

An old challenge

Hans van der Meer

June 30, 2010

Abstract

ADDRESS: Straat van Magelhaens 7, 1183 HB Amstelveen, Netherlands. Email: H.vanderMeer@uva.nl

ABSTRACT: A cryptogram originating in the First World War appeared in the second volume of *Cryptologia* (1978). It is proved to be a Fuer God message by applying the keys recorded in the papers of the American cryptanalyst Lt. J. Rives Childs. These keys and the permuted alphabets employed in the Fuer God are presented here.

KEYWORDS: Cryptanalysis, First World War, Fuer God, Wilhelm cipher, Rives Childs, polyalphabetic substitution.

1 Introduction

In one of the first issues of *Cryptologia* H. Gary Knight started a series of articles titled “Cryptanalysts’ Corner.” They were accompanied by cryptograms left for the reader to solve. In the second volume the following cryptogram was presented as “Problem No. 11” [1].

```
ARVHL YMHE T AZITF AHETZ CCEHH HCALR CNPYN MYHGU FNJLS BGHGA
OUYSL JEIIO GADPH CVTAE HEZRY YTNJP KVAHJ EQGNX ZZYUP NSIJE
SZIRB YPMU EXRRY SLCIE TAFMD QYZMM FHVND XKJHN BWADO ZORDA
YICCH QTRCB NXJCG UMYJN RECZJ ULHNI UUTUV HSIGX SHIEF WYRUZ
CQJNZ SZUPA LGGPO VFACC DHVBS MPZJT SYHXW HTEVG OVALN WGADU
QPBDU XVRTD VTXQV AOXSW HTTUI GTPIR WIPCC LNIBJ EMJJY KQTGP
EKFZI WHQTU SKTPU GHJIM MDBJM PPNPW FIGDX ZJTGL WFRZC NRRPB
ULHEP RJKAR BJORR RRAHM GDBMO YGVGL MPRRI GCNPZ ZQEYP NCOLL
NKGUS MPUCK WXGRH QTQWR QNUKU ZFIBN XOXHU ILHYI DCKKJ NLZIB
FSQDZ HCKLH VUIDJ YKXSQ SLVYC BGXSH IEFWZ RMYTR EXTND LWZZN
SUFRY UVYCW GBVRT WYQVW HEXKO RTYYS HBYGK AOLSP HJBXE XYZCU
YHORZ BSMSG WTIZU JWFFI POZ
```

Gary Knight wrote that it was not an English but a German text and the editor added “This is an unsolved WWI German cipher received by the author.” At the time, I decided to take up the gauntlet and started an attempt to solve this challenge.

Being nearly 600 letters in length, statistical tests should be able to distinguish between a monoalphabetic and a polyalphabetic system. The phi test clearly indicated polyalphabeticity and also established a period of length 18. Seasoned cryptanalysts, of course, would have concluded this even without resorting to computers. Some conspicuous repetitions point to this period, especially the long one GXSHIEFW. Further analysis made it clear that this is not a simple Vigenère or Beaufort, but probably has differently mixed alphabets.

A second clue in the analysis is provided by the three letters POZ at the end of the cryptogram. As a separate closing group of three letters, it rather seems some sort of sender signature or call sign than part of the contents. Buying and reading David Kahn’s “The Codebreakers” now pays off its investment. His description of the Fuer God cipher immediately comes to mind [2]. This cipher was used for messages between the German relay station at Nauen and a station with the call sign GOD. Hence the name Fuer God. Another name for it is “Wilhem cipher.” The messages with call sign POZ could be attributed to a German expedition in Tripolis headed by a certain captain Von Todenwart. The objective of the expedition was to raise disaffection against the Allies among the Arabs of North Africa [3].

The Fuer God has been in use from 1916 to 1918. It is described as a polyalphabetic substitution with 27 mixed alphabets and 30 message keys, in length varying from 11–18 letters. At the end of the First World War American cryptanalysts arrived in Western Europe; among them J. Rives Child. Kahn tells us that Childs received the 22 alphabets that had been solved, as well as the message keys found. Childs then found out the words on which the message keys were based. Of these Kahn mentions GOLDARBEITER and INSTRUMENTENMACHER [4].

2 Solution of the Cryptogram

So far so good. The statistical calculations being consistent with a polyalphabetic of period 18, and this taken together with the POZ end group, raise high hopes of finding a Fuer God message here. Comparing the 18 distributions it even seems possible that its key is the aforementioned INSTRUMENTENMACHER! But there the buck stops. At least my limited

abilities as a cryptanalyst fail to solve the cryptogram by reconstructing the alphabets used. And thus this cryptogram rested for many years among my other doubtless interesting, but unsolved challenges.

This situation remained until a visit of David Kahn to the Netherlands on the occasion of the thesis of Karl de Leeuw [5]. I am grateful to David Kahn for communicating to me the place where the papers of J. Rives Childs are kept. Also I am indebted to the people of Randolph-Macon College who were so kind as to locate these papers and sent me a copy, as well as permitting me to publish their contents [6]. This information made it possible to establish the fact that the message is indeed a Furer God with key INSTRUMENTENMACHER. After decryption the following contents of this message is found.

ganz zuverlissiger vertrauensman meldet unterm dritten august:
italienischer dampfer sumatra soll demnchst rest des dritten erythraeischen bataillons und das sechzehnte bataillon und urlauber von libyen nach port said berfhren sowie von port said das erste elfte und zwlfte bataillon nach lybien bringen. das 16. batl. ist augenblicklich in benghasi. es soll durch das 12. ersetzt werden. die erythraeischen bataillone in lybien sind sehr geschwcht. das in lybien befindliche 15. batl. zahlt nur noch 250 mann. zwischen lybien und port said verkehrt alle zehn tage ein postdampfer. der auch fr truppen transporte benutzt wird. pol. 30 07 4.

3 Remarks to Childs notes

The keys and alphabets of the Furer God do not seem to have been published elsewhere. It therefore may be considered of interest to make Childs' original notes on this cipher available to interested readers and let Childs himself describe the cipher and the solution of the keywords.

The material in the J. Rives Childs Collection at Randolph-Macon College consists of a main document of which page one is headed "Explanation of the "Furer God" or "Wilhelm" Cipher" and signed "J. Rives Childs, 2nd Lt. 31st Inf. U.S.R. Radio Intelligence." This first page is followed by three pages numbered 2-4, summarily describing the solution of the German keywords. These pages list the original, partially solved alphabets (table 1) and the original, non-solved keys (table 2). It seems probable that they were the alphabets and keys originally given to Childs.

There are two additional, unnumbered pages. The first headed "Alphabets for use with "Wilhelm" Cipher," and the other "Keys for use with

Alphabets of "Wilhelm" Cipher". These two pages list the alphabets (table 3) and keys (table 4) as changed by solving the German key words.

In table 3 there are, apart from the fact that the empty positions of table 1 are filled in, a few additions and handwritten corrections which merit attention. In the numerals section of table 3 the typed text "W? - 4" was changed by hand to "G - 4" and "Y? - 6" to "Z - 6". Added by hand are "X - =,=" and "Y - =.=". In view of Childs' mentioning these punctuation marks on page 1 of his notes, this might suggest that he made the handwritten corrections himself. It is not known whether he himself typed the notes or had them typed and thereafter corrected them.

In the I-alphabet of table 3 the sequence SQ (also present in the corresponding E-alphabet in table 1) was changed by hand into QS. A stranger thing must have happened to the S-alphabet of table 1 which corresponds to the F-alphabet in table 3. In the latter 4 letters were crossed out and replaced by others, leading to an alphabet containing two letters F and missing a Q:

F- Q Y Z V X - B C E F D M J I G K A P L N S - - - - (typed)
 F- Q Y Z V X A B C E F D M J I G K A P L N S R O Y U T (handwritten)
 F- W Y Z V X A F C E F D H J I G K M P L N S R O Y U T (changed)

Finally it may be noted that the four key words missing from table 2 (the numbers 25, 26, 28 and 29) were added in handwriting to table 4. In the typed text key word no. 22 originally was VOLLWICHTIGES, but crossed out and replaced by GOLDARBEITER.

4 Childs notes

EXPLANATION OF THE "FUER GOD" OR "WILHELM" CIPHER

1. These messages are enciphered by means of two tables, one a primary table consisting of 27 mixed alphabets (23 of which have been reconstituted) and a secondary table which governs the number and position of the alphabets to be employed for each message, from 1-30 inclusive. (27 of these have been determined.)¹
2. For example, messages 1 and 31, 2 and 32, etc. always employ the same number of alphabets; and these alphabets are arranged in the one

¹In the list of keys appended to the main pages all 30 keys are given. It cannot be determined from this document whether these are added by Childs himself after typing up his description, or if another person filled them in later on.

position as if there were 30 fixed keywords, which always determined the number and juxtaposition of the alphabets from 1-31 or for any number in excess of 1-31 to which 30 had been added any number of times. For example, 1, 31, 61, 91, etc. are always enciphered by the same secondary table or arrangement of alphabets.

