Eavesdropping on the Biafra-Lisbon Link – Breaking Historical Ciphers from the Biafran War

R. W. Bean[a], G. Lasry[b] and F. Weierud[c]

[a]School of ITEE, University of Queensland, Brisbane, 4072, Queensland, Australia; [b]The DECRYPT/CrypTool Projects, Germany; [c]Crypto Cellar Research, Oslo, Norway

ARTICLE HISTORY
Compiled May 13, 2020

ABSTRACT
The Biafran War, or Nigerian Civil War from 1967-1970 was a significant conflict in post-colonial African history. We obtained encrypted messages sent from Lisbon to Biafra via telex during the conflict. We employed manual and computerized cryptanalysis methods to decipher a series of transposition ciphers sent by Biafran officials in 1968 and 1969, which were encrypted using unknown variants of columnar transposition. We then derived the keywords the system was based on and the method used, and analyzed the codewords, names and traffic contained in the plaintexts. Some five-figure ciphers sent during the same period remain unsolved.

KEYWORDS
Biafra, Nigeria, columnar transposition, hillclimbing, cryptanalysis

1. Introduction

During the period from July 1967 to January 1970 the secessionist state of Biafra was involved in a conflict with the Nigerian Federal Government. The Republic of Biafra was proclaimed on 30 May 1967 by Colonel Odemegwu Ojukwu, a former military governor of the eastern region of Nigeria. After thirty months, Biafra surrendered and was incorporated again into Nigeria. According to the historian de St Jorre (1972), between half a million and a million Nigerians died, mainly from starvation, during the war.

Through the efforts of their roving diplomats during the war, Biafra achieved recognition from the states of Tanzania, Gabon, Haiti, Ivory Coast, and Zambia. Biafra also struggled to secure diplomatic and military support, purchase weapons, and smuggle them into its controlled territory via airlift. The efforts of the diplomats have recently come to light through the decryption of telexes sent from Portugal to Biafra during the war. The telexes were intercepted by professionals: the Swedish FRA[1] Grahn (2019) and the US Central Intelligence Agency (CIA) Kriebel (1968b). Some of them were also intercepted by at least one amateur radio operator, Frode Weierud. The transcriptions available can be found on the CryptoCellar website (Weierud (2019)).

CONTACT R. W. Bean: r.bean1@uq.edu.au; G. Lasry: george.lasry@gmail.com; F. Weierud: frode.weierud@gmail.com

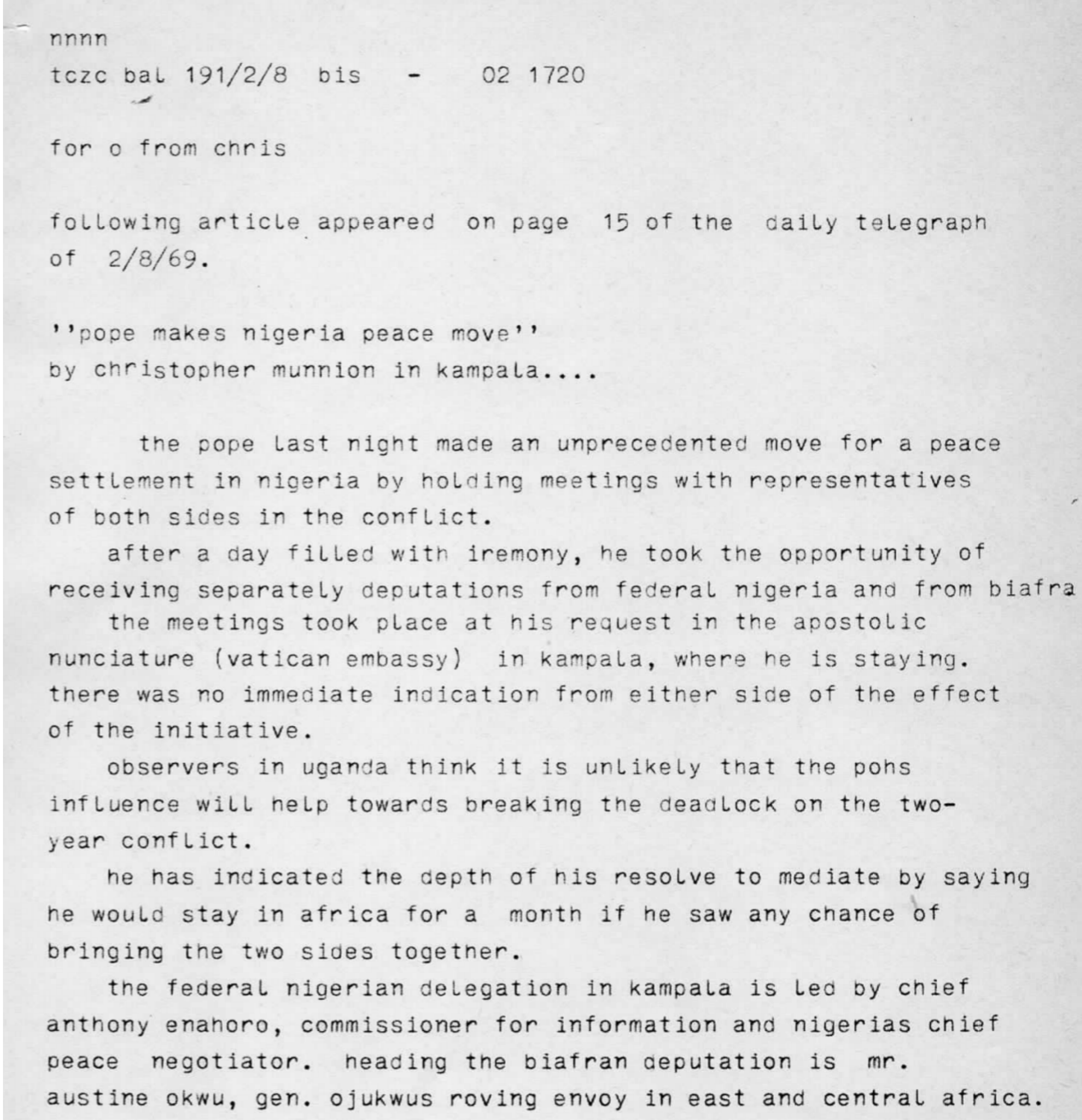
[1] Försvarets radioanstalt, the National Defence Radio Establishment - the Swedish signals intelligence agency

The remainder of this article is structured as follows: In Section 2, we describe the interception of the telex messages sent via the Lisbon link, and in Section 3, how we deciphered most of them via cryptanalysis. In Section 4 we present our interpretations of names and codewords that appear in the decrypted messages. In Section 5 we describe how we identified the various callsigns. In Section 6, we highlight some of the contents of the messages. We conclude our findings in Section 7. In the appendices, a personal account of the interception process is given, as well as a description of ITU telex channel indicators.

Note about notation: Elements of text extracted from ciphertexts, or excerpts from plaintexts are written in `monospace font`.

2. Intercepting Enciphered Messages from the Lisbon Telex Link

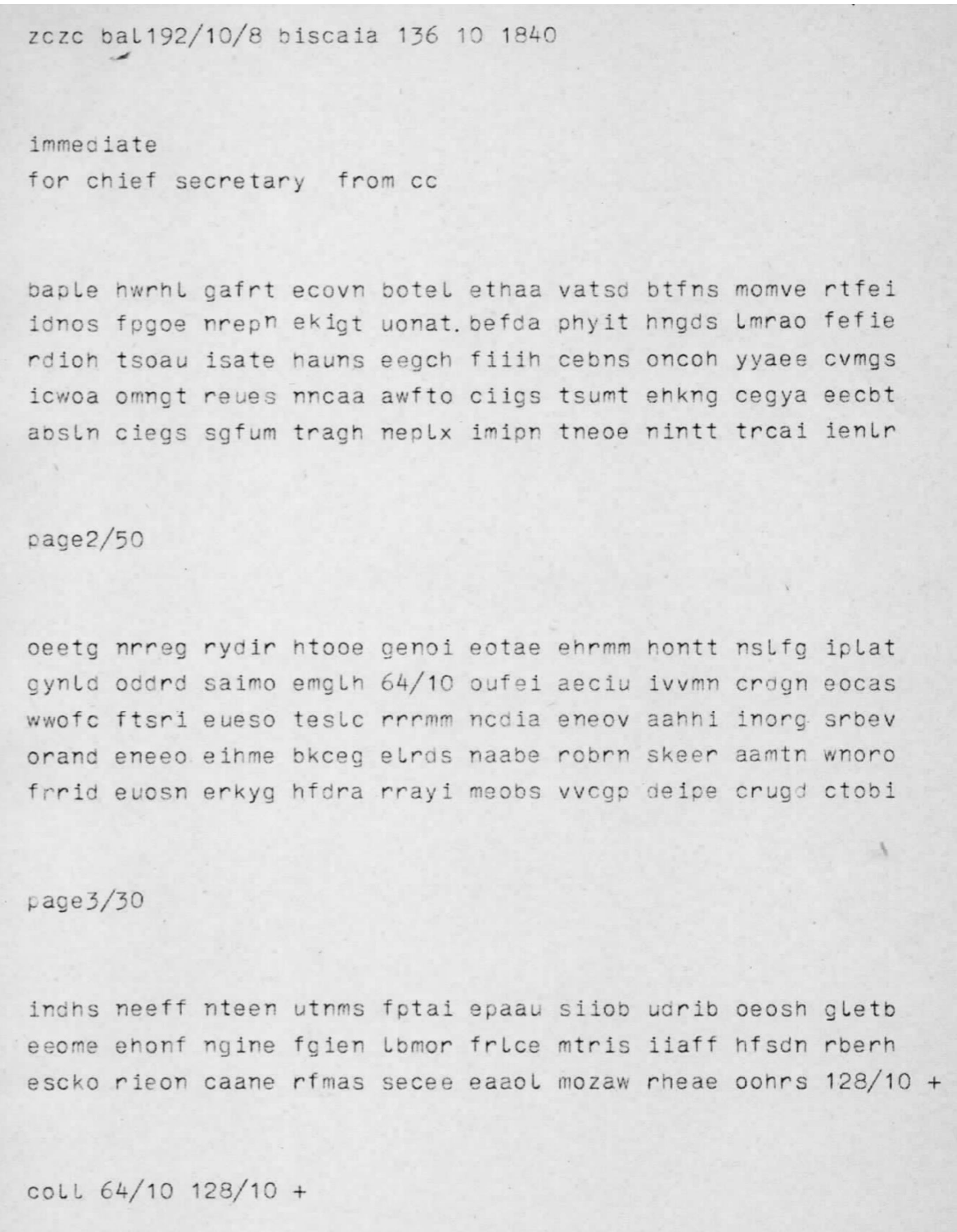
Frode Weierud, at the time an engineering student and radio enthusiast living in Oslo, intercepted a series of telex messages sent on short-wave frequencies in the months of August and October 1969. These appeared to be related to the secessionist state of Biafra, formerly part of Nigeria. The first message was in English plaintext and labelled “`BAL191 - FOR O FROM CHRIS`”, as shown in Figure 1.



```
nnnn
tczc bal 191/2/8  bis    -    02 1720

for o from chris

following article appeared  on page  15 of the  daily telegraph
of  2/8/69.

''pope makes nigeria peace move''
by christopher munnion in kampala....

      the pope last night made an unprecedented move for a peace
settlement in nigeria by holding meetings with representatives
of both sides in the conflict.
    after a day filled with iremony, he took the opportunity of
receiving separately deputations from federal nigeria and from biafra
    the meetings took place at his request in the apostolic
nunciature (vatican embassy)  in kampala, where he is staying.
there was no immediate indication from either side of the effect
of the initiative.
    observers in uganda think it is unlikely that the pohs
influence will help towards breaking the deadlock on the two-
year conflict.
    he has indicated the depth of his resolve to mediate by saying
he would stay in africa for a  month if he saw any chance of
bringing the two sides together.
    the federal nigerian delegation in kampala is led by chief
anthony enahoro, commissioner for information and nigerias chief
peace  negotiator.  heading the biafran deputation is  mr.
austine okwu, gen. ojukwus roving envoy in east and central africa.
```

Figure 1. BAL191 - cleartext message (Source: Frode Weierud)

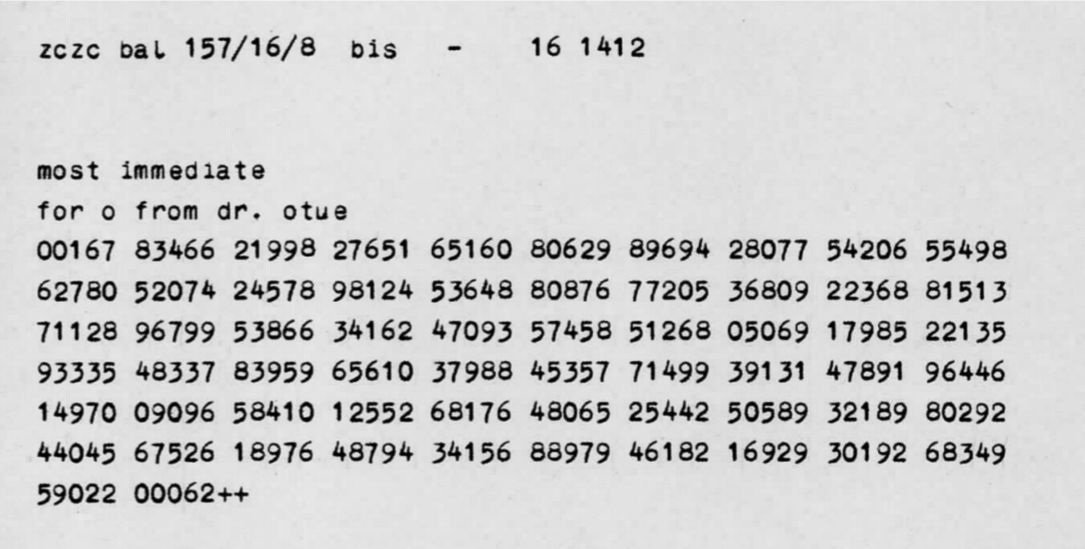
The first messages intercepted were in plaintext, but soon messages started arriving in ciphertext, in both five-letter and five-figure groups. For example, the message "`BAL192 - FOR CHIEF SECRETARY FROM CC`", shown in Figure 2, arrived on 10 August. The message was across three teleprinter pages, and consisted of 128 five letter groups. In the middle `64/10` appeared to mark the half-way point and `128/10` appeared at the end for a check. The `10` referred to the day of the month while `128` was the total number of five-letter groups. Based on the frequency of the letters, it appeared these messages were also in English.



```
zczc bal192/10/8 biscaia 136 10 1840


immediate
for chief secretary  from cc


baple hwrhl gafrt ecovn botel ethaa vatsd btfns momve rtfei
idnos fpgoe nrepn ekigt uonat.befda phyit hngds lmrao fefie
rdioh tsoau isate hauns eegch fiiih cebns oncoh yyaee cvmgs
icwoa omngt reues nncaa awfto ciigs tsumt ehkng cegya eecbt
absln ciegs sgfum tragh neplx imipn tneoe nintt trcai ienlr


page2/50


oeetg nrreg rydir htooe genoi eotae ehrmm hontt nslfg iplat
gynld oddrd saimo emglh 64/10 oufei aeciu ivvmn crdgn eocas
wwofc ftsri eueso teslc rrrmm ncdia eneov aahhi inorg srbev
orand eneeo eihme bkceg elrds naabe robrn skeer aamtn wnoro
frrid euosn erkyg hfdra rrayi meobs vvcgp deipe crugd ctobi


page3/30


indhs neeff nteen utnms fptai epaau siiob udrib oeosh gletb
eeome ehonf ngine fgien lbmor frlce mtris iiaff hfsdn rberh
escko rieon caane rfmas secee eaaol mozaw rheae oohrs 128/10 +


coll 64/10 128/10 +
```

Figure 2. BAL192 - ciphertext with five-letter groups (Source: Frode Weierud)

Another message labelled "`BAL157 - FOR O FROM DR OTUE`" arrived on 16 August. It was in a five-figure cipher with 62 groups, as shown in Figure 3.



```
zczc bal 157/16/8  bis   -    16 1412


most immediate
for o from dr. otue
00167 83466 21998 27651 65160 80629 89694 28077 54206 55498
62780 52074 24578 98124 53648 80876 77205 36809 22368 81513
71128 96799 53866 34162 47093 57458 51268 05069 17985 22135
93335 48337 83959 65610 37988 45357 71499 39131 47891 96446
14970 09096 58410 12552 68176 48065 25442 50589 32189 80292
44045 67526 18976 48794 34156 88979 46182 16929 30192 68349
59022 00062++
```

Figure 3. BAL157 - ciphertext with five-figure groups (Source: Frode Weierud)

Considering only the five-letter messages, the first set of 15 messages in 30 parts was received between 2-16 August 1969 and the second set of 9 messages in 11 parts from 19-21 October 1969. The message headers label the messages beginning `BAL` or `BIS`. `BIS` is thought to stand for "Biscaia" as in the "Bay of Biscay" beside France and Spain; the word had appeared in cleartext (e.g. message BAL089).

The messages were from what has been called the "Lisbon telex link" mentioned in (Stremlau 2015, p. 113). Biafra had only one telex machine and this provided the only link for communications to and from the outside world. Biafra was engaging the services of a public relations firm in Geneva, Markpress, to pass on information about the war in Biafra to members of parliaments and the public in Europe via the mass media, and many of the messages were intended for wide public distributions. Other encrypted messages were between Biafran diplomats in European cities (Lisbon, Paris, London, Frankfurt, Rome and other major cities) and the leaders of Biafra.

The Lisbon telex was located at the Biafran delegation house at 16 Avenida da Torre de Belém as mentioned in Freire (2017), Ângelo (2019) and Iroh (1976). Due to the fact that the radio signals from Lisbon could be received so well in Oslo, we are convinced they cannot have used any form of directional antennas. Most likely they used dipole antennas which radiated equally well in the North-South direction. The Biafran delegation house was a villa with a large garden well suited for such an antenna. Based on six different sources, we can conclude that the Biafran side of the telex link moved around during the war, and was located in Uli, Aba, and Umuahia at various times.

(1) Kirk-Greene (1971) implies that the Biafran telex machine was in Uli at the end of the war and went dead in January 1970. "[Uli] was finally in danger along with the Lisbon telex".
(2) This is backed up by Winnipeg Free Press 1970 stating: "The radio and teleprinter link with Biafra via Lisbon went dead on Monday morning Jan 12." (Although (Grahn 2019, p. 217) stated the last telegram FRA received was dated 30 January 1970.)
(3) Time Magazine (1970) stated "The last telex message from Biafra to Markpress, a Geneva public relations firm that has handled the Biafra account with skill,

said tersely: “Despite widespread rumors to the contrary, the airstrip at Uli is functioning normally.” Next day it fell and with it the nation that it had kept barely alive for so long.”

(4) Onwumechili (2000) noted “Telex links with the outside world and Radio Biafra station, which were constantly re-located, were effectively maintained throughout the war.”

(5) The Express (1968) said “Umuahia will be the only telex connecting Biafra to the world”.

(6) Special Libraries Association (1971) wrote “[in 1967 it] was to Aba that the Ministry of Information, the directorate of propaganda, and Biafra’s important telex machine were moved.”

A personal account of the interception process can be found in Appendix A. As far as the authors are aware, until contents of some of the messages were summarized in Grahn (2019), there were no mentions of the ciphers in any public writings in any language. Grahn does not discuss the deciphering methods used or describe success rates, and the only piece of information from the book that touched on methods was that a “transposition specialist” at the FRA worked on the ciphers. The FRA no longer has any of the original ciphertexts. In further sections, we touch upon the list of codewords and names Grahn compiled for his book.

Appendix B contains an attempt at traffic analysis to identify the origin of the messages, from where they were sent, by whom they were sent and to whom they were addressed. The intention is to clarify the extent and size of the Biafran overseas communication network.

3. Deciphering the Cryptograms

In this section, the process of deciphering the letter ciphertexts is described, highlighting the various steps towards the solution, including:

- Transcription and OCR, to allow for computerized cryptanalysis (in Section 3.1).
- An overview of the messages with dates of transmission, group and part counts (Section 3.2).
- A preliminary analysis, which led to the conclusion that a transposition cipher was involved (Section 3.3). An overview of the classical columnar transposition cipher is also given, as well as known methods for its cryptanalysis (Section 3.4).
- Identifying group count markers (Section 3.5).
- An initial breakthrough and the first two solutions (Section 3.6).
- A second breakthrough and the partial recovery of the plaintexts for five additional messages that match a certain scenario (Section 3.7), followed by the reconstruction of their full plaintexts using manual methods (Section 3.8).
- Reconstructing the encryption scheme (Section 3.9).
- Recovering additional keys under various scenarios (Sections 3.10, 3.11, and 3.12).
- Reconstructing the indicator system, found to be comprised of a base key and a per-message key, and correcting errors in previously recovered keys (Section 3.13).
- Solving three earlier messages that illustrate the evolution of the encryption scheme (Section 3.14).
- Formatting the decrypts and correcting errors, to assist in the analysis of their

contents (Section 3.15).

As a result, all the ciphertexts with five-letter groups can be deciphered and read in clear.

The five-figure ciphertexts were also analyzed but could not be deciphered (Section 3.16).

3.1. *Transcription and OCR*

As a first step, we transcribed the cipher printouts with the aid of Google Docs OCR. Some messages had been received multiple times, which aided reconstruction when errors in transmission or reception had occurred. Further corrections were made to the transcriptions, as progress was made in deciphering the messages.

3.2. *Overview*

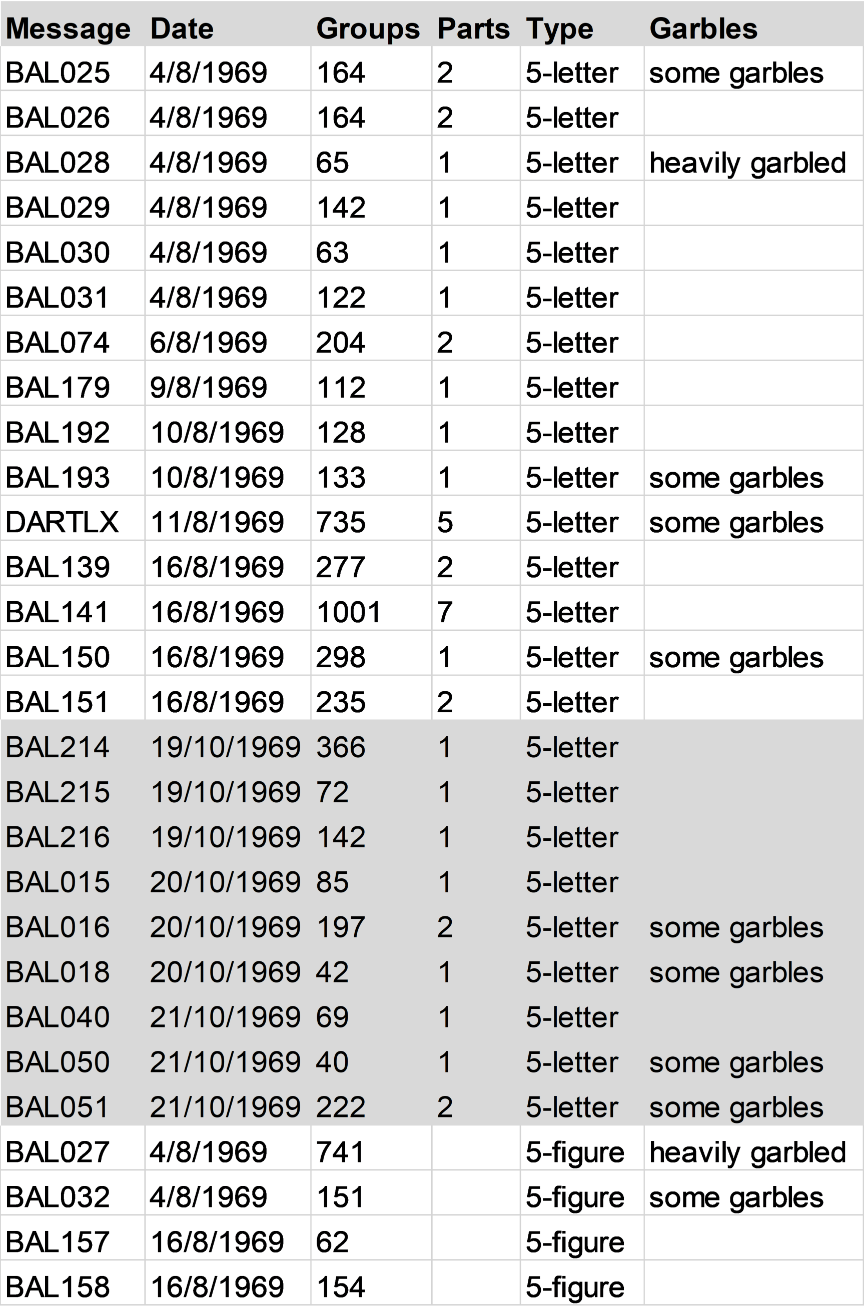
The five-letter messages intercepted by Frode Weierud in August and October 1969 consisted of 24 messages in 41 parts, as previously explained.

Generally, transposition ciphers are more tolerant to garbles, because the letters of a garbled group are spread throughout the plaintext and usually only affect one letter of a given plaintext word. Garbled five-letter groups only affect specific columns in the transposition rectangle (see Section 3.4). As long as there are not too many garbled columns, it is possible to correct the resulting decryption errors, based on adjacent columns in the transposition rectangle.

Also, some five-letter messages were repeated several times and from the multiply received messages, it was often possible to assemble a complete message without garbles.

A total of four five-figure messages were also received in August 1969 - BAL027, BAL032, BAL157, and BAL158. Of these, BAL157 and BAL158 were in almost perfect condition. BAL027 and BAL032 were garbled, with the group count of BAL027 indicating the complete message consisted of 741 groups, and the count of BAL032 listed as 151 groups. After removing errors, only 489 or 148 total or partial groups were present, respectively, including the group count.

A summary of the dates, group and part counts, type and garbles may be found in Figure 4. Further detail on the message contents, senders, and origin may be found in Appendix B.

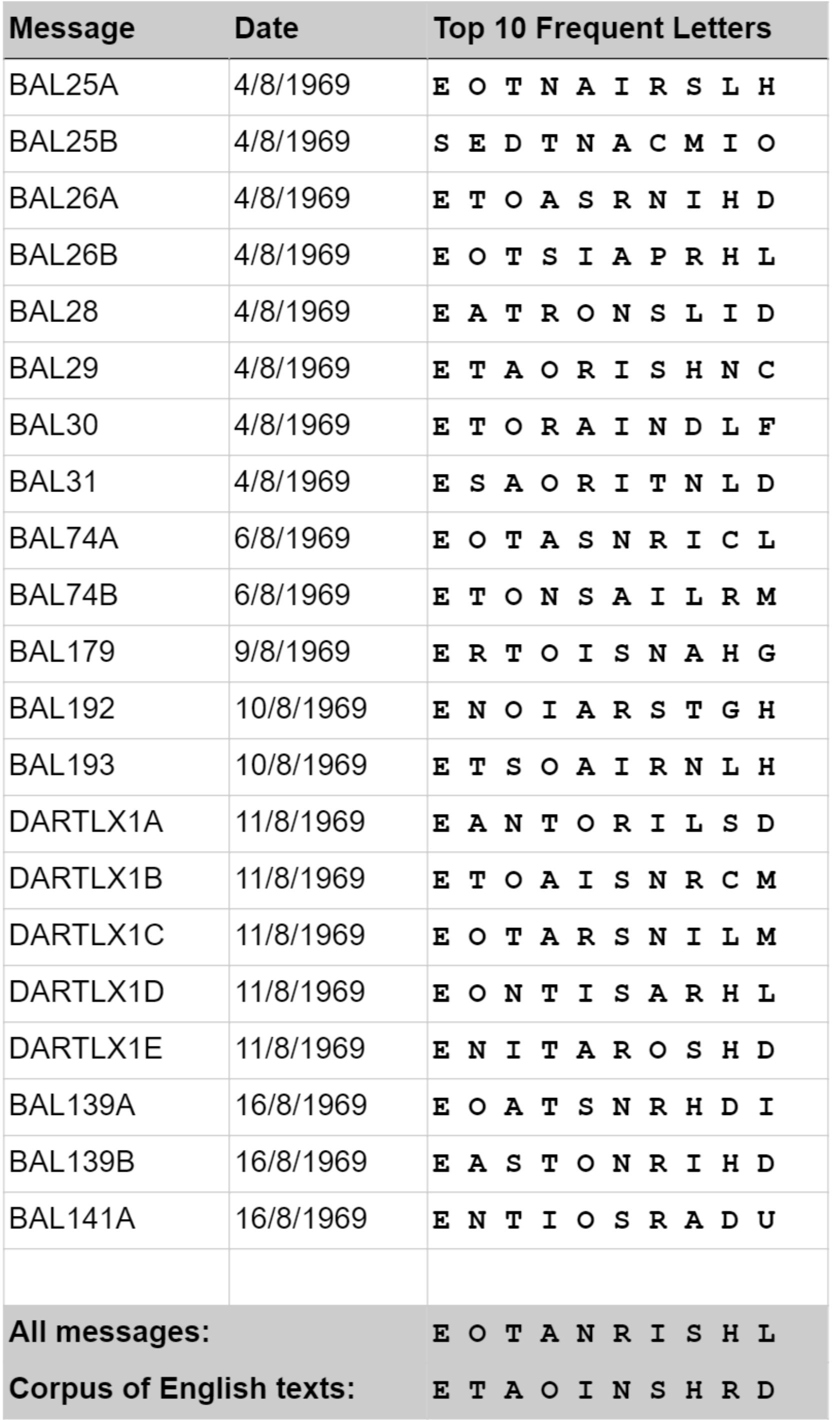


Message	Date	Groups	Parts	Type	Garbles
BAL025	4/8/1969	164	2	5-letter	some garbles
BAL026	4/8/1969	164	2	5-letter	
BAL028	4/8/1969	65	1	5-letter	heavily garbled
BAL029	4/8/1969	142	1	5-letter	
BAL030	4/8/1969	63	1	5-letter	
BAL031	4/8/1969	122	1	5-letter	
BAL074	6/8/1969	204	2	5-letter	
BAL179	9/8/1969	112	1	5-letter	
BAL192	10/8/1969	128	1	5-letter	
BAL193	10/8/1969	133	1	5-letter	some garbles
DARTLX	11/8/1969	735	5	5-letter	some garbles
BAL139	16/8/1969	277	2	5-letter	
BAL141	16/8/1969	1001	7	5-letter	
BAL150	16/8/1969	298	1	5-letter	some garbles
BAL151	16/8/1969	235	2	5-letter	
BAL214	19/10/1969	366	1	5-letter	
BAL215	19/10/1969	72	1	5-letter	
BAL216	19/10/1969	142	1	5-letter	
BAL015	20/10/1969	85	1	5-letter	
BAL016	20/10/1969	197	2	5-letter	some garbles
BAL018	20/10/1969	42	1	5-letter	some garbles
BAL040	21/10/1969	69	1	5-letter	
BAL050	21/10/1969	40	1	5-letter	some garbles
BAL051	21/10/1969	222	2	5-letter	some garbles
BAL027	4/8/1969	741		5-figure	heavily garbled
BAL032	4/8/1969	151		5-figure	some garbles
BAL157	16/8/1969	62		5-figure	
BAL158	16/8/1969	154		5-figure	

Figure 4. Message overview summary

3.3. *Preliminary Analysis*

A frequency analysis had already been conducted around the time the ciphertexts were intercepted, in an attempt to identify the type of cipher employed. Figure 5 shows the most frequent letters in a sample of messages, across all the messages, and in a corpus of English texts:



Message	Date	Top 10 Frequent Letters
BAL25A	4/8/1969	E O T N A I R S L H
BAL25B	4/8/1969	S E D T N A C M I O
BAL26A	4/8/1969	E T O A S R N I H D
BAL26B	4/8/1969	E O T S I A P R H L
BAL28	4/8/1969	E A T R O N S L I D
BAL29	4/8/1969	E T A O R I S H N C
BAL30	4/8/1969	E T O R A I N D L F
BAL31	4/8/1969	E S A O R I T N L D
BAL74A	6/8/1969	E O T A S N R I C L
BAL74B	6/8/1969	E T O N S A I L R M
BAL179	9/8/1969	E R T O I S N A H G
BAL192	10/8/1969	E N O I A R S T G H
BAL193	10/8/1969	E T S O A I R N L H
DARTLX1A	11/8/1969	E A N T O R I L S D
DARTLX1B	11/8/1969	E T O A I S N R C M
DARTLX1C	11/8/1969	E O T A R S N I L M
DARTLX1D	11/8/1969	E O N T I S A R H L
DARTLX1E	11/8/1969	E N I T A R O S H D
BAL139A	16/8/1969	E O A T S N R H D I
BAL139B	16/8/1969	E A S T O N R I H D
BAL141A	16/8/1969	E N T I O S R A D U
All messages:		E O T A N R I S H L
Corpus of English texts:		E T A O I N S H R D

Figure 5. Letter frequencies

It can be seen that the top letters are usually those expected in English texts, with some minor differences, like a higher prevalence of the letter O in the Biafran ciphertexts. Such a similarity is highly indicative of a transposition cipher, with underlying English plaintexts. This hypothesis was also supported by the fact that the Biafran ciphers were processed in the FRA, the Swedish SIGINT organization, by an expert on transposition ciphers.

In a transposition cipher, the plaintext elements are reordered, or transposed into different positions. This is in contrast with substitution ciphers, in which the elements are replaced with their respective substitutes. There are several types of transposition ciphers. Those include:

- The Columnar Transposition cipher, described in Section 3.4 and in Lasry, Kopal, and Wacker (2016).
- Double Transposition, in which two steps of columnar transposition are applied, using the same key or two different keys (see Lasry, Kopal, and Wacker (2014)).
- Other variants such as the Grille ciphers, Rail Fence ciphers, and Route ciphers (see Friedman (1941)).

The main weakness of transposition ciphers is that they do not conceal the original plaintext elements. A generic method to attack transposition ciphers is anagramming, i.e., sliding segments of ciphertext around, looking for sections that look like anagrams of English words or parts of words, and solving the anagrams.

Anagramming is more effective when applied in parallel to multiple ciphertexts that have the same length and are the result of different plaintexts being encrypted using the same key. This process is also known as Multiple Anagramming and it is described in Bauer (2002).

It is also possible to combine transposition and substitution in a composite cipher, such as the ADFGVX cipher (described in Lasry et al. (2017)), and in that case, anagramming does not work anymore.

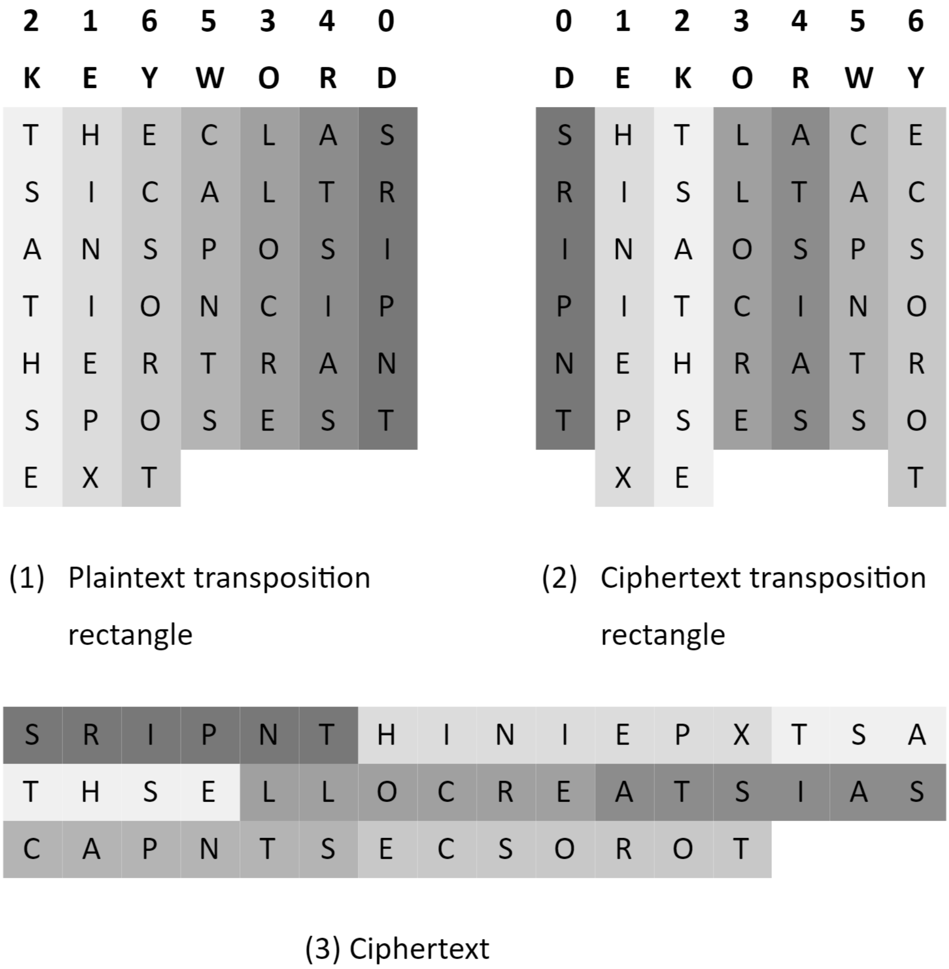
At this stage of the project, it was not clear what type of transposition might have been used, but as the columnar transposition cipher was historically the most widely used, it made sense to evaluate it first. The columnar transposition cipher and methods for its cryptanalysis are presented in the next section.

3.4. *The Columnar Transposition Cipher*

The columnar transposition cipher historically was and still is the most commonly used type of transposition cipher. Its working principle is simple. An example of encryption is illustrated in Figure 6.

Important note: In this paper, numerical transposition keys are indexed starting from 0, e.g., (2, 1, 6, 5, 3, 4, 0).[2]

[2] In the literature about columnar transposition ciphers, keys are usually indexed starting from 1, as this notation is more intuitive when illustrating a manual cryptanalysis method. In contrast, computerized algorithms employ numerical key values starting from 0, for convenience.



2	1	6	5	3	4	0
K	**E**	**Y**	**W**	**O**	**R**	**D**
T	H	E	C	L	A	S
S	I	C	A	L	T	R
A	N	S	P	O	S	I
T	I	O	N	C	I	P
H	E	R	T	R	A	N
S	P	O	S	E	S	T
E	X	T				

(1) Plaintext transposition rectangle

0	1	2	3	4	5	6
D	**E**	**K**	**O**	**R**	**W**	**Y**
S	H	T	L	A	C	E
R	I	S	L	T	A	C
I	N	A	O	S	P	S
P	I	T	C	I	N	O
N	E	H	R	A	T	R
T	P	S	E	S	S	O
	X	E				T

(2) Ciphertext transposition rectangle

S	R	I	P	N	T	H	I	N	I	E	P	X	T	S	A
T	H	S	E	L	L	O	C	R	E	A	T	S	I	A	S
C	A	P	N	T	S	E	C	S	O	R	O	T			

(3) Ciphertext

Figure 6. Incomplete columnar transposition

First, a transposition key must be selected and must be known by the transmitting side who encrypts the message and the receiving side who decrypts it. The transposition key consists of a series of numbers, specifying how the columns of the plaintext should be transposed or permuted. This key may be derived from a keyword (for short keys) or for longer keys, from key phrases, as those are easier to memorize than numerical keys.

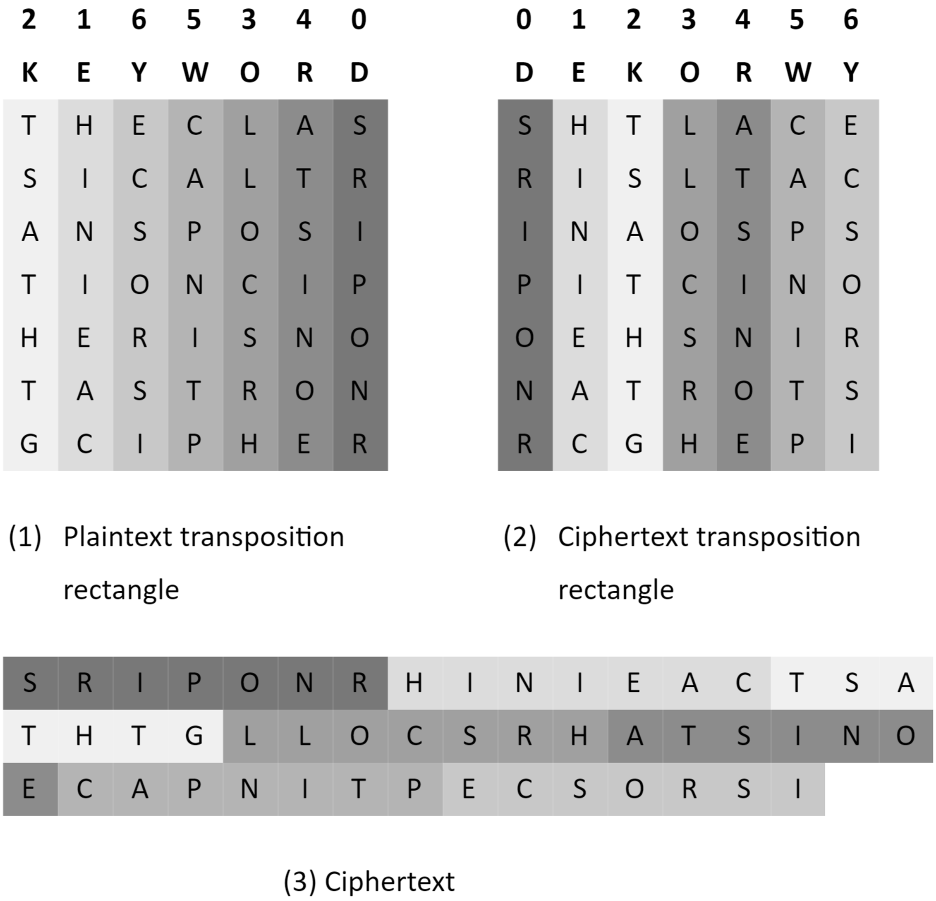
In case a keyword (or key phrase) is used, the equivalent numerical key is extracted by assigning each letter of the keyword a numerical value which reflects the relative position of the letter in the alphabet, from A to Z. In our example, the keyword is `KEYWORD`. `D` is the first of the keyword letters to appear in the alphabet, so it is assigned a numerical value of 0. `E` is the next letter and it is assigned the numerical value 1, and so on, until we obtain the full numerical key (2, 1, 6, 5, 3, 4, 0). In case a letter appears more than once in a keyword, successive numerical values are used. For example, the numerical key for the keyword `SECRET` would be (4, 1, 0, 3, 2, 5), with successive values 1 and 2 used to represent the letter `E` which appears twice.

To encrypt a plaintext, we first copy the plaintext, line by line, into a plaintext rectangle. The width of the rectangle is equal to the length of the key. On top of the rectangle, we inscribe the keyword, and on top of the keyword, we inscribe the equivalent numerical key. This is illustrated in part (1) of Figure 6. Note that the last rows of the rectangle are incomplete, and therefore the first three columns of the transposition rectangle, before transposition, are longer (by one row) than the other four columns. This case is referred to as an incomplete transposition rectangle or irregular columnar transposition (ICT). The case where all columns are of the same length and all rows are complete is referred to as complete columnar transposition (CCT). We use this terminology throughout this article.

Next, we transpose or reposition the columns according to the transposition key to form the ciphertext rectangle, as shown in part (2) of Figure 6. Plaintext column 0 is copied to column 2 in the ciphertext rectangle, plaintext column 1 to column 1, plaintext column 2 to column 6, and so on. The resulting ciphertext rectangle also has three columns longer than the others, but those are not necessarily the first columns from the left, as with the plaintext rectangle. Finally, after transposing the columns, we extract the text column by column from the ciphertext rectangle to obtain the final ciphertext, as shown in part (3) of Figure 6.

The decryption process is similar, but those steps are performed in reverse order. First, the ciphertext is copied into a rectangle, column by column, as shown in part (2) of Figure 6. Special care is required for the case of an incomplete transposition rectangle. In such a case, we first must determine which columns are long and which are short, according to the key. In our example, the ciphertext columns 1, 2, and 6 are long columns, as they correspond to the first three plaintext columns, 1, 0, and 2, respectively. After filling the ciphertext rectangle, taking into account the length of the columns, we reposition the columns by applying the inverse transposition key: Ciphertext column 0 is copied back to column 6 in the plaintext, ciphertext column 1 back to column 1, ciphertext column 2 back to column 0, and so on. Finally, we read the text from the rectangle row by row to obtain the decrypted plaintext.

Another example with a complete rectangle – CCT – is given in Figure 7. Encryption and decryption are easier, as all the columns have the same size.



2	1	6	5	3	4	0
K	E	Y	W	O	R	D
T	H	E	C	L	A	S
S	I	C	A	L	T	R
A	N	S	P	O	S	I
T	I	O	N	C	I	P
H	E	R	I	S	N	O
T	A	S	T	R	O	N
G	C	I	P	H	E	R

(1) Plaintext transposition rectangle

0	1	2	3	4	5	6
D	E	K	O	R	W	Y
S	H	T	L	A	C	E
R	I	S	L	T	A	C
I	N	A	O	S	P	S
P	I	T	C	I	N	O
O	E	H	S	N	I	R
N	A	T	R	O	T	S
R	C	G	H	E	P	I

(2) Ciphertext transposition rectangle

S	R	I	P	O	N	R	H	I	N	I	E	A	C	T	S	A
T	H	T	G	L	L	O	C	S	R	H	A	T	S	I	N	O
E	C	A	P	N	I	T	P	E	C	S	O	R	S	I		

(3) Ciphertext

Figure 7. Complete columnar transposition

Historically, several manual methods were used for the cryptanalysis of columnar transposition ciphers, including the CCT and the ICT cases. The best-known example is the strips method described in Friedman (1941), that can be applied to CCT cases with short keys. At first, the cryptanalyst arranges the ciphertext in columns on paper. He then cuts the text into strips, each column into one strip. Next, he manually tries to match the strips against each other using those arrangements which create the most probable bigrams, or pairs of successive letters. There are some bigrams that are easy to recognize, such as `Q` always followed by `U`. After that, he extends the process to the reconstruction of trigrams, quadgrams, and so on. The cryptanalyst repeats this process until the full key has been recovered. For ICT, the analyst may use “hat diagrams” to apply this process to all possible starting and ending positions of the columns. Those methods tend to be cumbersome for keys of length longer than 20, and in particular for the case of ICT.

Another example of a manual method is multiple anagramming. This method can be applied to the special case of two (or more) plaintexts having the same length and being encrypted with the same key. The permutation of letters as a result of transposition is identical for both plaintexts. Therefore, any rearrangement (anagramming) of some of the ciphertext letters which produces a valid plaintext when applied to the first ciphertext would also produce a valid plaintext when applied to the second ciphertext. A good description of multiple anagramming can be found in (Bauer 2002, p. 467).

A number of publications describe modern computerized approaches, based on hillclimbing, simulated annealing and genetic algorithms (see Matthews (1993), Giddy and Safavi-Naini (1994), Clark (1998), Russell, Clark, and Stepney (2003), Dimovski and Gligoroski (2003), Chen and Rosenthal (2012)). Those attacks are effective when the length of the key is less than 20, and they are less effective with lengths above 30 or for the case of ICT.

A powerful two-phase attack for columnar transposition ciphers with longer keys may be found in Lasry, Kopal, and Wacker (2016). At the first phase, the algorithm looks at all combinations of potentially adjacent columns, assigns a score to each combination - the adjacency score, and from them builds a tentative initial key, which is improved at the second phase using quadgram scoring. CCTs with very long keys (up to 1000 elements) can be solved. The method is also effective with ICT. In the case of ICT, the exact starting and ending positions of the original columns in the ciphertext are unknown (unless the key is known), and each such position falls between some range. For ICT, in the first phase, all possible starting and ending positions of potentially adjacent columns are evaluated and scored using an alignment score, and both the adjacency and the alignment scores are employed to generate a tentative initial key. With ICT, the method can recover keys with up to 120 elements. The attack is described in detail in Lasry, Kopal, and Wacker (2016) and in Lasry (2018). It was used extensively in the current research.

3.5. *Identifying Group Count Markers*

In messages which consist of five-letter groups. markers of the form n/d such as `11/4`, `22/4`, `75/11`, or `149/11` can be found. The second part d, after the / sign, was found to indicate the day (of the month) the message was encrypted. For example, `11/4` indicates that the message was encrypted on the 4th of a certain month.

After further examination, it was hypothesized that each message may consist of one or more distinct cryptograms. It was found that the first part n of n/d indicates the count of five-letter groups from the beginning of a certain cryptogram. Those markers always appear in pairs, denoted as n_1/d and n_2/d, and either $n_2 = 2n_1$ or $n_2 = 2n_1 - 1$. The second marker - n_2/d - is positioned at the end of the cryptogram, and n_2 is the total number of five-letter groups in the cryptogram. If n_2 is even (there is an even number of five-letter groups) then $n_2 = 2n_1$ and the second marker - n_1/d - is placed between the two halves of the cryptogram, as shown in BAL25B, for example:

```
TDDTA SMLES CHESS ACFCE DTSDS BICTR OEDSS BNDEE NAANS NNEDI
PEEEM 11/4  OODME RTUTS WMETG EEDSN NOPGS ICDAS LRRSS TENTS
GYDSD AMEES LYISS 22/4
```

If n_2 is odd (there is an odd number of five-letter groups), the first marker n_1/d is placed after the group in the middle of the cryptogram (the median group), and in this case, $n_2 = 2n_1 - 1$, or $n_1 = (n_2 + 1)/2$. An example (BAL40) is given below:

```
CTSGT IYEEF CSINL ESFVG HVRAR PEHBU EPTSO WNPOW OWIAF EDSLT
EEEEE ETERI SXPTA HNISS DAFUT IKRRB ACAOS CSNIM EEEYM CWOUR
VMDNI GCEEN BEOHN VEEMR OSEON EINPP TIOVU RFDZV UPEAY TAGON
CUROE OERRB HNEIA VOYND RLHTW 35/21 RXSOH HERDE RIOAE SRAEU
HEEHS RBHRR AEOTF BOEOE RTLNN EFAPO OEELC EEEES ACELN AGTEP
GFJRF NOIDS DRNEE IHHHE HSSOH REFTR RHOLT RGREL ETDNI ESIPS
FTPTS EOHER NAUET OWIIF EYRAE CJETA WEKSR ARSSK EENRC IROKE
69/21
```

Often, the second marker n_2/d is followed by another sequence of five-letter groups. As mentioned above, it was assumed that those groups were the beginning of a new cryptogram. It later turned out that long plaintexts were indeed split into smaller parts, each part being encrypted separately. Therefore, the n_2/d marker might indicate not only the end of a cryptogram, but also the beginning of the next one.

3.6. *Initial Breakthrough - BAL25B and BAL26B*

Both ciphertexts BAL25B and BAL26B have 110 characters each. Both are from August 4, 1969. Those are the shortest ciphertexts, and each ciphertext consists of 22 groups of 5 letters, with markers 11/4 and 22/4. Upon examination, they were found to share a common code group (BICTR). Also, in multiple groups, the first letter of certain five-letter groups (in **bold** below) is identical in both ciphertexts.

BAL25B

TDDTA **S**MLES CHESS **A**CFCE DTSDS **BICTR** OEDSS **B**NDEE NAANS NNEDI
PEEEM 11/4 **O**ODME **R**TUTS **W**METG **E**EDSN **N**OPGS **I**CDAS LRRSS **T**ENTS
GYDSD AMEES LYISS 22/4

BAL26B

TBHHL **S**SHNI UTINE **A**MOWO MAPGE **BICTR** SMNIE **B**AEDS EHLOE OOERT
PETSO 11/4 **O**RPOA **R**EFIO **W**EETE **E**LOOE **N**YEIV **I**ALOD RSUOE **T**MTSP
GWPSA WTECS TOGTE 22/4

This finding is consistent with two CCTs with 5 rows each, their first row sharing a significant number of identical letters (T, S, A, B, P, O, R, W, E, N, I, T, G), possibly resulting from an identical plaintext beginning. With this hypothesis, an attempt was made to solve the transposition by combining the two ciphertexts and interleaving the five-letter groups (e.g., TDDTA TBHHL SMLES SSHNI CHESS UTINE ...), so that the combined ciphertext has 10 rows.

Using hillclimbing and hexagram scoring, the following plaintext was obtained, consisting of what seemed to be two distinct original plaintexts (as expected as two ciphertexts were combined before decryption):

PARTTWOBEGINSANDCOLBNL
ECTEDMONEYCOMMATHEYINR
EFUNDEDDDDDPLEASEDICER
ECTTTTMESSAGEENDSSSTDS
MESSAGEENDSSSSSSSSSSRIS
PARTTWOBEGINSWEMUSTBOR
EMEMBERALWAYSTHATMOIOS
TOFTHEPEOPLEHELPINGCEU
SWISHTODOSOINCOGNITTRO
OOOPLEASEADVISEEEEERTE

The transposition key (the first index is 0):

10, 3, 12, 18, 0, 13, 11, 7, 14, 19, 16, 15, 1, 20, 8, 4, 2, 6, 21, 5, 9, 17

Several observations could be made:

(1) The two parts indeed start with the same phrase `PARTTWOBEGINS`, which is composed of the identical letters found in the same respective positions (T, S, A, B, P, O, R, W, E, N, I, T, G).

(2) The penultimate column and the one on its left (`NNEDIOOERT` and `BICTRBICTR`, respectively) are not part of the original plaintext. At this stage, they were assumed to be either dummy columns or some form of indicator.

(3) In some words like "refunded", "direct", "end", "incognito", and "advise", the last letter is repeated (e.g., `ADVISEEEEE`). Those repetitions seem to appear at the end of sentences, and probably replace a full stop.

(4) Another punctuation mark, `COMMA`, is spelled out in full.

(5) In addition to the stereotyped beginning (`PARTTWOBEGINS`), there seems to be a stereotyped ending (`MESSAGEENDS`).

(6) Even after removing the two columns which are not part of the plaintext from the key, it was not possible to match the numerical key with a keyword from a dictionary or a corpus of word n-grams.

Following this initial success which occurred on November 26, 2019, an attempt was made using a similar technique to solve other ciphertexts, either:

- Single ciphertexts:
  - BAL18 assuming key length 42 and 5 rows
  - BAL50 assuming key length 40 and 5 rows.
- Combining ciphertexts that are from the same day and have the same n/d markers, e.g.:
  - Several messages from BAL141, combining them into 30 rows and assuming a key length of 149.
  - Combining BAL25A, BAL26A, and BAL29 into 15 rows and assuming a key length of 142.

Trying to solve transpositions with such long keys required the use of the attack described in Lasry, Kopal, and Wacker (2016). However, those attempts did not produce any results. Since the attack is otherwise able to successfully solve CCTs with similar or even more challenging parameters (e.g., longer keys and/or shorter ciphertexts), this clearly hinted at the possibility that the Biafran ciphers might not be just "textbook" CCTs. Also, there are no documented historical examples in the literature of key lengths much longer than 25. Key lengths 142, 149, and even 40 or 42 are anyway difficult to process while encrypting or decrypting a message, and did not look very likely.

The possible crib `PARTONEBEGINS` was used in order to try to solve BAL25A and BAL26A, which precede BAL25B and BAL26B, respectively. The n-gram statistics were also adjusted to account for repeated letters (e.g., `EEEEEE` or `SSSSSS`), without any success.

In parallel, attempts were made to find solutions that do not assume that the ciphertexts are columnar transpositions. Multiple anagramming allows for the recovery of plaintexts regardless of the transposition type, provided the messages were encrypted using the same key and have the same length (Bauer 2002, p. 467). Such an attempt was made on messages with the same markers and from the same day (e.g. messages from BAL141), using quadgrams and even hexagrams, without any result. This could also indicate that those messages were not encrypted with the same key.

Other hypotheses were considered, that would encompass the BAL25B and BAL26B scenario as a special case, again, without any success.

3.7. *Second Breakthrough - BAL31*

The next breakthrough was achieved on December 12th, 2019, by assuming BAL31 (markers `61/4 122/4`) to be a CCT with 10 rows and a key length of 61. Hillclimbing produced in the following decryption (probable words are marked on the right side):

OSPSIXZEROTHSEORDASHTHEYHAVENSEWRCRESTMAREACLOWISILSHOONTRACT
SHABAFROMCHIDDIJ**PASSVORT**SSEMTEUIRDCIYGWUYDXOPENDRA**PIRED**THEYAR (passport, expired)
EDRYYYYTENDEREAND**DOCTOR**SIKORTRALEPRYNTEDMOGPVTOHANGLINEATHEGG (doctor)
LINS**APPLYING**ADLOIKORADASHAPOORRACEINSOSSHEMDELECTAMPLEROFTHEG (applying)
ROUHE**SWISS**REHAS**DONALD**ASHHEHADBYHASOCIFOFISAHSTNPTASHHEADIPLOM (swiss, donald)
ATITRY**VISAFORTAREVELCERTIFICPRESS**STARORENNASABYCTASPPOEMICOLO (visa for travel certificate press)
NDREE**DOCTOR**SEPTAFL**FIVEWANT**TOUTALMERNAFTHREGALAAMARGOIRATMUGGL (doctor, five want)
ISESTOCTMEINMISTEELKINONAU**GUIDE**LOSTOOURSEACWWDEMTLORTNSSILLIG (guide)
REPRELIEVEFIIGSVEN**MESSAGEEND**AFLINSMENINTOSTANOVENESALLEMICOLO (messageend)
NMRKINGATABORDSH**ENDSSSSSSSSS**TONNEASHESWORETHEMSAGAINGESHALLAR (endsssssssss)

Recovered transposition key:

```
16, 28, 32, 55, 46, 43, 21, 58, 12,  3,  0,  6, 47, 44, 51, 49,
26, 11, 42, 57, 48, 45, 23, 60, 14,  5,  2,  8, 19, 15, 18, 10,
52, 22, 36, 34, 39, 37, 24,  9, 40, 17, 38, 31, 30, 27, 33, 53,
20, 54, 25, 29, 41, 56, 59, 13,  4,  1,  7, 50, 35
```

Even though some of the guesses later turned out to be wrong (e.g. `Donald`), the presence of so many significant fragments of plaintext could not be the result of pure chance. In addition, the presence of a stretch of repeated S was expected from the decryption of BAL25B and BAL26B.

Another attempt with an improved version of the software implementing Lasry, Kopal, and Wacker (2016) resulted in the following decryption, with longer significant fragments:

E**WHOSECONTRACT**SOSPINALLEST**MARSIXZEROTHRE**CROWISS**DASHTHEYHAVE**OR
DIREDDDD**THEYARE**SHADTXPPUIGWUYBA**FROMCHIJI**ORENARY**PASSVORT**SSEMIC
OLIN**REPEATH**EGGREDRHTGGVALTEDMYYYYTENDENYPETON**ANDDOCTORSIKORA**R
EA**LEADEROFTHE**GRLINCOMMERPOSSHS**APPLYING**ONDCLEAT**SIKORADASHAPOLI**
SH**HEHASADIPLO**MBROUPDASSYHFOFI**HESWISSRED**CHAT**NATIONALDASHHEHAS**O
NS**PORTSEMICOLO**RATICPASAEPOR**ENTRYVISAFOR**ASSBYA**TREVELCERTIFICAT**
ELI**REPEAT**MUGGLTNDRMUGGLA**OFTHREEDOCTORS**ANAMAARAAFL**FIVEWANTTO**TR
ALTNMISSSILLIGDI**SEMICO**WERURSESTOCTME**INTO**WODELTOEELKINON**AUGUST**
SILLIG**SEMICOLO**F**REPEAT**SNLAIN**TORELIEVEFIVE**ANOVENNEN**MESSAGEENDS**M
ENGER**DASH**ALLARONMRATTIENNS**WORKINGAT**ABOHHHEM**SAGEENDSSSSSSSSSSS**

Since BAL31 had markers of the form $n_2 = 2n_1$ (`61/4 122/4`) and could be partially decrypted using $n_1 = 61$ as the key length, attempts were made on other messages with the same characteristics. For some reason (not clear at the time) the attack under those similar assumptions failed for most of the messages with $n_2 = 2n_1$, such as BAL214A (`71/19 142/19`).

However, the attack was successful against four additional messages: BAL192 (`64/10 128/10`), BAL139B (`64/16 128/16`), BAL214C (`41/19 82/19`), and BAL151B (`43/16 86/16`), as shown here.

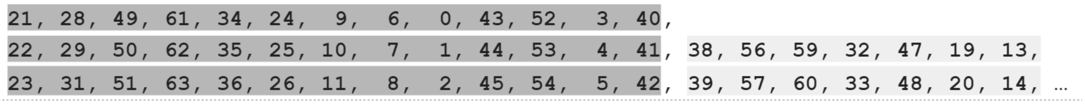
BAL192 (with key length 64)

SECRETLNBSEVENNNE**FORUGWUMBAFROMCC**TSUR**TRIPBEGINSFRIDAYA**RGN**EIGHT**EI
GHT**FORM**RAKPANESEATEDOANDOKAGBUEEENA**THEYSHOULDARRIVEBY**WEY**CHIEF**SEC
FROMCCREPEATE**PLEASEINFORMCHIEF**OGBEINESDAY**TOENABLEVISA**FUNDOANDUGW
UMBAAAA**PLEASE**LFFOR**TOARRIVEHEREBY**NOM**MALITIESTOBECOMPLETELINFORM**CO
M**MISSION**ERUDOXG**FLIGHTTOBEGIN**HISASEO**SECRETLNBSEVEN**NENEOSDAFFIATHA
THISWIFEHASBEIINMENT**BEFOREILEAVE**ONEFORHHHEEE**FROMCC**CCCCNOENHEREFO
R**ONEWEEKWAITI**MPTOUR**SECRETLNBSEVENIMPORTANTREPORTARRIVIN**DNGFORHIM
ANDCONFIRMIFHILE**ZERO**FORO**FROMCC**CCCNG**THROUGHKOGBARA**DUEMICDEISTAKIN
G**THEFLIGHTON**MPAEASE**ADVISE**DROKIGBOTLAR**MONDAYMORNINGGGGG**ARONDAYNIG
HT**SECRETLNBSE**NTNWOGU**ANDHISGROUP**TH**THISMESSAGEENDSENDSSS**ADVENEIGHT

Recovered transposition key:

```
 21, 28, 49, 61, 34, 24,  9,  6,  0, 43, 52,  3, 40, 22, 29, 50,
 62, 35, 25, 10,  7,  1, 44, 53,  4, 41, 38, 56, 59, 32, 47, 19,
 13, 23, 31, 51, 63, 36, 26, 11,  8,  2, 45, 54,  5, 42, 39, 57,
 60, 33, 48, 20, 14, 17, 16, 30, 37, 55, 58, 27, 46, 18, 12, 15
```

Some regular patterns were observed in the key, when tabulated differently (see Figure 8).



```
21, 28, 49, 61, 34, 24,  9,  6,  0, 43, 52,  3, 40,
22, 29, 50, 62, 35, 25, 10,  7,  1, 44, 53,  4, 41, 38, 56, 59, 32, 47, 19, 13,
23, 31, 51, 63, 36, 26, 11,  8,  2, 45, 54,  5, 42, 39, 57, 60, 33, 48, 20, 14, …
```

Figure 8. BAL192 – patterns in recovered key

At this stage, there was no clear explanation for those patterns that seemed to be hinting at some kind of transposition with a key shorter than 64 but with some yet-to-be-explained discrepancies.

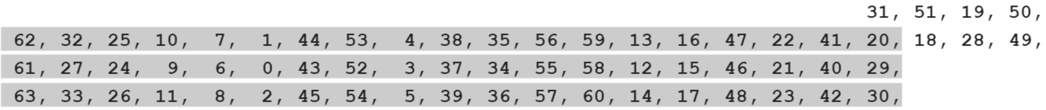
BAL139B (with key length 64)

WNN**TOHUNABELTHENEXTDAY**I**PARTTWOBEGINSTUESDAY**SNS**WHICHWILLTAKESOME**Y
ERBACKETSUNDAY**UNBRACKET**AND**TNURSDAYSRESPECTIV**LEE**ORFOURDAYSSSS**THEA
DSTTT**THEREIS**ANEASTLATIVELYYYY**BRACKET**BUNBRACKSITTOASHDOD**OFCOURSE**N
KSVN**AIRWAYSCONNECTION**BPET**SABENAAIRLINEFLIGHT**MES**NOTROUBLE**PARAWILS
SDEWEENMOSSMANANDSMIGLLSLROMSUCRONYTOMOSSMANRVISEYOUASSOONASWEHE
AREONLYONCEAWEEKDASHONEBRACKETASHDOD**UNBRACKE**SFROMLUMETIERANDSUVO
CHS**TURDAYSPARAHAVEMADE**IT**DASHONLYONEFLIGHT**AWER**ANDPERHAPS**KIMCHEYQH
ERE**QUIRIESTOTHEEMBASS**IUEKKKK**DEPARTS**KOLLONTAYTY**YOUWILLINANYCASE**WI
SHECONCERNEDBUTHAVENOTI**ONFRIDAYARRIVING**CULLOATO**INFORMUSOFTHE**SCHO
DUYT**RECEIVEDTHEIRREACT**EDEN**SATURDAYCOMMARETUR**TLES**OFTHEIRFLIGHTS**SA

Recovered transposition key:

```
31, 51, 19, 50, 62, 32, 25, 10,  7,  1, 44, 53,  4, 38, 35, 56,
59, 13, 16, 47, 22, 41, 20, 18, 28, 49, 61, 27, 24,  9,  6,  0,
43, 52,  3, 37, 34, 55, 58, 12, 15, 46, 21, 40, 29, 63, 33, 26,
11,  8,  2, 45, 54,  5, 39, 36, 57, 60, 14, 17, 48, 23, 42, 30
```

This key also has some regular patterns (see Figure 9).



```
                                                                     31, 51, 19, 50,
62, 32, 25, 10,  7,  1, 44, 53,  4, 38, 35, 56, 59, 13, 16, 47, 22, 41, 20, 18, 28, 49,
61, 27, 24,  9,  6,  0, 43, 52,  3, 37, 34, 55, 58, 12, 15, 46, 21, 40, 29,
63, 33, 26, 11,  8,  2, 45, 54,  5, 39, 36, 57, 60, 14, 17, 48, 23, 42, 30,
```

Figure 9. BAL139B – patterns in recovered key

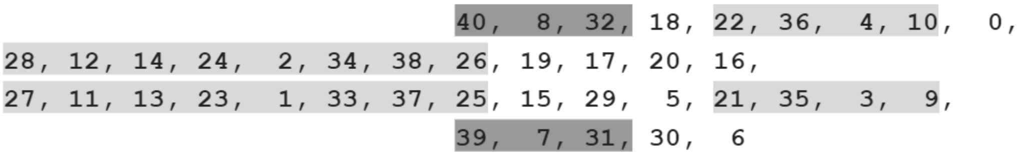
BAL214C (with key length 41)

CONTAINIMPORTANTMEGTA**BEGINS**INTHETHREPARTE
RIALLLL**THESEMATER**RHRI**RIVINGTONIG**SERANOMAL
S**COULDNOTBEOPENED**HOWI**ISMARKED**PPP**WHICHTO**NT
HE**CUSTOMSHERE**EEESPO**TOMATERIALS**ANKEPPSTRPL
EASEARRANGEFORPACEUTKDTOHHHNNN**ONSIGN**DCOAG
ES**TOBEOPENEDTHERE**SSI**THEYAREAIR**RRUUUUUBONO
RDERTHATEXPECTEDOAGWIOM**ESSEXXXX**ITEDFEIGNE
RS**MAYBEKNOWNNNN**PLIEEN**WHATTHEYARE**TKNODONAS
E**KEEPMEPOSTEDASTO**GLWO**HEYBELONGGGWHOM**ORTHA
T**THEFINDINGSAREEE**LDEN**THEPACKAGES**SPECGISEE

Recovered transposition key:

```
40,  8, 32, 18, 22, 36,  4, 10,  0, 28, 12, 14, 24,  2, 34, 38,
26, 19, 17, 20, 16, 27, 11, 13, 23,  1, 33, 37, 25, 15, 29,  5,
21, 35,  3,  9, 39,  7, 31, 30,  6
```

This key also has some regular patterns (see Figure 10).



```
                                    40,  8, 32, 18, 22, 36,  4, 10,  0,
28, 12, 14, 24,  2, 34, 38, 26, 19, 17, 20, 16,
27, 11, 13, 23,  1, 33, 37, 25, 15, 29,  5, 21, 35,  3,  9,
                                    39,  7, 31, 30,  6
```

Figure 10. BAL214C – patterns in recovered key

BAL151B (with key length 43)

PHEIIGHT**OFTHEINSPECTO**RN**TWOBEGINS**OFTWOUNNRST
A**GENERALOFPOLICELETTER**T**GERMANFILMCOMPAN**IEND
EREFERENCESSS**ONEZEROTW**AS**THEYALSOCLAIMTHE**SOS
IO**STROKEONESEVENNINE**ONA**RESTOFAMERICAN**ANDTIE
FE**OFONESIXAUGUST**ONENINICH**TTTVVVSTATION**SSEHN
SE**SIXEIGHTCOMMA**YOUCONSTAH**GEOTLEMENARE**KNOBOO

WIDER**TNEIRVISIT**NOWOPPOPMPOREERS**ANDFRIENDS**BU
SR**TUNEDANDINTHEINTERE**SISAFRIAAA**WHILE**THERFYB
ETOFDALFON**PLEASECONVEY**ONLOCRL**OBJECTIONTO**SAN
T**APPROVALEARLIESTTTTTTT**RRVISXT**COMMABUTIN**TEGI

3.8. *Reconstructing Full Plaintexts with the Strips Method*

Next, an attempt was made to fully recover the original texts of the five messages for which a partial decryption was now available. For that purpose, the team took advantage of pre-computer-age means that have historically been highly effective in solving transposition ciphers. The recovered texts were either printed and cut into strips containing each one column of 10 letters or manually written into a paper grid and then cut.

The results of manual plaintext reassembly for BAL19B are shown in Figure 11.

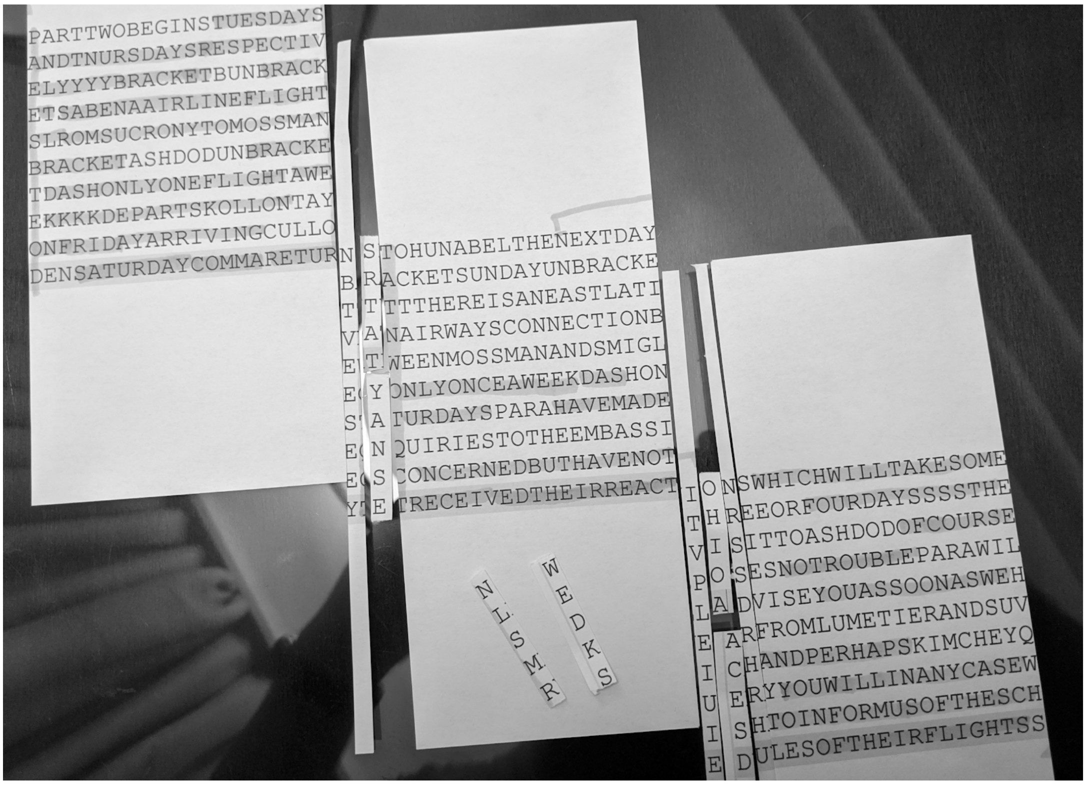


Figure 11. BAL139B – plaintext recovery using the strips method

The initial results for BAL31 are shown in Figure 12 and an improved version in Figure 13.

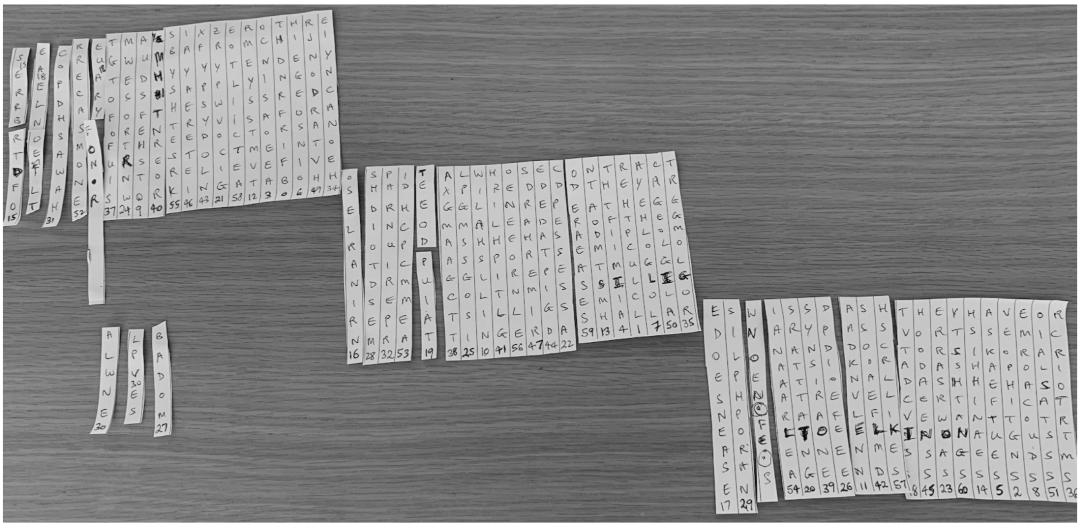


Figure 12. BAL31 – plaintext recovery using the strips method

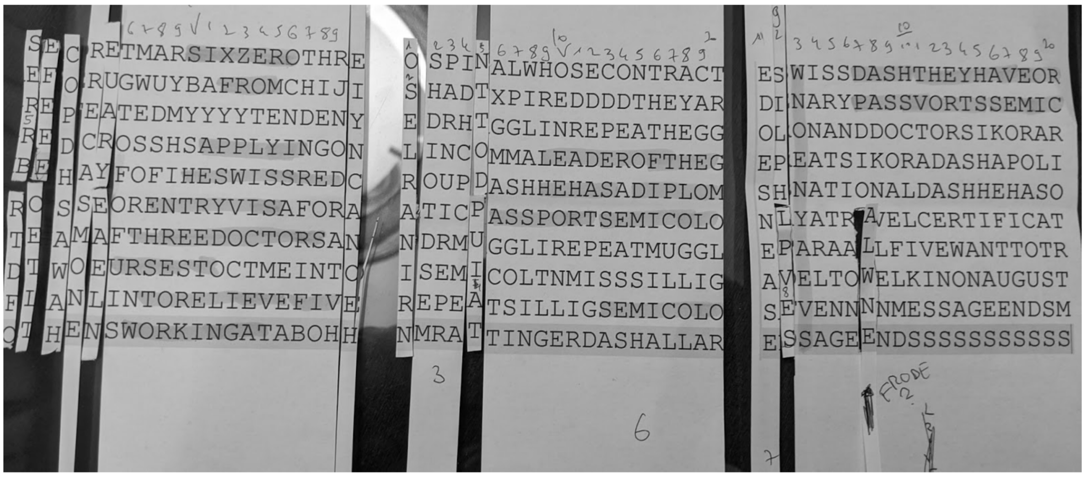
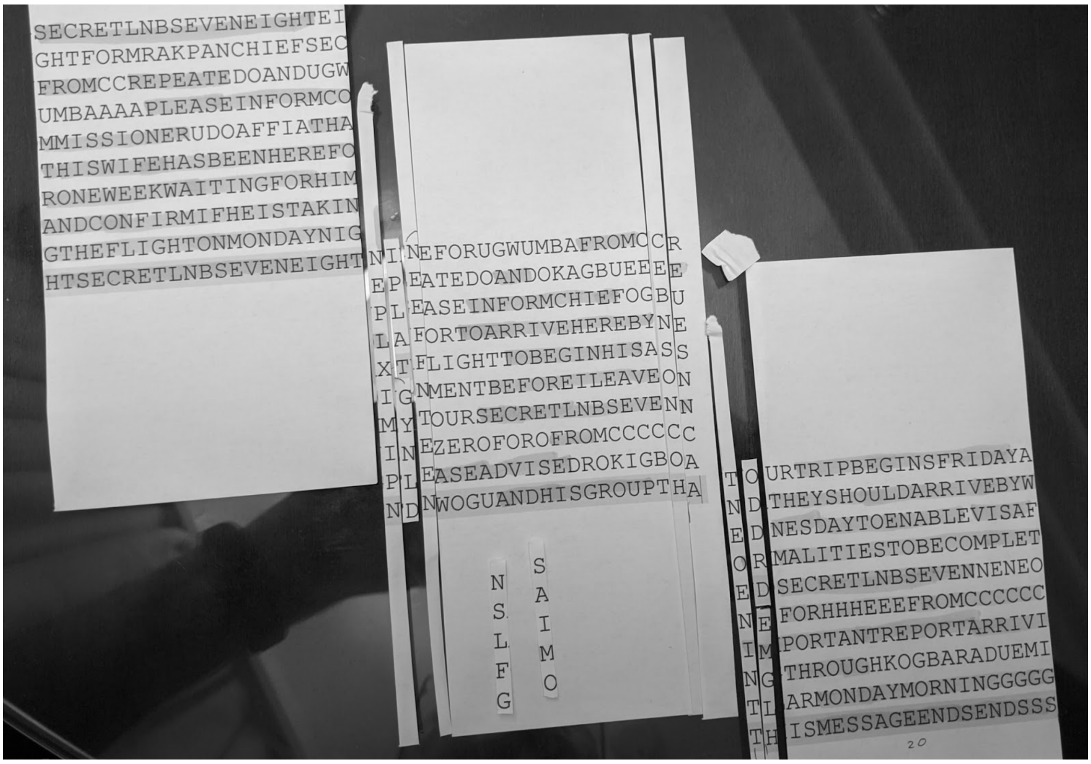


Figure 13. BAL31 – improved plaintext recovery using the strips method

The results for BAL192 are shown in Figure 14.



```
SECRETLNBSEVENEIGHTEI
GHTFORMRAKPANCHIEFSEC
FROMCCREPEATEDOANDUGW
UMBAAAAPLEASEINFORMCO
MMISSIONERUDOAFFIATHA
THISWIFEHASBEENHEREFO
RONEWEEKWAITINGFORHIM
ANDCONFIRMIFHEISTAKIN
GTHEFLIGHTONMONDAYNIG
HTSECRETLNBSEVENEIGHT
```

```
NINEFORUGWUMBAFROMCCR
EPEATEDOANDOKAGBUEEEE
PLEASEINFORMCHIEFOGBU
LAFORTOARRIVEHEREBYNE
XTFLIGHTTOBEGINHISASS
IGNMENTBEFOREILEAVEON
MYTOURSECRETLNBSEVENN
INEZEROFOROFROMCCCCCC
PLEASEADVISEDROKIGBOA
NDNWOGUANDHISGROUPTHA
```

```
TOURTRIPBEGINSFRIDAYA
NDTHEYSHOULDARRIVEBYW
EDNESDAYTOENABLEVISAF
ORMALITIESTOBECOMPLET
EDSECRETLNBSEVENNENEO
NEFORHHHEEEFROMCCCCCC
IMPORTANTREPORTARRIVI
NGTHROUGHKOGBARADUEMI
TLARMONDAYMORNINGGGGG
THISMESSAGEENDSENDSSS
```

20

Figure 14. BAL192 – plaintext recovery using the strips method

For BAL214C, the plaintext was this time conveniently reconstructed with the help of a spreadsheet, clearly showing two side-by-side separate plaintext segments, the right one being the continuation of the left one (`THEPACKAGES ... CONTAININPORTANT`).

```
PARTTHREEBEGINSINTHE CONTAINIMPORTANTMATE
NOMISERARRIVINGTONIG RIALLLLTHESEMATERIAL
HTONWHICHISMARKEDPPP SCOULDNOTBEOPENEDINT
STROKEPPPMATERIALSAN HECUSTOMSHEREEEESOPL
DCONSIGNEDTOHHHNNNON EASEARRANGEFORPACKAG
UBOGUUUUTHEYAREAIRFR ESTOBEOPENEDTHEREINO
EIGHTEDFROMESSEXXXXI RDERTHATEXPECTEDOWNE
DONOTKNOWWHATTHEYARE RSMAYBEKNOWNNNNPLEAS
ORTOWHOMTHEYBELONGGG EKEEPMEPOSTEDASTOWHA
GISUSPECTTHEPACKAGES TTHEFINDINGSAREEEEEE

Unused groups: SAIGL, SGELD
```

From those reconstructions, a few observations could be made:

- Two sets of five letters are not part of the reconstructed plaintext.
- In each of the reconstructions, there seem to be two or three separate parts, that need to be reassembled separately.
- Each of the parts is composed of a set of continuous columns that can be recovered by the automated program. Some columns/half columns cut from various places can manually be stitched either to the left or to the right, to form a coherent and continuous decryption.

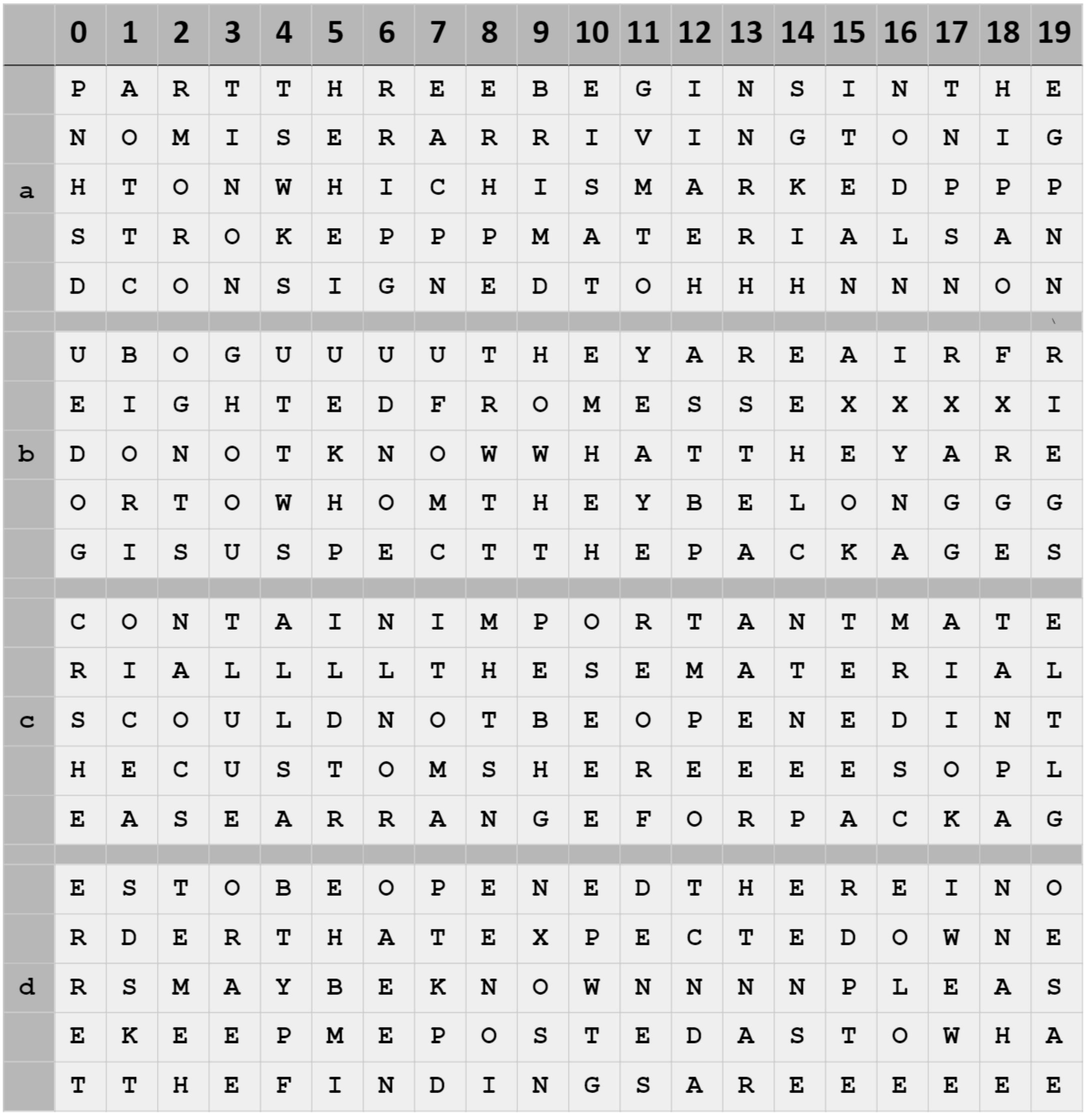
3.9. *Reconstructing the Encryption Mechanism*

Further analysis showed that the two unused sets of five letters always came from the same places, relative to the middle of the ciphertext. For example, in BAL214C, the two unused sets are in the second group (`SAIGL`) and the sixth group (`SGELD`) to the left of the marker `41/19` (this marker is placed in the middle of the ciphertext).

```
MHTSN EENOI NNRRH RSTEA AAEER HTNAR RRIPG UDNOE NLNOR OAEEN
EGPNN RIEGS ELTLG OESAE AOTTC BIORI OICEA SDSKT EACPN UFOMC
ITOMA PTKPD EISAT EMHEH OSEEE EPWTG GVMTO YEAYE REORF DENES
TNPSN RXAGG AIIOK TINON GHOOU SGELD TLUUE ORAEE ERHPE SAIGL
TRWTT 41/19 IWEWE TSWKS UTTWS ALLSA BTYPF IIAEH ASTBP TMPEO
TCNDA NODLN IXYNA MRDSC EOLOE BRIMD HOWHT PEBHG NXOSN HIPAO
FXRGE TANPA NNAHE RMORO OGNTS NAOCS TEMEH SGKIH EEHLC NTNEP
EENSE HEHEI UEKHP ILDTR EHBMI ITEAN AXEOK TEEEA RDPTE PNHSD
UEDOG CRSHE ERRET 82/19
```

The unused sets could all be found in similar positions, in BAL31, BAL192, and BAL139B.

The aforementioned regularity in the structure of the assumed long keys had already hinted at the possibility of transposition keys shorter than the ones assumed during automated recovery using hillclimbing. The fact that each reconstruction consisted of two or three separate parts was also hinting at that direction, given that they were a continuation of one another (for example: `THEPACKAGES` followed by `CONTAINIMPORTANT`). The separate parts could also be considered to extend the height of the plaintext rectangle, rather than extending its width (as in the first reconstructions). For example, the two plaintext parts of BAL214C can be tabulated with 20 columns and 20 rows (instead of 40 columns and 10 rows), as shown in Figure 15.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	P	A	R	T	T	H	R	E	E	B	E	G	I	N	S	I	N	T	H	E
	N	O	M	I	S	E	R	A	R	R	I	V	I	N	G	T	O	N	I	G
a	H	T	O	N	W	H	I	C	H	I	S	M	A	R	K	E	D	P	P	P
	S	T	R	O	K	E	P	P	P	M	A	T	E	R	I	A	L	S	A	N
	D	C	O	N	S	I	G	N	E	D	T	O	H	H	H	N	N	N	O	N
	U	B	O	G	U	U	U	U	T	H	E	Y	A	R	E	A	I	R	F	R
	E	I	G	H	T	E	D	F	R	O	M	E	S	S	E	X	X	X	X	I
b	D	O	N	O	T	K	N	O	W	W	H	A	T	T	H	E	Y	A	R	E
	O	R	T	O	W	H	O	M	T	H	E	Y	B	E	L	O	N	G	G	G
	G	I	S	U	S	P	E	C	T	T	H	E	P	A	C	K	A	G	E	S
	C	O	N	T	A	I	N	I	M	P	O	R	T	A	N	T	M	A	T	E
	R	I	A	L	L	L	L	T	H	E	S	E	M	A	T	E	R	I	A	L
c	S	C	O	U	L	D	N	O	T	B	E	O	P	E	N	E	D	I	N	T
	H	E	C	U	S	T	O	M	S	H	E	R	E	E	E	E	S	O	P	L
	E	A	S	E	A	R	R	A	N	G	E	F	O	R	P	A	C	K	A	G
	E	S	T	O	B	E	O	P	E	N	E	D	T	H	E	R	E	I	N	O
	R	D	E	R	T	H	A	T	E	X	P	E	C	T	E	D	O	W	N	E
d	R	S	M	A	Y	B	E	K	N	O	W	N	N	N	N	P	L	E	A	S
	E	K	E	E	P	M	E	P	O	S	T	E	D	A	S	T	O	W	H	A
	T	T	H	E	F	I	N	D	I	N	G	S	A	R	E	E	E	E	E	E

Figure 15. BAL214C – recovered plaintext tabulated with 20 columns

In this new tabulation, each plaintext column has 20 elements, or four five-letter groups, each of which also appears in the ciphertext. We denote the four groups in a column with the letters a, b, c, and d. For example, group 0b (the second group of the first column) is `UEDOG`.

Using this notation, we were able to map each ciphertext group to its original location in the plaintext rectangle above, as shown in Figure 16 (`xx` indicates the unused five-letter groups which appear in the ciphertext but are not part of the original plaintext).

Ciphertext group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19		
Plaintext group	8 c	8 d	13 a	13 b	13 c	13 d	6 a	6 b	6 c	6 d	19 a	19 b	19 c	19 d	1 a	1 b	1 c	1 d	7 a	7 b		
Ciphertext group	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
Plaintext group	7 c	7 d	10 a	10 b	10 c	10 d	11 a	11 b	11 c	11 d	17 a	17 b	17 c	3 a	3 b	xx	3 c	3 d	8 a	xx	8 b	17 d
Ciphertext group	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61		
Plaintext group	4 a	4 b	4 c	4 d	12 a	12 b	12 c	12 d	16 a	16 b	16 c	16 d	9 a	9 b	9 c	9 d	18 a	18 b	18 c	18 d		
Ciphertext group	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81		
Plaintext group	2 a	2 b	2 c	2 d	14 a	14 b	14 c	14 d	5 a	5 b	5 c	5 d	15 a	15 b	15 c	15 d	0 a	0 b	0 c	0 d		

Figure 16. BAL214C – mapping of the ciphertext groups to their original plaintext locations

From the mapping in Figure 16, we can see that for most of the plaintext columns, their four groups (a, b, c, and d) appear consecutively in the ciphertext, as would have been expected with a CCT and a key with 20 elements.

There are, however, a few exceptions:

(1) In the beginning of the ciphertext, only group c and d of plaintext column 8 appear (ciphertext groups 0 and 1, and plaintext groups 8c and 8d, respectively). The remaining two groups – 8a, and 8b – are near the middle of the ciphertext (the middle of the ciphertext is between ciphertext groups 40 and 41).

(2) The order of the groups near the middle part of the ciphertext also seems to have been disrupted:

   (a) In ciphertext groups 30, 31, and 32, only the first three groups of plaintext column 17 appear (17a, 17b, and 17c). The last one (17d) is at ciphertext group 41. There is a gap of eight groups between 17c and 17d in the ciphertext.

   (b) The groups of plaintext column 3 are separated by a group which is unused in the plaintext.

   (c) Similarly, the last two groups of plaintext column 8 (8c and 8d) are also separated by a group unused in the plaintext.

From the layout of the ciphertexts of this message and from other reconstructed plaintexts, it was possible to formulate a hypothesis as to the underlying encryption scheme, as follows (using BAL214C for illustration):

(1) The plaintext is written in a rectangle with 20 columns, row by row.

(2) Some transposition key is applied to shuffle the columns.

(3) The resulting text is written column by column, to generate an interim ciphertext. So far, those steps are consistent with a “textbook” columnar transposition. But now comes the twist.

(4) To this interim cipher, an additional group is inserted between the groups that were second and third before insertion. Another one is inserted between the

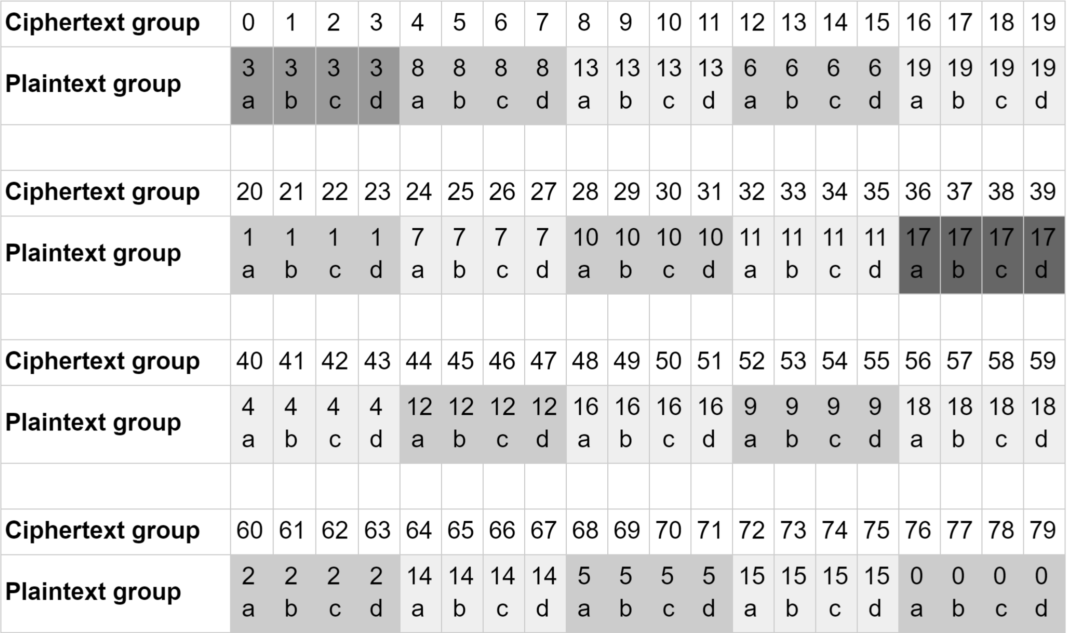
groups that were fifth and sixth before insertion.

(5) The first eight groups, which now include the two newly inserted groups, are then extracted and repositioned so that they end right before the middle of the ciphertext.

When deciphering a (final) ciphertext, an reversed process should be applied.

As only ciphertexts with markers with $n_2 = 2n_1$, were examined at that time, it could be established that the middle point was indicated, in the final ciphertext, by the first marker - n_1/d. In the case of BAL214C, the last of those eight groups would therefore be group 40 (the 41th counting from 0) in the final ciphertext, followed by the marker `41/19`.

Based on this hypothesis, it was possible to reconstruct the order of the groups in the interim ciphertext, before steps (4) and (5), for BAL214C, using the mapping shown in Figure 17.



Ciphertext group	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Plaintext group	3 a	3 b	3 c	3 d	8 a	8 b	8 c	8 d	13 a	13 b	13 c	13 d	6 a	6 b	6 c	6 d	19 a	19 b	19 c	19 d
Ciphertext group	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
Plaintext group	1 a	1 b	1 c	1 d	7 a	7 b	7 c	7 d	10 a	10 b	10 c	10 d	11 a	11 b	11 c	11 d	17 a	17 b	17 c	17 d
Ciphertext group	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
Plaintext group	4 a	4 b	4 c	4 d	12 a	12 b	12 c	12 d	16 a	16 b	16 c	16 d	9 a	9 b	9 c	9 d	18 a	18 b	18 c	18 d
Ciphertext group	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
Plaintext group	2 a	2 b	2 c	2 d	14 a	14 b	14 c	14 d	5 a	5 b	5 c	5 d	15 a	15 b	15 c	15 d	0 a	0 b	0 c	0 d

Figure 17. BAL214C – mapping of the interim ciphertext groups to their plaintext locations

From the mapping of the plaintext to the interim ciphertext, we could recover the original transposition key for BAL214C:

`19, 5, 15, 0, 10, 17, 3, 6, 1, 13, 7, 8, 11, 2, 16, 18, 12, 9, 14, 4`

The keys for the other messages for which the plaintext had been recovered using the strips method (BAL31, BAL192, and BAL139B) could also be reconstructed when assuming the proposed encryption scheme. The length of the keys was either 20 or 21.

3.10. *Solving Other CCT Messages with $n_2 = 2n_1$*

To test the hypothesis aforementioned, additional messages were examined, first generating the interim ciphertext, and checking key lengths so that the resulting rectangle is complete (CCT), as follows:

- The key for BAL18 (`21/20 42/20`) was recovered with a key length of 21 and

10 rows.

- BAL25A, BAL26A, BAL29, BAL214A, BAL214B, BAL216, BAL16A, BAL51A have the same size and have markers of the form of `71/d 142/d`. Their respective keys could also be recovered when assuming a key length of 20 (and 35 rows in the plaintext and the interim ciphertext rectangles).

Those latest recoveries raised the following question: Why couldn't the messages with markers `71/d 142/d` be at least partially decrypted assuming 10 rows by applying the attack on the final ciphertext, as it had been possible for messages such as BAL214C?

While the messages previously solved with a (wrong) assumption of 10 rows also were CCTs with and $n_2 = 2n_1$, the main difference is that those previously solved messages had a number of rows – in the original plaintext rectangle – which was either 10 or a multiple of 10. In contrast, the number of rows in BAL25A, BAL26A, BAL29, BAL214A, BAL214B, BAL216, BAL16A, BAL51A is 35 which is not a multiple of ten.

- With BAL214C, the transition from the interim ciphertext to the final ciphertext preserves the alignment modulo 10 of most of the originally adjacent groups (in the plaintext rectangle), as it involves an insertion of two new groups ($2 \cdot 5 \bmod 10 = 0$) and the transition of eight groups ($8 \cdot 5 \bmod 10 = 0$) from position 0 to a new position which is also 0 modulo 10. Therefore, an (inverse) transposition with key length 10 will still be able to realign most of the original half columns (10 letters).
- In contrast, when an interim ciphertext with 35 rows is transformed into a final ciphertext, the alignment modulo 10 of most of the groups is not preserved.

3.11. *Solving ICT Messages with* $n_2 = 2n_1$

Four messages could not be solved when assuming a key length between 15 to 25, and a complete plaintext rectangle (CCT), as follows:

- BIS215 (`36/19 72/19`)
- BAL179 (`56/9 112/9`)
- BAL50 (`20/21 40/21`)
- BAL51B (`40/21 80/21`)

Those messages were then tested with key lengths that result in ICT, and all could be solved using a key length of 20. For example, the decryption for BAL50 is shown here:

```
SECRETLDBONEONEZEROF
OROFROMKOGBARAREPEAT
EDCHIJIIIIYRTELFAHTW
OONEZEROOOODESPATCHI
NGFIVEHUNDREDPOUNDST
OCHIJITUESDAYCOMMATW
OONEOCTOBERRRRTHISWI
LLBRINGTOTALSENTSINC
ELASTWEEKTOTWOTHOUSA
NDPOUNDSSS
```

Transposition key:

```
19, 5, 13, 0, 10, 15, 3, 6, 1, 12, 7, 8, 11, 2, 14, 18, 9, 16, 17, 4
```

3.12. *Solving Messages with $n_2 = 2n_1 - 1$*

In messages with markers so that $n_2 = 2n_1 - 1$, the (final) ciphertext has an even number of groups, therefore it cannot be split into two halves with exactly the same lengths. It was not clear whether another encryption scheme was used for those messages, or some adaptation was required to the encryption scheme hypothesis.

Various tests were made in order to identify where the ciphertext "middle" position should be, e.g., in the middle of the median group, before it, or after it. The presence of the n_1 marker was helpful in that regard, as it appeared right after $n_1 = (n_2 + 1)/2$ groups. When assuming the first marker to indicate the 'middle' position of the ciphertext (with this extended definition of the 'middle' position), successful recovery was achieved for additional messages assuming key lengths resulting in CCT, and for others, allowing for key lengths that result in ICT. Most of the messages had markers of the form `75/d 149/d`, e.g., BAL141A with `75/16 149/16`. Others were shorter, such as BAL16 with `28/20 55/20`, for which the decryption and the key are shown here:

```
PARTTWOBEGINSDOCTORU
CHEASLEADERANDCHIDIO
FONGTOGETHERWITHERON
INICOMMATOGOANDEXPLO
REALLTHEPOSSIBILITIE
SANDREPORTTTTINTHELI
GHTOFTHISCOMMAIWOULD
LIKETOVARYTHEREQUEST
TOMISTERERONINITOSAY
THATHEISREQUESTEDTOR
ETURNTOFLANDINIMMEDI
ATELYAFTERTHEYUGOSLA
VIATRIPPARAPLEASEADV
ISEEE
```

Transposition key:

```
19, 4, 13, 0, 8, 15, 3, 5, 1, 11, 6, 7, 9, 2, 14, 18, 17, 12, 10, 16
```

Having solved all the messages in the collection of Frode Weierud's intercepted messages, one last question remained, from the cryptographic perspective: What was the purpose of the two extra groups?

3.13. *Reconstructing the Indicator System*

A hypothesis was raised as soon as the existence of two extra groups was ascertained, that one or both serve as some kind of indicator. This hypothesis was also supported by the fact that the keys were almost always different, even for messages of the same size and on the same day, with the exception of three messages, BAL25B, BAL26A and BAL26B, which share the same key. For those three messages, one of the two extra groups was identical, BICTR, at the same position in the ciphertexts, that is, the sixth group back from the middle-point marker n_1. It was also thought that the purpose of that middle point marker was intended to help in locating the indicator and the position of the segment that needed to be moved back to the beginning, in order to obtain the original interim ciphertext.

The keys recovered so far were tabulated, together with the extracted indicator. They could be roughly clustered into three ranges of dates, as follows:

- August 4 and 9 - the length of all keys is 20.
- August 10, 11, and 16 - key length is 21.
- October 19, 20, and 21 - key length is 20.

With some exceptions, the keys recovered by hillclimbing in each cluster are quite similar. In the case of three messages from August 4, they are identical, as shown in Figure 18.

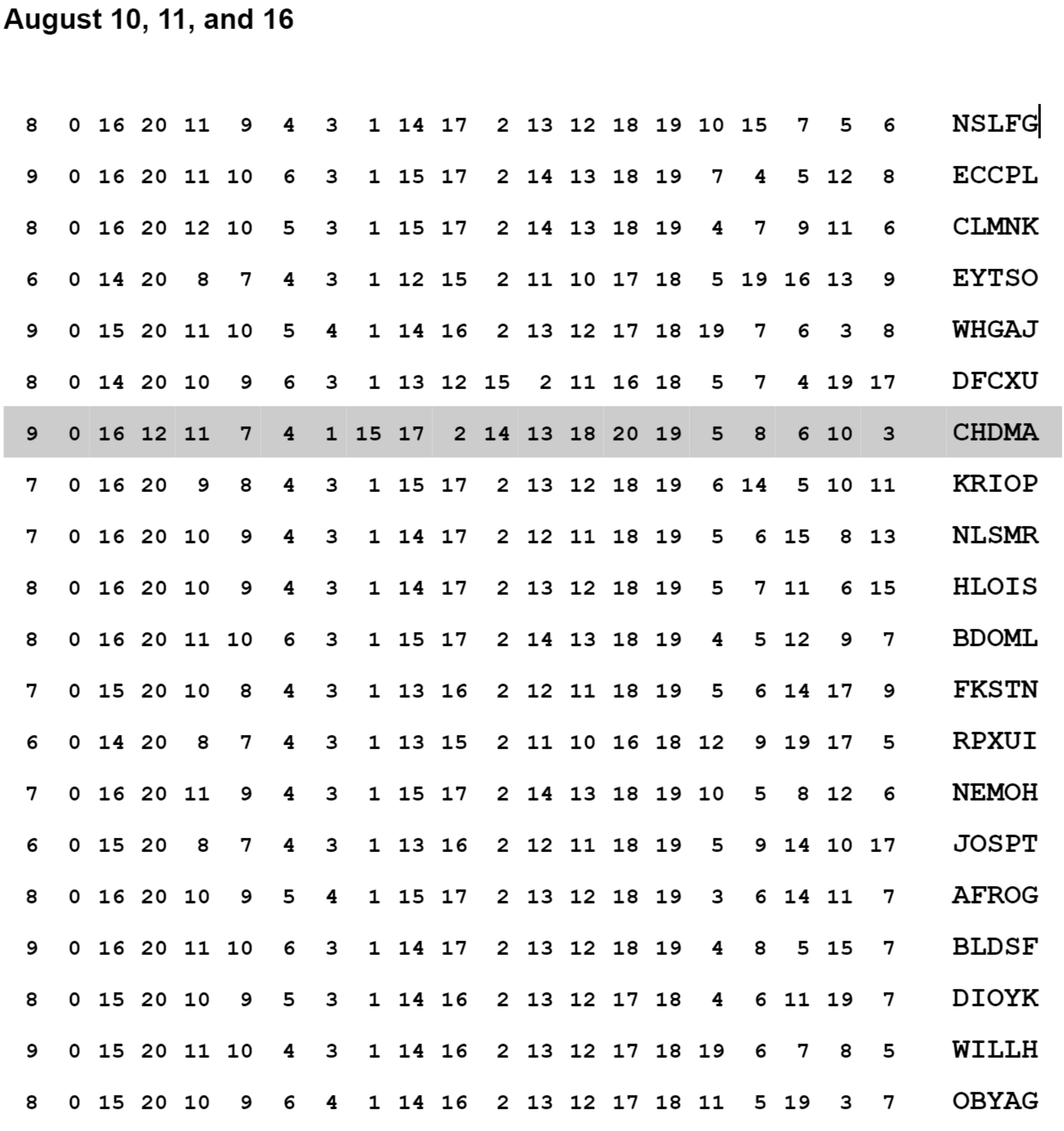
August 4 and 9

3	0	9	17	4	11	7	1	12	18	14	13	5	19	2	16	10	6	8	15	SMIKP
5	0	10	16	6	11	9	3	12	17	14	13	7	18	4	1	8	2	19	15	BICTR
5	0	10	16	6	11	9	3	12	17	14	13	7	18	4	1	8	2	19	15	BICTR
5	0	10	16	6	11	9	3	12	17	14	13	7	18	4	1	8	2	19	15	BICTR
4	0	8	17	5	10	7	2	11	14	12	6	19	3	18	15	16	13	1	9	RONAM
4	0	9	16	6	10	8	2	11	17	13	12	7	18	3	1	15	14	19	5	BROTH
6	0	10	16	7	11	9	2	12	17	14	13	8	18	3	5	15	1	4	19	GODET
6	0	10	17	7	12	9	4	13	18	15	14	8	19	5	2	1	3	16	11	BADOM
4	0	10	16	5	12	9	2	13	17	15	14	6	18	3	1	7	8	19	11	DJJYM

Figure 18. Recovered keys and indicators for August 4 and 9

The three identical keys share the same indicator, BICTR. The other keys in the group seem to be closely related, with a variance of +/- 3 in the numerical value of the first ten elements of the key. The variance is more pronounced in the last ten elements. Could the indicator mostly affect the elements in the second half of the key?

A similar pattern was discernible in the keys from August 10, 11, and 16 (with the recovered key associated with indicator CHDMA being less similar than the other keys) as shown in Figure 19.



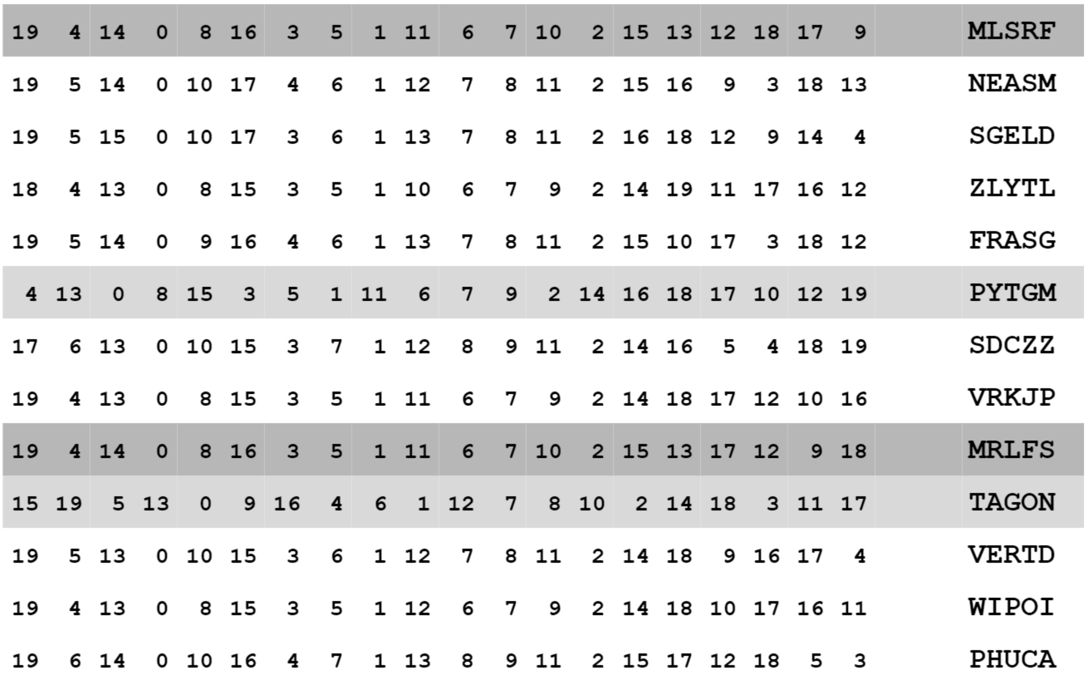
August 10, 11, and 16

8	0	16	20	11	9	4	3	1	14	17	2	13	12	18	19	10	15	7	5	6	NSLFG
9	0	16	20	11	10	6	3	1	15	17	2	14	13	18	19	7	4	5	12	8	ECCPL
8	0	16	20	12	10	5	3	1	15	17	2	14	13	18	19	4	7	9	11	6	CLMNK
6	0	14	20	8	7	4	3	1	12	15	2	11	10	17	18	5	19	16	13	9	EYTSO
9	0	15	20	11	10	5	4	1	14	16	2	13	12	17	18	19	7	6	3	8	WHGAJ
8	0	14	20	10	9	6	3	1	13	12	15	2	11	16	18	5	7	4	19	17	DFCXU
9	0	16	12	11	7	4	1	15	17	2	14	13	18	20	19	5	8	6	10	3	CHDMA
7	0	16	20	9	8	4	3	1	15	17	2	13	12	18	19	6	14	5	10	11	KRIOP
7	0	16	20	10	9	4	3	1	14	17	2	12	11	18	19	5	6	15	8	13	NLSMR
8	0	16	20	10	9	4	3	1	14	17	2	13	12	18	19	5	7	11	6	15	HLOIS
8	0	16	20	11	10	6	3	1	15	17	2	14	13	18	19	4	5	12	9	7	BDOML
7	0	15	20	10	8	4	3	1	13	16	2	12	11	18	19	5	6	14	17	9	FKSTN
6	0	14	20	8	7	4	3	1	13	15	2	11	10	16	18	12	9	19	17	5	RPXUI
7	0	16	20	11	9	4	3	1	15	17	2	14	13	18	19	10	5	8	12	6	NEMOH
6	0	15	20	8	7	4	3	1	13	16	2	12	11	18	19	5	9	14	10	17	JOSPT
8	0	16	20	10	9	5	4	1	15	17	2	13	12	18	19	3	6	14	11	7	AFROG
9	0	16	20	11	10	6	3	1	14	17	2	13	12	18	19	4	8	5	15	7	BLDSF
8	0	15	20	10	9	5	3	1	14	16	2	13	12	17	18	4	6	11	19	7	DIOYK
9	0	15	20	11	10	4	3	1	14	16	2	13	12	17	18	19	6	7	8	5	WILLH
8	0	15	20	10	9	6	4	1	14	16	2	13	12	17	18	11	5	19	3	7	OBYAG

Figure 19. Recovered keys and indicators for August 10, 11, and 16

The recovered keys for October 19, 20, and 21 were more interesting, as shown in Figure 20.

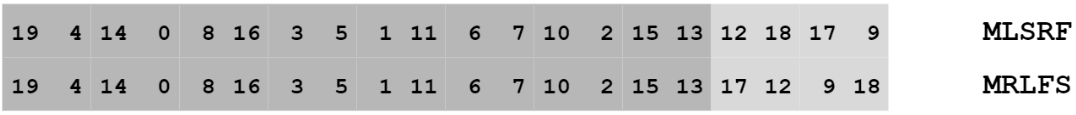
October 19, 20, and 21



19	4	14	0	8	16	3	5	1	11	6	7	10	2	15	13	12	18	17	9	MLSRF
19	5	14	0	10	17	4	6	1	12	7	8	11	2	15	16	9	3	18	13	NEASM
19	5	15	0	10	17	3	6	1	13	7	8	11	2	16	18	12	9	14	4	SGELD
18	4	13	0	8	15	3	5	1	10	6	7	9	2	14	19	11	17	16	12	ZLYTL
19	5	14	0	9	16	4	6	1	13	7	8	11	2	15	10	17	3	18	12	FRASG
4	13	0	8	15	3	5	1	11	6	7	9	2	14	16	18	17	10	12	19	PYTGM
17	6	13	0	10	15	3	7	1	12	8	9	11	2	14	16	5	4	18	19	SDCZZ
19	4	13	0	8	15	3	5	1	11	6	7	9	2	14	18	17	12	10	16	VRKJP
19	4	14	0	8	16	3	5	1	11	6	7	10	2	15	13	17	12	9	18	MRLFS
15	19	5	13	0	9	16	4	6	1	12	7	8	10	2	14	18	3	11	17	TAGON
19	5	13	0	10	15	3	6	1	12	7	8	11	2	14	18	9	16	17	4	VERTD
19	4	13	0	8	15	3	5	1	12	6	7	9	2	14	18	10	17	16	11	WIPOI
19	6	14	0	10	16	4	7	1	13	8	9	11	2	15	17	12	18	5	3	PHUCA

Figure 20. Recovered keys and indicators for October 19, 20, and 21

While two keys (associated with PYTGM and TAGON) were materially different from the rest, one pair stood out: MLSRF, and MRLFS. Those indicators are composed of the same letters, four of them in a different order. Those keys are shown together in Figure 21, highlighting the parts of the numerical key that are identical, and those that differ.

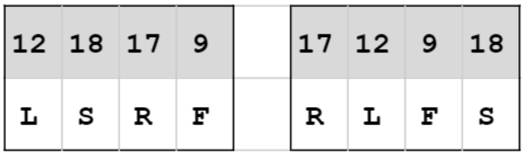


19	4	14	0	8	16	3	5	1	11	6	7	10	2	15	13	12	18	17	9	MLSRF
19	4	14	0	8	16	3	5	1	11	6	7	10	2	15	13	17	12	9	18	MRLFS

Figure 21. Keys with similar indicators

The first 16 key elements are the same, while the last four differ. This number of different key elements - four, is the same as the number of letters that differ in the indicators MLSRF and MRLFS, and the differences are at the end of the keys and of the indicators, respectively.

Next, the last four elements of the keys and of the indicators were examined, as shown in Figure 22.



12	18	17	9		17	12	9	18
L	S	R	F		R	L	F	S

Figure 22. Keys with similar indicators – numerical order analysis

It can be seen that in both keys, the same number represents the same indicator letter, e.g., 12 represents L.

More generally, the numerical order reflects the alphabetical order, that is $F < L < R < S$ and the same order applies to their numerical representation, that is $9 < 12 < 17 < 18$. This characteristic was found to hold true for the vast majority of the keys (looking at the last five key elements) and their associated indicators.

A hypothesis was proposed to factor in those findings. It was assumed that the key for each message was constructed as follows:

- A (secret) base key, in effect for multiple days, is exchanged in advance by the communicating parties.
- For each message, the operator selects a five-letter message key (it is not clear if he needed to select it from a list, or just choose five random letters). This message key is sent in clear as an indicator (as described in Section 3.9).
- The message key is appended to the base key, to form the full alphabetical message keyword.
- From this keyword, a numerical key is extracted, using the rules described in Section 3.4.

The main purpose of this method was probably to generate a different key for each message. It also explains why attempts to solve message using multiple anagramming failed, because except for the three messages with `BICTR`, each message had a unique key.

The next question was how to reconstruct the base keys from the recovered (numerical) keys and five-letter message key indicators. At first, an attempt was made to extract one of the base keys, by establishing a list of constraints derived from the position and order of the key elements and of the letters of the indicators. A matching base key for August 10, 11, and 16, could be found with tedious manual work:

`MATZONEBASTARQUW`

Since the other time periods included a smaller number of keys, a more generic automated method was developed, employing hill-climbing to search for the optimal base key, each time changing one of its letters. To assess the quality of a putative base key, each indicator is appended to it to create a putative keyword, from which a putative numerical key is computed. Each putative numerical key – denoted as PK – is compared to the recovered numerical key – denoted as RK. All possible pairs of positions i and j are examined in PK and RK:

- If $PK_i > PK_j$ and $RK_i > RK_j$ one point is added to the score.
- Similarly, if $PK_i < PK_j$ and $RK_i < RK_j$ one point is added to the score.

With this method, the following base keys could be recovered:

- August 4 and 9: `HALTINKENTONITE` or `HAMTINKENTONITE`.
- August 10, 11, and 16: `MATZONEBASTARQUW` or `MATZONEBASTARQUV`.

- October 19, 20, and 21: ZENAFOBEAKEEGAN.

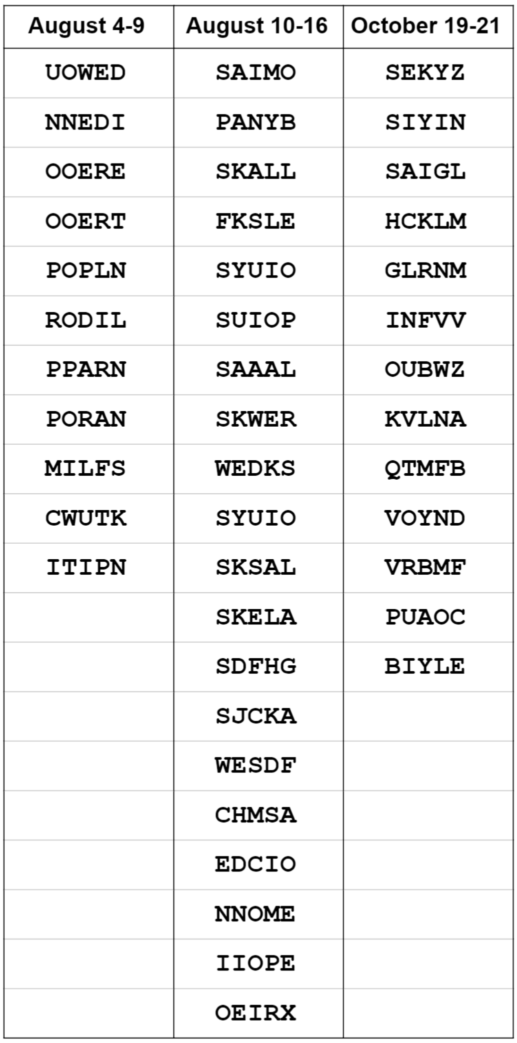
While most of the recovered keys fully matched the key generated by combining the relevant base key and the message key, there were some discrepancies, some of which could be observed already in Figures 18, 19, and 20. In five messages, BAL28 (RONAM), DARTLX1D (DFCXU), DARTLX1E (CHDMA), BAL15 (PYTGM), and BAL40 (TAGON), the recovered key had several mistakes, mostly due to extensive garbles that affected entire columns. In BAL139B, the indicator turned out to be wrong, as a result of a garbled first letter (should be HLSMR, was wrongly transcribed as NLSMR).

Hypotheses for the Second Unused Group

The precise role of the second unused group (the penultimate group before marker n_1/d) could not be yet established. The following hypotheses were considered:

(1) A dummy group, intended to further disrupt the order of the ciphertext groups, after transposition.
(2) Some kind of message integrity check, so that errors in encryption, transmission and reception can be detected by the receiving side.
(3) Integrity check for the indicator, as a corrupted indicator would not allow the receiving side to properly decrypt the message.
(4) Some kind of signature, so that the identity of the transmitting side can be ascertained by the receiving side.

Figure 23 shows the second unused groups for the three periods messages were intercepted.



August 4-9	August 10-16	October 19-21
UOWED	SAIMO	SEKYZ
NNEDI	PANYB	SIYIN
OOERE	SKALL	SAIGL
OOERT	FKSLE	HCKLM
POPLN	SYUIO	GLRNM
RODIL	SUIOP	INFVV
PPARN	SAAAL	OUBWZ
PORAN	SKWER	KVLNA
MILFS	WEDKS	QTMFB
CWUTK	SYUIO	VOYND
ITIPN	SKSAL	VRBMF
	SKELA	PUAOC
	SDFHG	BIYLE
	SJCKA	
	WESDF	
	CHMSA	
	EDCIO	
	NNOME	
	IIOPE	
	OEIRX	

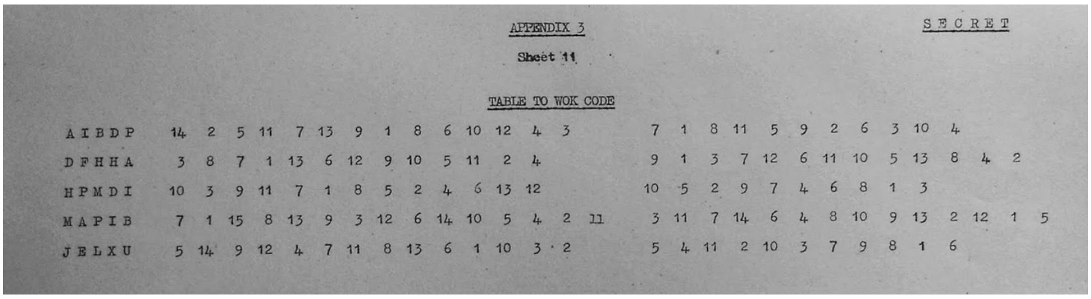
Figure 23. Unused five-letter groups

It is evident that those were not randomly generated (at least not using a strong randomization method). For example, in the August 10 to 16 messages:

- 11 of the 20 groups start with the letter S.
- Several have four letters in common, for example:
  - `SKALL`, `SKELA`, and `SKSAL` (A, K, L, S)
  - `WEDKS` and `WESDF` (D, E, S, W)
  - `SUIOP` and `SYUIO` (I, O, S, U)
- Many others have 3 letters in common, e.g.:
  - `FKSLE`, `SKELA`, `SKWER`, `WEDKS` (E, K, S)

If the second unused group was indeed intended to serve a dummy, a more random distribution would have been expected.

Considering the second hypothesis, a checksum (or a more basic parity check) in theory may help detect errors and validate the integrity of a transmitted cryptogram. However, manually computing some kind of checksum would have been a tedious and error-prone process. Also, with transposition ciphers, a missing letter/group (or extra letter/group) is more damaging than a wrong letter. In the present collection



APPENDIX 3

Sheet 11

S E C R E T

TABLE TO WOK CODE

AIBDP	14 2 5 11 7 13 9 1 8 6 10 12 4 3	7 1 8 11 5 9 2 6 3 10 4
DFHHA	3 8 7 1 13 6 12 9 10 5 11 2 4	9 1 3 7 12 6 11 10 5 13 8 4 2
HPMDI	10 3 9 11 7 1 8 5 2 4 6 13 12	10 5 2 9 7 4 6 8 1 3
MAPIB	7 1 15 8 13 9 3 12 6 14 10 5 4 2 11	3 11 7 14 6 4 8 10 9 13 2 12 1 5
JELXU	5 14 9 12 4 7 11 8 13 6 1 10 3 2	5 4 11 2 10 3 7 9 8 1 6

Figure 24. SOE double-transposition sample keys

of ciphertexts, markers are provided that indicate the beginning, middle, and end positions of cryptograms, as well as the counts of five-letter groups, and those are useful in handling the former type of errors (see Section 3.5).

The third hypothesis, i.e., an integrity check for the indicator, is a likely option since a corrupted indicator would not allow the receiving side to properly decrypt the message. Unfortunately, we were not able to establish a clear connection between the first and second unused groups/indicators.

To assess the fourth hypothesis, some background on a WWII transposition cipher used by the British Special Operations Executive (SOE) and its relevance to the Biafran ciphers is given here. According to Marks (2012), the SOE initially used a double transposition cipher with keys derived from poems, to communicate with its agents in German-occupied European countries, including France. Marks identified the weaknesses of such a scheme, which frequently led to the arrest of French Resistance fighters. Firstly, the agent could reveal under torture the book from which the poems were taken. Secondly, the solution of a single ciphertext could lead to the source of the poems. Thirdly, there was nothing to prevent the reuse of the same poem, allowing for multiple anagramming attacks.

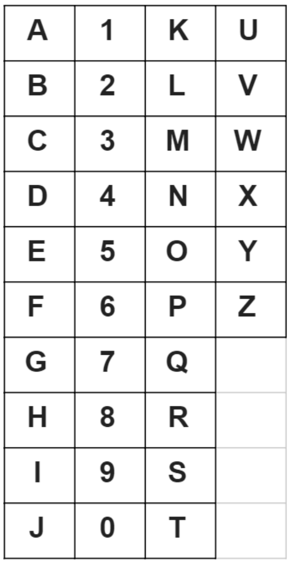
Marks proposed a new scheme, based on one-time random keys. An agent dispatched to Europe would carry with him a set of transposition keys, written on strips of silk, containing pairs of keys (one for each step of the double transposition) randomly generated, rather than derived from poems. Next to each pair, a five-letter indicator would be inscribed as well. To encrypt a new message, the agent would perform the following steps:

- Select a strip with a pair of keys.
- Use the two keys to encrypt the plaintext.
- Insert the indicator as part of the transmission.
- Destroy the keys, by tearing down the strip from the silk sheet, and burning it.

With this process, enemy cryptanalysis would be much harder. Each key was used only once, thwarting any attempts at multiple anagramming. Furthermore, the capture of an agent would not result in the compromise of other encoded transmissions, as in the case of keys derived from a book of poems. Also, agents would likely not remember previously used keys, so previously transmitted messages would not be compromised if the agent was arrested.

An example of such a list of keys is illustrated in Figure 24 from Miersemann (1944).

Marks realized that if an agent was captured, he could still be forced to send messages prepared by German intelligence and containing false information. He therefore suggested an additional five-letter indicator, based on the agent identifier, and a coding



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

Figure 25. SOE agent identifier coding

table (see Figure 25).

For example, if the agent unique identifier is `JTA` then the five-letter group is created as follows. First letter is random (e.g., C), second letter equals a number based on the table above. For example `H=8`. This means that the letters of the agent's code are moved forward eight steps, so:

```
J+8=R
T+8=B
A+8=I
```

So the agent identifier group will be `CHRBI`.

A final message ready for transmission would include:

- The key indicator (e.g., `AIBDP`).
- The agent coded identifier (e.g., `CHRBI`).
- The ciphertext.
- The key indicator, again (e.g., `AIBDP`).
- The total count of five-letter groups and a date.

If the agent was captured, he could simply generate a wrong agent identifier.

Going back to the fourth hypothesis for the second unused group in the Biafran ciphers: Could this be some kind of (encoded) agent identifier? To assess this hypothesis, it might be helpful to consider the origins of Biafran cryptography. We might consider the following possibilities:

- Knowledge on ciphers was obtained from public sources. This is unlikely, as in the late 1960s, there were few publications on the subject (e.g. Gaines (1956), Kahn (1967), Sinkov (1968)). Also, the methods used, while not highly secure, required practical know-how not available from the publications (e.g., one-time keys).
- Some Biafran officers were trained in cryptography, by British instructors, at

the time they were serving in the Nigerian army. On the one hand, the Biafran transposition scheme is simple (a single transposition). On the other hand, it includes a mechanism to avoid depths by creating one-time keys (and including a five-letter indicator in the message). Since the British SOE had created the (double) transposition scheme also based on one-time keys and key indicators sent as part of the messages, it is possible that the Biafran ciphers were at least inspired by knowledge transferred by the British to the Nigerian army.

- Training and methods were obtained from France. There is ample evidence that France, under the direction of Jacques Foccart, de Gaulle's Secretary-General for African and Malagasy Affairs, provided covert support to the Biafran state in a wide range of topics, from arms purchase and smuggling, recruitment of mercenaries, propaganda, as well as securing support and recognition by a number of African countries, such as Gabon and Ivory Coast (see Griffin (2015)). More specifically, they established a system of encoded radio messages between general Ojukwu and Philippe Lettéron, Foccart's man in Libreville, described in (Bat 2018, p. 96). This system was said to be "comparable to the codes used by the [French] Resistance" in WWII. In WWII, Foccart and several of his collaborators had served in the Bureau Central de Renseignements et d'Action (BCRA), the intelligence service of the Free France. The BCRA worked closely with SOE and the Resistance, and would have used SOE codes to communicate with agents in France. Interestingly, the same codeword – `Big Brother` – for Félix Houphouët-Boigny, the president of the Ivory Coast, was used in the Biafran ciphers and in the code internally used by the Foccart network, further hinting at Foccart's team involvement in Biafran cryptography (Bat 2018, p. 96) (Grahn 2019, p. 304).

Assuming that the most likely source for the cryptographic methods used by the Biafran stage was France and Foccart's network, inspired by the French Resistance and SOE ciphers, it is possible that the transposition cipher scheme used by Biafran envoys also included a sender identifier. On the other hand, those identifiers were used in WWII for agents in enemy territory and not for fixed stations as in the Biafran network. Furthermore, the authors were unable to identify how those could have been generated.

The exact nature of the second unused group thus remains a mystery.

3.14. *Earlier Messages*

The team received three additional transcripts that had been kept by the FRA, partially dated - with day of the month and the month, but without the year. Furthermore, the transcripts did not include the markers found in the set of messages from 1969, and they had no label (e.g, BAL25). In this section, we simply label them as FRA1, FRA2, and FRA3.

At first, attempts were made to decipher the messages assuming the encryption scheme, the indicator system, and one of the three base keys used for the 1969 messages. Those attempts were not successful. This might have indicated that other base keys were in effect.

Interim ciphertexts were then automatically generated from the ciphertexts, assuming the encryption scheme used for the messages from 1969 was also employed for those three messages. Hillclimbing with various key lengths was tried but the transposition could not be recovered. It seemed that there had been another scheme to transform an interim ciphertext into a final one.

Next, the hill-climbing algorithm was adapted so that it first selects a set of 4 to 10 groups from a random place in the final ciphertext, discards two of them, and moves the remaining ones to the beginning of the ciphertext to create an interim ciphertext, before starting a new round of hill climbing. With this method, some meaning fragments of words could be obtained when a segment not far away from the beginning was moved – to the beginning. This seemed to indicate that there might be no segment move at all, and just the insertion of two extra groups (the indicator and the dummy), near the beginning. Further tests produced promising results, when assuming that the extra groups were inserted at the same relative positions as in the 1969 scheme (see Section 3.9). With this method, the keys could recovered for two messages, from March 28 (FRA2) and April 3 (FRA3), both with a key length of 20:

FRA2

```
AMMENDNUMBEROFRIFLES
TOREADEIGHTZEROZEROR
EPEATEIGHTZEROZEROIN
STEADOFONEZEROZEROER
RORNEOUSLYREPORTEDPA
RAREFERENCEYRTELMFAO
NEFOURTHREEEEEWILLCO
NTACTACHEBEOVERWEEKE
NDANDPOSSIBLYVISITIN
ORDERASSESSSITUATION
ANDWILLREPORTBISECTS
ECRETFOURONESIXFORHE
FROMCCCCCCMYTELFOURO
NEONEEEEGRATEFULLLLL

Indicator: DJMZA

Transposition key:
 12, 0, 16, 11, 7, 2, 6, 13, 5, 17, 14, 18, 4, 9, 15, 3, 8, 10, 19, 1
```

FRA3

```
APPRECIATEASKBANKOFA
NNZEHHOWTHISISSELLIN
GCOMMAWITHSOMEFIGURE
SOFSALESANDMAYBECOMM
ENTFROMBANKCHAIRMANN
NNTHANKSANDREGARDSCO
MMABERNHARDTENDSSSSW
ILLBEGRAFULFOREARLYR
EPLYBISECTSECRETFOUR
FOURTWOFOROFROMIKKKK
FOLLOWINGREQUESTRECE
IVEDTODAYFROMBERNHAR
DTCOMMAGENEVABEGINSS
```

```
SSREGARDINGTWOFIVEZE
ROZEROZEROZEROZEROZE
ROPOUNDSDEFENCEBONDI
SSUESECONDAPRILCOMMA

Indicator: ADHOC

Transposition key:
 11, 12, 15, 14, 16, 10, 17, 4, 5, 19, 3, 8, 7, 13, 18, 0, 2, 6, 9, 1
```

The key for FRA3 is quite different from the key for FRA2, indicating that they were not generated from a common base key. It seems, however, that each of them was generated from some base key, as the numerical order of the last five elements of the key matches the alphabetical order of the letters of the indicator.

FRA1

An additional effort was required for FRA1 (March 16), which was shorter, and could not be solved assuming CCT. It was finally solved when allowing for ICT and with a key length of 18, as follows:

```
SECONDQUESTIONNNNND
ETAILSINMYNEXTMAIL
BISECTSECRETTHREET
HREEZEROFORHAMILTO
NFROMAMBROSEEEEYRT
ELMFATHREESEVENNNN
YESISTHEANSWERTOYO
URRR

Indicator: FCDAH

Transposition key:
 11, 16, 0, 17, 13, 2, 14, 8, 10, 5, 9, 12, 15, 6, 3, 4, 1, 7
```

From 1968 or 1969?

It was clear that between the time those three messages (FRA1, FRA2, and FRA3) had been sent and August 1969, there had been a change in the encryption scheme. The indicator and the extra dummy were still inserted at the same positions in the interim ciphertexts, but in the messages from August and October 1969, the initial block of eight groups (which include the inserted indicator and dummy) had to be moved right before the middle position marker. The change was introduced in 1969 probably to add another element of confusion and thwart attempts to solve the transposition, by further disrupting the alignment of the original plaintext columns.

According to Grahn (2019), on 15 July 1969 Chiji reported from Paris that "there is now clear evidence that the old code no longer is secure". According to Dr. Dike (Dr. Kenneth Dike) the "old code had apparently been broken 18 months ago". Colonel Ojukwu replied on 16 July notifying all Biafran units that "special instructions are given to the cipher operators units that from now on messages concerning supplies, security and political reports must be sent with the new system. The only exception is for circular messages." It might very well be that the new system refers to the change in the encryption scheme.

We still needed to determine the year the FRA1, FRA2, and FRA3 messages were sent. Since the war started in July 1967 and it ended in January 1970, the FRA messages (which are from March and April) can be either from 1968 or 1969.

Another piece of information strongly hints at the year being 1968. According to Grahn (2019), from about 1 September 1967 the Biafrans also started to use codewords in the ciphertexts for place and country names. This list of codewords was replaced in September 1968 with a new and expanded list which was in use until the end of the war. In this new list frequently-used names had multiple codewords, e.g. Biafra which had the codeword `ANNZEH` in the first list would be replaced in the second list with the codewords `DALFON` or `FLANDIN`.

The "`Bank of ANNZEH`" is mentioned in FRA3. This codeword belongs to the list in effect before September 1968. Therefore, FRA1, FRA2, and FRA3 are most likely from March 16, March 28, and April 3, 1968, respectively.

3.15. *Formatting the Decrypts and Correcting Errors*

A special program was developed to format the raw decrypts so that they are more readable. The raw decrypt is in the form of a consecutive sequence of letters. This sequence had to be split into logical elements, mainly words, numbers, and punctuation signs. The process is semi-automatic, allowing for some automatic interpretations to be overridden. First, the sequences that represent punctuation are interpreted as follows:

- `COMMA` → ,
- `COLON` → :
- `SEMICOLON` → ;
- `BRACKET` → (
- `UNBRACKET` →)
- `DASH` → -
- `STROKE` → /
- `PARA` starts a new line, possibly adding a full stop to the preceding word.

If a letter is repeated more than twice, this is interpreted as a full stop being added at the end of that word. '`ADVISEEEE`" is replaced by "`ADVISE.`", for example.

Next, numerals that are spelled out (e.g., `ZERO` or `HUNDRED`) are interpreted. Composite numerals such as `ONE HUNDRED` or `TWO ONE` are replaced by 100 and 21, respectively. Other numerals used standalone (e.g., `FIVE NURSES`) are left spelled out.

Some names and places appear in the messages as code words. A list of code words was compiled as progress was made in deciphering the messages, and for some, an interpretation could be assigned. In the readable output, the codewords are formatted in full capital letters, e.g., `SUCRONY`, with the meaning specified if known (e.g., `FLANDIN[=Biafra]`). Other names and places which are not in the form of a codeword and appear in a list (also compiled incrementally), are capitalized, e.g., `Chiji` or `Libreville`.

Using a dictionary, the remaining parts of the decrypts are split into words, with the option of overriding the automated split. An example of a formatted output is given below for BAL28:

```
SECRETPARSIXZEROTWOF
ORUGWUMBAFROMARTHURR
```

```
EPEATEDOANDNWANZEEEE
IHOPETOBEINDALFONFRI
DAYNIGHTTTTPLEASECON
TACTMYPERMANENTSECRE
TARYANDADVISEHIMTOSE
NDMETRANSPORTTTTALSO
CONTACTMRFINECOUNTRY
OFTHEPOLICEFORMYORDE
RLYYYYPLEASEDONTLETM
EDOWNASTRANSPORTISNO
WAVERYSERIOUSPROBLEM
ATULIANDIWILLHATETOB
ESTRANDEDAGAINASUSUA
LLLLREGARDSSSSS

>>> 4/8/1969

>>> BAL28 128/4/8 BIS  -  04 1900
MOST IMMEDIATE
FOR UGWUMBA FROM ARTHUR REPEATED O AND NWANZE

Secret PAR 602:
For Ugwumba from Arthur repeated O and Nwanze. I hope to be in
DALFON[=Biafra] Friday night. Please contact my permanent secretary
and advise him to send me transport. Also contact Mr Finecountry of
the police for my orderly.
Please don't let me down as transport is now a very serious problem at
Uli and I will hate to be stranded again as usual. Regards.
```

The readable printouts were highly useful in order to recover letters missing from the transcripts, and to fix various garbles due to reception or transmission errors. Spelling errors in most cases were not corrected (when it could be established that there was a spelling error, such as `GRAFUL` instead of `GRATEFUL` in one of the messages). There were very few of those, however. Overall, it seems that the messages were carefully written and encrypted.

3.16. *Five-figure ciphers analysis*

We began with the same process as for the five-letter ciphers - a frequency count of the digits, singly and in groups, and by looking for repeated groups of digits in the transcripts as presented, and transposed into matrices with column heights of five or ten. The transcripts do not contain the "halfway" and "end" markers found in the five-letter ciphers. However, we noticed that the last five-figure group is a count of the number of groups.

BAL157 and BAL158 are messages without garbles, with 5 x 62 and 5 x 154 numbers. The digit "3" occurs only 51 times in BAL158. Excluding the group count, BAL158 has 764 legible decimal digits, and to have any digit present 51 or fewer times occurs about 0.8% of the time in a random collection of this length. Nothing special was observed in an analysis of repeated substrings or a frequency count of two to five decimal digit numbers.

Name	Frequency count
Ugwumba	11
Chiji	6
Chris	6
Onubogu	6
Eronini	5
Kogbara	5
Austine	4
Bernhardt	4
Chabert	4
Ugboma	4
Akpan	3
Arthur	3
Emodi	3
Ichoku	3
Iwunze	3
Kennedy	3
Nwachukwu	3
Nwanze	3
Nwogu	3
Nwokedi	3
Obi	3
Obonna	3
Onah	3

Table 1. Names table

"One-time pad" traffic would require a secure link, such as a courier, with the capacity to transmit and receive a key of the same length as the messages, and no key should ever be reused.

4. Interpretation of Names and Codewords

In this section, we present the main characters mentioned in the messages, as well as our interpretation of some of the codewords.

Table 1 lists all names mentioned in plaintexts more than twice.

The most frequently mentioned name in the messages is "Ugwumba", mentioned eight times in the preambles of the messages (BAL28, BAL29, BAL30, BAL31, BAL51, BAL151, BAL214, and BIS215) in both August and October 1969. This is Austin Ugwumba, or A. E. O. Ugwumba, the Permanent Secretary (to the head of state of Biafra, Colonel Ojukwu) and Head of the Civil Service of Biafra.

The abbreviation "CC" in the messages refers to Christopher Chukwuemeka Mojekwu (1920-1982) (Ikejiani 2007, p. 483). Stremlau (2015, p. 166) recounts that he was part of the delegation to the Kampala peace conference in May 1968, and is described as "commissioner for internal affairs and Ojukwu's most trusted adviser". As "Commissioner of Home Affairs" he was part of the delegations to Libreville in July 1968 and to Addis Ababa in August 1968 (p. 190, 198). He also attended a meeting in Monrovia in April 1969 and was described as "one of Biafra's leading hawks" (pp 313-314). Jeffs (2012) refers to him as portrayed in Mezu (1972) as "the former Solicitor-General of the Eastern Region, Ojukwu's cousin, and Biafra's Interior Minister".

Mezu bases the "Ifedi squad" of his pseudo-fictional novel, "Behind the Rising Sun" (Mezu 1972) on real-life Biafrans in Paris. Jeffs explains who they are: "Raph Uwechue (the actual head of the office in France), C. C. Mojekwu, Dr. Kenneth Dike (former Vice-Chancellor of the University of Ibadan, later roving ambassador for Biafra), Francis Nwokedi (former head of Federal Ministry of External Affairs, afterwards a special advisor to Ojukwu and a foreign envoy)" and others. The squad in the novel is nepotistic, ineffective and often concerned with claiming the credit for arms deals, shopping, and staying in one of the most expensive hotels in Paris, the Hotel Lutetia. (Draper 1999, p. 65) writes "Templewood [Aviation] was dealing directly with Christopher Mojekwu who had by then [1968] become the most important Biafran outside Biafra".

de St Jorre (1972) describes Mojekwu as a "super hawk" (p112), "Biafra's powerful home minister and chief emissary in Europe" (p. 192-193), and "[Ojukwu's] closest confidant of all" (p. 397). After the war "Mojekwu finally left Lisbon for Chicago. At the end of one letter applying for a job he signed himself, 'Biafra's most senior refugee."' (p. 412). He taught at Lake Forest College from 1972 until his death in a car crash in 1982.

The name "Chris" may refer to Christopher Onyekwelu, described in a US State Department cable of 1970 as "Biafran finance man in Europe and brother-in-law of Ojukwu".

"Chiji" (referred to in messages from Paris, sometimes marked PAR - e.g. BAL28, 29, 30, 31, 40, 50) is Chiji (Chijioke) Dike. In the memoirs of Godwin Onyegbula (Onyegbula 2005, p. 182), the author "left Lisbon for home via Paris on 29 December 1969". Chiji Dike is described there as "our Biafran representative who had taken over from Ralph Uwechue" with "Chuma Azikiwe" and "Kogbara, our London representative". In this context, Kogbara is Ignatius Kogbara (d. 2002). Raphaël Chukwu Uwechue has been referred to as both Raph and Ralph.

"Onubogu" in the context of these message is Harold Onubogu of the Biafran Lisbon delegation house (Udekwu (2011); Ângelo (2019)). Draper (1999) explains that "Biafra's senior representative in Lisbon was H. N. Onubogu". Another Biafran figure sharing this surname was the aide-de-camp (ADC) to Ojukwu, Obi Udezuwe Onubogu. The messages contain a name "Obi" three times (BAL18, 179, 214). This is most likely Luke Obi, chief political officer of the Biafran Ministry of Foreign Affairs, stationed for some time on São Tomé.

Eronini refers to Barrister Rufus Eronini (BAL16) who put the Biafran diplomats in touch with "`Yugoslavian authorities`".

Austine refers to either Austine S.O. Okwu, based in Tanzania, the special representative to East and Central Africa (DARTLX, concerning the UN General Assembly) or Austine Okwesa (BAL15). Okwesa is referred to in Draper (1999) as "Austin Okwesa", Biafra's "UK Emissary" or "London-based agent."

Ugboma refers to Michael Ugboma of the Biafran Rome office (Getty Images (1969)). Ntieyong Udo Akpan (1924-) was Chief Secretary of the Government and Head of the Civil Service of Biafra.

Sylvanus John Sodienye Cookey (1934-) is referred to as "Commissioner for Special Duties, one of Colonel Ojukwu's closest confidants" by Forsyth (1977). His name is seen in the preamble of one of the unsolved five-figure ciphertexts, BAL027.

Arthur is Arthur Mbanefo, a roving diplomat (Mbanefo (2015)). Kennedy is Father Raymond Kennedy of Africa Concern; Nwanze is George Nwanze, Ojukwu's cabinet secretary; Okigbo is Dr Pius Okigbo; Nwogu is Egbert Nwogu, another Biafran diplomat; Nwokedi is Francis Nwokedi, as above, a Biafran emissary mentioned in

Codeword	Frequency count
DALFON	8
FLANDIN	5
TEYFIK	4
ASHDOD	3
SUCRONY	3
SUVICH	3
TENDENY	3
CODGER	2
GONONEH	2
HEYWOOD	2
HOBOKON	2
HUNABEL	2
KOLLONTAY	2
LUMETIER	2
MITLAR	2
MOSSMAN	2
NOMISER	2
PEDUOR	2
SMIGLEY	2
TUREEN	2
WELKIN	2

Table 2. Codeword table

de St Jorre (1972); Obonna is Dr. Aaron Obonna, a Biafran representative in West Germany, and so on.

Dr Otue is Dr Nwonye Otue, Biafra's special representative to the United Nations in New York.

The person "Chabert" of BAL29 remains unidentified.

The acronym "H. E." refers to "His Excellency" or Colonel Ojukwu throughout. The acronym "H. Y." is in many preambles and messages (e.g. BAL31, 51, 179, 214) and in cleartext (BAL162) but has not been identified. Similarly "O" refers to Ojukwu throughout.

Table 2 contains the list of codewords that occur more than once in the plaintexts.

`DALFON` and `FLANDIN` are codewords for Biafra while `TEYFIK` is Nigeria. From BAL139, we have an enormous number of codewords of locations with airports: `HUNABEL`, `HEYWOOD`, `CODGER`, `SUCRONY`, `ASHDOD`, `SUVICH`, `BIENNAL`, `HATHELY`, `HOMFRAY`, `LUMETIER`, `JAPURG`, `KAPPUT`, `TIKIOSH`, `PULTEN`, `KAGULAH`, `KOLLONTAY`, `SMIGLEY`, `MOSSMAN`, `CULLODEN`, `and KIMCHEY`.

The codeword `TENDENY` is found in messages BAL29, BAL31, and BAL40. BAL40 reads `Review in TENDENY press is unlikely before books appear in MERCIAH` and the context concerns reviewing English books in the French press. Thus, `TENDENY` seems likely to refer to France and `MERCIAH` to Paris.

BAL141 also proved useful as it referred to public figures and public events but still used codewords. This error in cryptographic protocol allowed us to identify many codewords. For example:

- "`[T]he return of Adoula who has been in KEACHEN these last four years`" indicated that `KEACHEN` is the USA.

- "PEDUOR was behind the sweeping changes" and "PEDUOR D.C." means that PEDUOR is Washington.
- "Jaja Wachukwu, TEYFIK's former foreign minister" indicated that TEYFIK is Nigeria.
- "Gizenga, the former leader of the Stanleyville govt now in HOLDPON" probably implies that HOLDPON is Moscow where he went to study.
- "the White House appears to have won the battle with the BULLITS" implies that BULLITS are the Belgians in the Congo.
- DARTLX refers to the "WALMSEY papal visit" meaning that WALMSEY is Uganda, as Pope Paul VI visited there from 31 July to 2 August 1969.

The interpretation of additional codewords is given in Section 6.

5. Traffic analysis

In this section, we identify the call signs and telex channel indicators used in the messages.

The messages were intercepted in Oslo and thus only the messages sent from Lisbon, Portugal to Biafra were printed out in Oslo.

The messages often refer to YR TLX (your telex) followed by FAF, MFA or FAH. As these are replies, the original messages would have been sent from within Biafra. The call sign used by the station in Biafra was LDA/3 or Luanda/3.

Similarly, the messages often begin with SECRET followed by another indicator, LNB, DAR, FRA, LSO, LDB, PAR, MAR, or GAB.

As above PAR refers to Paris, and the DAR messages, DARTLX, BAL139, BAL141 are all "FOR O FROM AUSTINE" with BAL139 "FOR ONUBOGU" as well. Since Austine Okwu was based in Dar es Salaam, Tanzania, it seems that DAR stands for that city.

LSO messages are often from Onubogu in Lisbon.

The GAB messages (BAL179) contain plaintext "here in Libreville" meaning that GAB is Gabon. The three messages within BAL179 are each marked "FROM HY".

Dr. Obonna was based in Frankfurt (FRA).

The message numbers (after the three letter indicator) are in sequential order for each indicator. For instance, we have message numbers 313 to 331 for FRA, 762 to 793 for LNB, and 289 to 296 for LSO (all incomplete).

The telex channel indicator meanings are further explained in Appendix B.

6. Content

We discuss the messages under the themes of (a) logistics, travel and shipments, (b) diplomatic efforts, (c) international diplomacy, (d) public relations activities and (e) expenses. We also note that other organizations, for instance the Swedish FRA ("National Defence Radio Establishment") signals intelligence agency and the FBIS (Foreign Broadcast Information Service) were listening into the telex link.

6.1. *Logistics, Travel, and Shipments*

In the messages, we see many references to air travel. For example, there are references to arms shipments via Lisbon, medical and aid visa applicants, food supplies, and travel to international conferences. Also, the roving diplomats of Biafra request land transport to be ready for them when they arrive at Uli ("Annabelle"), which was the busiest airport in Biafra in the time period spanned by the messages. Another smaller facility was the Uga airstrip.

de St Jorre 1972 noted that after a statement by de Gaulle in September 1968 on aid for Biafra, "French weapons, routed via Abidjan and Libreville, began to pour in" (p. 211). He goes on to explain the French motivation for its Biafran policy. He also notes that Lisbon was Biafran's "chief arms-buying mission" (p. 219) and the Portuguese provided assistance with airports at Lisbon, Bissau and São Tomé.

Message FRA2 dated 28 March 1968 is from C. C. Mojekwu to General Ojukwu. It refers to 800 rifles and contacting "Achebe". This may refer to Chinua Achebe, one of the roving ambassadors, who spent time in Lisbon and São Tomé.

The keyword `NOMISER` or `TUREEN` seems to refer to an airplane of some description. Messages which contain these codewords are BAL51 (`TUREEN`) and BAL214 (`NOMISER`). Airplane registrations are given explicitly in BAL51 and BAL214.

Message BAL51 dated 21 October 1969 is addressed to Austin Ugwumba from (Ignatius) Kogbara repeated O and H.Y. It is marked `LDB` (from London). It refers to requesting approval for Raymond Kennedy of Africa Concern (Afcon) to travel to Uli via `MITLAR` (presumably Libreville or São Tomé) on a DC-6A with registration `OO-GER`. This plane is referred to in (Draper 1999, p. 158). It was leased from Belgian International Air Services. The message then goes on to discuss the possibility of flights for salt and meat, and the extension of a hospital under the direction of Dr Edgar Ritchie. Dr Ritchie was an Irish obstetrician, and was the director of Queen Elizabeth Hospital in Umuahia, the capital of Biafra from September 1967 to April 1969. Message BAL214 dated 19 October 1969 is addressed to Austin Ugwumba and O from (Harold) Onobogu in Lisbon, repeated for Obi and H.Y. It is marked `LSO` (from Lisbon).

The plane referred to is N86525, an L-749A Constellation mentioned in Draper (1999). This was obtained by Biafra in late July 1969 from Western Airways. In late autumn, after a visit to São Tomé by FAA inspectors, it was re-registered as 5N85H. This airplane crashed on 28 November 1969 in Morocco, killing all aboard.

In the list of cargo, the first items are "`44 cases HAMILTON`" and "`47 cases containing 3000 rounds 20 mm for LASHAN`". The interpretation of `HAMILTON` and `LASHAN` is not clear, but "`20 mm`" may refer to Oerlikon 20 mm cannon ammunition (Venter (2016)).

BAL215 refers to the Biafra Air Force (BAF) (Iroh (1976)) and to `TAs` or `TAS` who wish their nationality to be kept confidential and who want to avoid photography. At this time, Count Carl Gustaf von Rosen of Sweden was reforming the Biafran Air Force. We were unable to determine what the acronym `TA` or `TAS` might stand for.

6.2. *Diplomatic Efforts and Politics inside Africa*

Message BAL141 describes the internal politics of Congo, with a long description of Mobutu's recent cabinet reshuffle, the struggle for outside influence between Belgium and the US, and the ethnic groups of the Mobutu ministry. For example, the ethnic groups the Binza and Mongos are mentioned; while the `DRAXTERNS` and `MOROUKS` seem to be codewords for other groups or ethnicities.

From the discussion of the "East and Central LATIVA Good Neighbours Conference" in BAL141, we were able to determine that TRANSOK was a codeword for Lusaka or Zambia, as the "Fifth Summit Conference of East and Central African States" was held in Lusaka from 14-16 April 1969. At the end of the message, TEYFIK is clearly a reference to Nigeria, and this codeword is repeated in the BAL139 and DARTLX messages. LATIVA was clearly a reference to Africa in general, seen in many messages.

Message BAL139 discusses flight arrangements for BIENNAL or HATHELY by the 25th August 1969. The airlines Alitalia, East African and Sabena were mentioned in plaintext (except that East African had been encoded to "East LATIVAN"). The Organization for African Unity (OAU) conference was held in Addis Ababa, Ethiopia, from 27 August to 6 September 1969. The message conveys the urgency of getting two teams into place. Thus, BIENNAL could refer to Ethiopia while HATHELY can refer to Addis Ababa. By examining the Sabena airline timetables of 1969 available online, we were able to make some guesses about the meanings of the codewords CULLODEN, KOLLONTAY and HUNABEL in BAL139.

The plaintext reads:

```
Sabena Airline flights from SUCRONY to MOSSMAN (ASHDOD) - only one
flight a week departs KOLLONTAY on Friday arriving CULLODEN
Saturday, returns to HUNABEL the next day (Sunday)
```

This might refer to a flight that in 1969 went from Brussels at 20:30 on Friday via Vienna (arrival 22:05 - departure 22:55) and that would arrive first in Entebbe/Kampala on Saturday at 08:20 departure 09:10 and finally arrive Nairobi at 10:10. This flight would return on Saturday evening from Nairobi at 20:30 with arrival first in Entebbe/Kampala on 21:30 with departure 22:30 for so to arrive in Vienna at 03:55 on Sunday morning again departing at 04:55 for Brussels where it would arrive at 06:25.

KOLLONTAY could be Vienna because there was another flight leaving for Entebbe from Brussels on Sunday, but this flight did not continue to Nairobi, so connecting KOLLONTAY with Vienna depended on what the destination CULLODEN was. CULLODEN must have been either Entebbe/Kampala or Nairobi. HUNABEL could, depending on the destination, be Entebbe, Vienna or Brussels.

We decided that the most likely possibility was that KOLLONTAY is Brussels, CULLODEN is Nairobi and that HUNABEL is either Brussels or Belgium. Note that the codeword list allows for multiple codewords for the same entry.

6.3. *International Diplomacy*

Rufus Eronini is a barrister mentioned in the message BAL16 of 20 October 1969, for N. U. Akpan from K (Kogbara), repeated CC and O. As the message refers to "Chidi Offong of my office", it is presumed to be from London where Offong was a Biafran representative. Eronini offered to introduce the Biafran delegation to "Yugoslav authorities at the highest level". He was then requested to return to Biafra immediately after the delegation visited Yugoslavia. As Yugoslavia is not mentioned in Stremlau (2015) at all, the Yugoslavian visit was perhaps not of a diplomatic nature; it could have been an attempt to procure Yugoslavian or Eastern European arms.

The message DARTLX (from Dar Es Salaam, the capital of Tanzania) from Austine Okwu on 11 August 1969, was sent in the context of Biafra seeking foreign recognition and struggling against the lack of diplomatic recognition from the OAU (Organization for African Unity). The main topic is the United Nations General Assembly Meeting.

It refers to many different countries given in codenames (e.g., "Latin American countries [which] could be lobbied through CODGER and YUCCAH"). The five permanent members of the Security Council (US, UK, France, Soviet Union and China) are named (in some order) as HOBOKON, GIDIRON, PENELOZAH, MAYNARD and "nationalist CHELTEN". We cross-referenced this with a sentence in message BAL141, also of a diplomatic nature, which read "there has been some tussle between the HOBOKON and BARTHOU on who should control the economic and political fortunes of the Congo."

The definite article before HOBOKON could mean that HOBOKON is the US, the UK, or the Soviet Union. In the context of trade and economic politics, Belgium and the US were competitors for the favours of the new Congolese republic. It was mainly the Congolese rich mineral deposits that interested the two countries. Thus, HOBOKON is most likely the US.

Strangely, Britain is mentioned again in plaintext: "QUETZAL and Britain will of course choose to stress the political phase ...".

Okwu suggested raising the Nuremberg principles of "crimes against humanity" and the genocide convention of 1948. Unfortunately, only the first five parts of the message are available.

However, this part of the message refers to the "so-called team of international observers". This observer team is mentioned by de St Jorre (1972, p. 283-284). The "Observer Team in Nigeria" was drawn from Britain, Canada, Poland, the United Nations and the OAU to inspect the behaviour of Federal troops. de St Jorre states that after sixteen months of investigations, the "OTN's presence and work ... undermined, if not totally destroyed the Biafran claim of genocide".

KEACHEN in the same context seemed to refer to the U.S.A. The secession of Katanga on 11 July 1960 from Congo, mentioned in BAL141, was supported by Belgium, while Congo-Brazzaville gained independence from France on 15 August 1960. The context of message BAL141 mentioning Katanga is interesting as de St Jorre 1972 explains how the Soviet Union and France viewed Biafra through the lens of the previous secessionist experience of Katanga. For example, Jacques Foccart, General de Gaulle's special adviser for African affairs, who helped obtained arms for Biafra, "was a firm believer in the use of mercenaries to back French policies and had employed them before, notably in Katanga and the Yemen."

Latin America is mentioned briefly in BAL193 in the context of discussing visa and flight arrangements. The plaintext states that the mission is confirmed for Chile and Argentina, while the arrangements for Brazil and Uruguay were "not yet concluded". (Stremlau 2015, p. 364-365) states that Dr Pius Okigbo (mentioned in BAL192, "Dr. Okigbo and Nwogu and his group"), Ojukwu's chief economic adviser, led a small delegation around Latin America for fund-raising in fall 1969. He was believed to have visited Peru, Chile, Bolivia, Ecuador, