fortsetzung und II. Bandes--die Ausgabe der

" S Y S T E M E D E S D E C H I F F R I E R E N S "

in Aussicht gestellt worden ist.

"Vis major" verhinderte damals das Erscheinen dieses Werkes: 1926/27 wurde vom Bundeskanzleramte über Betreiben des Regesministeriums, das wieder vom deutschen Generalstabe dazu veranlasst worden war, die Herausgabe verboten. Das zu einem Drittel fertig gedruckte Werk musste zurückgezogen werden, das Manuscript wurde beschlagnahmt und lag zuletzt als Studienbehelf im Ministerium des Inneren, Abteilung General Renze. Von dort wurde es mit allen Akten dieser Abteilung nach dem Wimmarsche der Deutschen in Oesterreich nach Berlin gebracht. Dort ist das Manuscript spurlos verschwunden, im Jahre 1940 fand ich nur einige verstreute Blätter und alle Nachforschungen nach den übrigen Teilen blieb erfolglos. Bis heute kam nichts davon an den Tag.

Aus Aufzeichnungen, Entwürfen, Skizzen und aus dem Gedächtnisse, dann aus den Erfahrungen der letzten Dienstjahre und aus Studien nach

+) Von Oberst Andreas FIGL, Verlag Ulrich Moser, Graz 1926 (jetzt Styria-Buchhandlung, Graz)

meinen Ausscheiden aus der Aktivität, zu denen es vorher an Zeit gebrach, entstand ein neues, in mancher Hinsicht ergänztes und bereichertes Manuscript der

"SYSTEME DES DECHIFFRIERENS"

Wie schon der Titel besagt, ist darin einzig die Kunst dargestellt wie die Lösung von Geheimschriften ohne Besitz des zugehörigen Schlüssels, als die Enträtselung bewirkt werden kann. Das ganze Werk ist also als Lehr- und Studienbehelf gedacht. Es kann sowohl für Vorträge und Kurse als Unterlage dienen, wie auch von Berufskryptographen und von Liebhabern zum Selbststudium verwendet werden. Im Vereine mit den seinerzeit erschienenen "Systemen des Chiffrierens" kann es auch zur Verfassung von Übungsaufgaben für die Studenten dienen.

Schliesslich gibt das Werk die Möglichkeit, daraus Grundsätze und Regeln abzuleiten, wie eigene Geheimschreibebefehle zu gestalten sind, um die angestrebte Sicherheit zu gewährleisten, d.h. zu zeigen, was und wie man es nicht machen darf, wenn man seinen Geheimgespräch wirklich geheim gestalten will.

Das Werk ist aus der Praxis und für die Praxis geschrieben, doch sind aus begrifflichen Gründen die zur Lösung gestellten Beispiele solchen aus dem Verkehrsleben nachgebildet, erfüllen aber trotzdem ihren Lehrzweck.

Im I. Teile sind die einleitenden Begriffe, die Enträtselungsgrundlagen und die Verarbeiten, die analytischen Untersuchungen dargestellt.

Der II. Teil gibt die eigentlichen Enträtselungsvergänge von den einfachsten Verfahren bis zu den Zweibüchern, d.s. Kodes aus Chiffriert und Dechiffriert bestehend, dann die Lösung von Überschlüsselungen wieder.

In Nachträgen sind einerseits Verfahren zum Schlüssel finden enthalten, welche dem Verfasser bis in die jüngste Zeit bekannt wurden; andererseits ist die Enträtselung solcher Verfahren entwickelt. Hiedurch ist das Werk bis in die jüngste Zeit fortgeführt, so dass Lehrende, wie Lernende auch über Aktuelles darin Aufschluss finden.

Das Manuscript zählt 281 eng mit Maschine einseitig beschriebene Seiten im Formate 21 x 34 cm. Beigegeben sind 75 Tabellen udgl. mit 49 Hilfsblättern, einseitig, Format 21 x 34 cm.

Die Nachträge zu den "Systemen des Chiffrierens" zählen 68 wie oben beschriebene Seiten und 28 Tabellen udgl., jener zu den "Systemen des Dechiffrierens" umfasst 68 wie vor beschriebene Seiten und 71 Tabellen udgl., alle im Formate 21 x 29 cm. vereinzelt auch grösser.

Ein reichhaltiges Literaturverzeichnis liegt bei und ein genaues Sachregister erleichtert das Nachschlagen im Werke.

S A L Z B U R G , im September 1953.

INHALTSVERZEICHNIS.

I. T E I L .

1. ABSCHNITT : EINLEITUNG .

Kapitel:		Seite	Beilage	Hilfsblatt
1.	Allgemeine Begriffe.....			
2.	Fachausdrücke.....			
3.	Eigenschaften des Enträtselers.....			
4.	Materialie und dessen Beschaffung.....		1	
5.	Einzelschriften.....			
6.	Massenschriften.....			

2. Abschnitt: Enträtselungsgrundlagen.

7.	Allgemeines.....			
8.	Buchstabenhäufigkeit in verschiedenen Sprachen.....		2, 3	
9.	Häufigkeiten der deutschen Sprache.....		4	
10.	" " " " englischen Sprache.....		5	
11.	" " " " französischen Sprache.....		6	
12.	" " " " italienischen Sprache.....		7	
13.	" " " " spanischen Sprache.....		8	
14.	" " " " russischen Sprache.....		9	
15.	" " " " serbo-kreatischen Sprache.....		10	
16.	" " " " tschechischen Sprache.....		11	
17.	" " " " polnischen Sprache.....		12	
18.	" " " " ungarischen Sprache.....		13	
19.	Kennzeichen der Verfahren.....			

3. ABSCHNITT : VORARBEITEN.

20.	Allgemeine Untersuchung, 1. Beispiel.....	14, 15		1, 2
21.	" " " " 2. B " ".....			
22.	" " " " 3. " " " ".....	16		1, 2, 3,
23.	" " " " 4. " " " ".....			
24.	" " " " 5. " " " ".....	17		1
25.	" " " " 6. " " " ".....	18		1
26.	Absender, Empfänger; Schlüsse daraus.....			
27.	Untersuchung der Häufigkeit, Schlüsse daraus.....			
28.	Forschen nach dem Verfahren.....			
29.	Freies Enträteln, Beweis der Richtigkeit.....			
30.	Verstümmelungen.....			

II. T E I L .

DIE ENTRÄTSELUNGSARBEITEN .

4. ABSCHNITT. DIE ENTRÄTSELUNG VON BUCHSTABENVERFAHREN.

31.	Enträtselung von Verkehrschriften.....	19		
32.	" " " " Zeilenschriften.....	19		1, 2
33.	" " " " Spaltenschriften.....	20		1, 2
34.	" " " " einfacher Ersatzverfahren: 1. Beispiel.....	21		
	2. " " " ".....	21		1
	3. " " " ".....	20, 21		2
	4. " " " ".....	22		1
	5. " " " ".....	22		2
35.	Enträtselung einfacher Würfel.....	23, 24		1
36.	" " " " von Nihilistenquadraten.....	23, 25		
37.	Behandlung erweiterter u. ergänzter Alphabete.....	26		1
38.	" " " " von Gittern, 1. Beispiel.....	27		3
39.	" " " " " " 2. " " " ".....	28		2
40.	" " " " " " Doppelalphabeten, 1. Beispiel.....	29/1		
41.	" " " " " " " " 2. " " " ".....	29/2		1

Kapitel:	Seite	Beilage	Hilfsblatt
42. Enträtselung von Crenfelds Verfahren.....		30 31	1
43. Lösung von Tritheim, 1. Beispiel.....		32/3 33	1
44. " " " 2. "		34	1
45. " " " 3. "		35	
46. " " " Portas (Napoleons) Verfahren.....		36	2
47. " " " Sprungchiffres.....		37/4	
48. " " " Mehrfachalphabeten (erweiterten Tritheim)		38/4	
49. " " " Trapezverfahren.....		39/2	
50. " " " Dreieckverfahren.....		40/2	
51. " " " des Doppelwürfels, 1. Beispiel.....		41	
52. " " " " 2. "		42	
53. " " " " 3. Beispiel.....		43	
54. " " " Einfachen englischen Schlüsselquadrates		44/3	
55. " " " Verbesserten " " " 1. Beisp.		45/3	
56. " " " " " " 2. "		46	
57. " " " von einfachen Versetzungen.....		47	
58. " " " Doppelversetzungen.....		48/2	
59. " " " Kannchiffres.....		49/3	
60. " " " Fullgittern.....		50, 51, 52	
61. " " " Fleisznerns Patronschrift.....		53, 54, 55	
62. " " " Diagonalverfahren, Einschreiben.....		56/3	
63. " " " " " Abschreiben.....		57/2	
64. " " " mechanischen Verfahren.....			
65. Das Lüften von Verschleierungen.....			
65 a. Aufsuchen verborgener Sigelschriften.....			

5. ABSCHNITT. ENTRÄTSELUNG VON SCHÜSSELTAFFELN.

66. Erkennen und Untersuchung von Schriften nach Tafeln	58/3
67. Enträtseln von Schriften nach Tafeln.....	59 60
68. Verwertung der Enträtselungen.....	61
69. Schlüsselwechsel an der gefundenen Tafel.....	62

6. ABSCHNITT. ENTRÄTSELUNG VON SCHRIFTEN AUS SCHLÜSSELBÜCHERN.

70. Erkennen u. untersuchen von Schriften nach Schlüsselbüchern	63
71. Sonderuntersuchung von Schriften aus Schlüsselbüchern	64/2, 65
72. Untersuchung von Anfängen und Enden.....	66, 67
Harte Deutungen.....	68, 69
73. Sichtung der Ergebnisse; Erwägungen.....	
74. Enträtselung des Inhaltes der Schriften.....	70/2
75. Enträtselung von Zweibüchern.....	71
76. Die Lösung von Überschlüsselungen:.....	
77. " " " A) Umstellungen (Transpositionen)	
78. " " " B) Umwandlungen (Transformationen)	72/2
79. " " " C) Umschreibungen (Transcriptionen)	
(Rechenoperationen) 1. Beispiel.	73/3
80. " " " " " 2. Beispiel.	74/2
81. " " " " " 3. Beispiel.	75/2
82. " " " Aufbauschungen.....	

Schlusswort.....
 Sachregister.....
 Abkürzungen.....

K A P I T E L - G E

ZU DEN ERSTES GEDRUCKTEN WERKE:
 "S I S T E M E D E S C H I F F R I E R E N S."

Kapitel:	Seiten:	Beilagen:
18a Kammschiffre oder Schieberegister.....	2	9a
19a Das Schlüsselkreuz.....	1	10a
23a Das Kammern Quadrat.....	2	12a
30b Kominternquadrat.....	2	---
31a Erweiterter Caesars Zeichencaesar.....	1	---
31b Russencaesar mit Uberschlüssel.....	1	---
31c Rockinger Festvortrag Chiffren u. 16. Jahrhundert derts....	21	davon 1b Beil.
39b Verbessertes Hililistenquadrat.....	1	---
40a Die Sigramtabelle.....	2	20 a
54a Der Ungleichsteller.....	2	---
54b Morsechiffre "Columbus" (nach Ing. A. Schütz)....	3	23a
62a Umwandlung von Zähler-in Wortsigel m. Wechsel- system.....	2	20a
65b Uberschlüsselung m. Sigramtabelle in I. Zwei- zifferer... II. Umwandlung in Sigelwörter... III. Verzahnte Uberschlüsselung von Zahlensigeln... IV. Umwandlung von Zahlen-in Wort- sigel u. Verzahnung... V. Anfertigung von Sigramtabellein.	1 1 1 1 1	25a 25a ---
65c Streifenüberschlüsselung. a) für Zahlensigel b) für Buchstaben- sigel.....	2 2	25b, 1. 25b II.
76a Die Zahlenwurmtablel.....	2	27a
76b Uberschlüsselung mit Zahlenwürmern.....	1	---
76c Scheiben-Sigelverdichter (-Kondensoren).....	2	27b
76d Tafel-Sigelverdichter (-Kondensoren).....	2	27c, I. II.
76e Di-Trigrammtablel als Sigelverdichter u. Ueber- schlüssel.....	1	27a
76f Miracle-Sigelverdichter von Hoinmann, Wien....	2	34
76g Superior-Verdichter von Tecklenburg, Hamburg....	2	---
76h Tip-Top-Verdichter von KROTTENBERG, HAMBURG. von Knusser, Hamburg.....	2 2	35
76i Washington-Verdichter von Perotti & Cie., Hamburg.....	2	36
84a Die Di-Trigramm-Schlüsseltablel.....	1	31a
85 Verdichtung von Buchstaben-(Wort-)Sigeln regel- mässiger Bildung.....	2	32, 33,
78 a Verbergen (Tarnen) der Schlüssel.....	2	---

Diese Kapitel kommen in die "Systeme des Chiffrierens" nach den gleich nummerierten gedruckten Kapiteln einzuschalten.

F96

SYSTEME DES DECHIFFRIERENS.

INHALTSVERZEICHNIS

zum Hauptmanuskripte:

Kapitel	Seiten:	Beilage :
34a Die Enträtselung von Ungleichstellern.....	4	22a, I, 2.
42a B. Die Lösung mehrerer kurzer Schriften (Cronteld)....	2	31a,
46a Enträtselung von Sigelschriften nach Sigramm- tafeln.....	10	36a/3, b, c, a/2
46b Lösung von Bi-Trigrammtafeln.....	4	37a/2, b, c,
46a Enträtselung des russischen Cäsars.....	3	38 a, b, c,
56a Enträtselung des verbesserten Kihilisten- quadrates.....	1½	46 a, b, c,
64 zu Enträtselung mechanischer Verfahren, Ergänzung.....	3	-----
83 Die Lösung von Bigramm-Überschlüsseln....	9	76/7, 77 bis 81
84 Die Lösung von Bigrammüberschlüsseln bei Wechsel des Schifireschlüssels und der Tafel	6	82/4 bis 87
85 Die Lösung verzahnter Bigrammüberschlüssel..	6	88/5, 89, 90
86 Die Lösung verzahnter Bigrammüberschlüssel bei Schlüssel- und Tafelwechsel.....	1	91/5, 92, 93
87 Die Lösung von Sigelverdichtungen.....	1	94/2, 95
88 Untersuchung von Schriften auf Verdichtung	9	96/2, 97, 98, 99,
89 Untersuchung weiterer Schriften auf Verdich- tung.....	3	100/2, 101, 102,
90 Untersuchen von Superior-Schriften auf Ver- dichtung.....	1	103,
91 Untersuchen von Tip-Top-Schriften auf Ver- dichtung.....	1	104,
92 Untersuchen von Washington-Schriften auf Ver- dichtung.....	1	105,
93 Resumé aus diesen Untersuchungen.....	2	106,

Diese Kapitel sind im Hauptmanuskript nach den vorhergehenden Kapitel-
nummern, bezw. am Schlusse einzuräumen.