3. All numbers included in the message are enclosed on either side by "Q" and have been enciphered by a double process. First, the letters by which they are represented are deciphered with the body of the message, and then when the numbers have been identified by the "Q's" on either side, these letters enclosed by the "Q's" are re-deciphered according to the table for numbers from 1-10.
4. Punctuation marks are indicated sometimes by "X" and "Y" and sometimes by "X" and "Y" enclosed by "Q's". For example, "QXQ" or "QYQ".
5. The horizontal alphabet running above the primary table gives the value of the letters of the 23 mixed alphabets. The vertical alphabet gives the arbitrary symbol for identification of the alphabets in their proper position in the secondary table, this latter table, as stated, being determined by the number of the message.
6. To decipher any message, say, for example, a message numbered "47". This message has been enciphered by the same secondary table as "17". Let us say the first cipher letter is "P". Referring to table No. 17 we look for alphabet "B" in the vertical column, and running horizontally along this line until we have reached "P" we find the true value of "P" in the straight horizontal alphabet at the top of the table, "R", et cetera.

J. RIVES CHILDS
2nd Lt. 31st Inf. U.S.R.
Radio Intelligence.

The alphabet beginning "S Q R Y V" was known as the A alphabet, that beginning "L O P N M" as the B alphabet etc.

Messages numbered 1, 31, 61 etc. were decipherable by the alphabets J V C E P Q H C M P Q G P.

Messages numbered 2, 32, 62 etc. were decipherable by the alphabet T B U U L E N F K E Q G C.

Table 1: *Unordered alphabets.*

	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	NUMERALS
A-	S Q R Y V X U Z T W B D C A E J H K I F G P M O N L	H - 1
B-	L O P N M Q S R T U V Z X Y W C A B H E D G J F K I	P - 2
C-	P O N M R T S Q W Y U X Z V C A B E D F J G K H I L	J - 3
D-	I F H J G N K L M P O T S R Q V Y U X Z W D B C A E	W? - 4
E-	X U V Z Y W A C B E D G I H J F K M O N L T R S Q P	D - 5
F-	U X Z W Y V E A B C F D I H G J N K M L S P O R T Q	Y? - 6
G-	A C D B H J F I G E M N L K O T R S P Q Y Z V U X W	V - 7
H-	B A D C F G E I H J N O K M L S R P T Q W X Z	R - 8
I-	T R S Q Y W X Z V U E B A C D K F J I G H M L O	A - 9
J-	L M O N T Q R P S Z X U Y V W B A C D E G J H F K I	F - 0
K-	M O K N L Q S R P W Z T V U X Y D B A C E F J G I H	
L-	I E H F G L O M J K N Q P T R S X V Y U Z B C	
M-	H F I G N M J K O L Q P S R V T Z U W X Y B E A	
N-	C D A B G H E J F I K M P O L N T R Q S X U Z W V Y	
O-	E C D B A F J I G H L K O N M S P Q T R Z U X V W Y	
P-	R Q P S Z W T V U X Y D B C A G I E J H K F O N L M	
Q-	V Y X U Z W C A B E D I H G F L K N M J Q O T P S R	
R-	B A C H D J F E G I L O N P K M S Q R U Z T Y X	
S-	Q Y Z V X B C E F D M J I G K A P L N S	
T-	E D I G H F L M K P O N R Q X T Z W V C A B	
U-	R T S W V Y Z U X F A C D E B J K I G H O N M P Q L	
V-	M O L N P S R Q X T Y W Z U V A D C B H F I K G	
W-		
X-		
Y-		
Z-		

It will be noticed that the same alphabets as P, for instance, in message 1² is repeated three different times and there are also other repetitions such as C and Q. Again, the E and Q and G which occur in 1 occur also in 2.

From the appearance of certain of the letters, the frequency for example of G and the inseparable combinations NF and NA, N never appearing unless followed by F or A, it was thought extremely probable that these letters arbitrarily chosen to represent the 22 different alphabets in reality represented key words of intelligible German text.

N was taken to represent C and F, H and G, the most frequent letter

²Obviously meant is key 1 in table 2.

Table 2: *List of the original key words.*

1	JVCEPQHCOMPQGP	11	ABCADEGFGC	21	VSGORGTGCIEGKGC
2	TBUULENFKEQGJ	12	DMNAGCDOPQG	22	TBUULENFKEQGJ
3	VCBHEGCJKGEP	13	JNFLEGGCTOKGC	23	FOPRUMPQJQGFEUSG
4	IOCEBPGKKGPJVEGUGC	14	LEGUOPQGROMGCKGJ	24	EOPRJNFMFIONFGC
5	HGJKEIIMPQJBCK	15	LEGTEGUABJKGKGJ	25	
6	SOFCKMPKGCHCGNFMPQ	16	SCGIRGPHMNF	26	
7	LOQGPLGNFJGU	17	HGPGREAKEPGC	27	COREGCQMIIE
8	LBUUGPJEGSOFCEGP	18	JGUKGCLOJJGC	28	
9	PBNFGKLOJIEUNF	19	HGELGIAOMSGPJEG	29	
10	GJJNFIGNAKIEC	20	OVOEGCFOPRUMQ	30	CGNFKJJQGUGFCKGC

which was never absent from any of the series, E. This simple substitution was continued until familiar German syllables began to appear and finally the complete key words themselves.

The values were found to be:

A-K	H-B	O-A	B-O	I-M	P-N
C-R	J-S	Q-G	D-Z	K-T	R-D
E-I	L-W	S-F	F-H	M-U	T-V
G-E	N-C	U-L	V-P		

J. RIVES CHILDS
2nd.Lt. Inf.

5 References

1. Knight, H. Gary. 1978. *Cryptanalysts' Corner*, Cryptologia Vol.2 (1978): 239–240.
2. Kahn, D. 1967. *The Codebreakers*, New York, Macmillan: 310-311.
3. Childs, J. Rives 1978. *My Recollections of G.2 A.6*, Cryptologia Vol.2 (1978): 201–214.
4. Kahn, D. 1967. *The Codebreakers*. New York, Macmillan: 337.
5. Leeuw, K. de. 2000. *Cryptology and Statecraft in the Dutch Republic*, Thesis University of Amsterdam, ISBN 90-57760-39-8.
6. Childs, J. Rives. *Explanation of the "Fuer God" or "Wilhelm" Ciphers*, ts. J. Rives Childs Collection, McGraw-Page Lib., Randolph-Macon Coll., Ashland, VA.

Table 3: Alphabets for use with "Wilhelm" Cipher.

	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	NUMERALS
A-	E C D B A F J I G H L K O N M S P Q T R Z U X V W Y	H - 1
B-	B A D C F G E I H J N O K M L S R P T Q W X V Y U Z	P - 2
C-	C D A B G H E J F I K M P O L N T R Q S X U Z W V Y	J - 3
D-	B A C H D J F E G I L O N P K M S Q R U Z T Y V W X	G - 4
E-	A C D B H J F I G E M N L K O T R S P Q Y Z V U X W	D - 5
F-	W Y Z V X A F C E F D H J I G K M P L N S R O Y U T	Z - 6
G-	V Y X U Z W C A B E D I H G F L K N M J Q O T P S R	V - 7
H-	U X Z W Y V A E B C F D I H G J N K M L S P O R T Q	R - 8
I-	X U V Z Y W A C B E D G I H J F K M O N L T R Q S P	A - 9
J-		F - 0
K-	S Q R Y V X U Z T W B D C A E J H K I F G P M O N L	X - ,
L-	R T S W V Y Z U X F A C D E B J K I G H O N M P Q L	Y - .
M-	T R S Q Y W X Z V U E B A C D K F J I G H M L P N O	
N-	R Q P S Z W T V U X Y D B C A G I E J H K F O N L M	
O-	L O P N M Q S R T U V Z X Y W C A B H E D G J F K I	
P-	M O L N P S R Q X T Y W Z U V A D C B H F I K E J G	
Q-		
R-	P O N M R T S Q W Y U X Z V C A B E D F J G K H I L	
S-	L M O N T Q R P S Z X U Y V W B A C D E G J H F K I	
T-	M O K N L Q S R P W Z T V U X Y D B A C E F J G I H	
U-	H F I G N M J K O L Q P S R V T Z U W X Y B E D C A	
V-	E D I G H F L M K P O N R Q J S U X T Z W V Y C A B	
W-	I E H F G L O M J K N Q P T R S X V Y U Z W B A D C	
X-		
Y-		
Z-	I F H J G N K L M P O T S R Q V Y U X Z W D B C A E	

Table 4: *Keys for use with Alphabets of "Wilhelm" Cipher.*

1	SPRINGBRUNNEN	11	KORKZIEHER	21	PFERDEVERMIETER
2	VOLLWICHTIGES	12	ZUCKERZANGE	22	GOLDARBEITER
3	PROBIERSTEIN	13	SCHWIEGERVATER	23	HANDLUNGSGEHILFE
4	MARIONETTENSPIELER	14	WIELANGEDAUERTES	24	HANDSCHUHMACHER
5	BESTIMMUNGSORT	15	WIEVIELKOSTETES	25	INSTRUMENTENMACHER
6	FAHRTUNTERBRECHUNG	16	FREMDENBUCH	26	KAMELTREIBER
7	WAGENWECHSEL	17	BENEDIKTINER	27	RADIERGUMMI
8	WOLLENSIEFAHREN	18	SELTERRASSER	28	BESORGEDIEPFERDE
9	NOCHETWAS MILCH	19	BEI WEM KAUFENSIE	29	DUNKELKAMMER
10	ESSCHMECKTMIR	20	PAPIERHANDLUNG	30	RECHTSGELEHRTER

BIOGRAPHICAL SKETCH

Hans van der Meer has been working at the University of Amsterdam in the faculty of Mathematics and Computer Science as a teacher of computer science, cryptography, and computer security. After his retirement he continued teaching his course on cryptography.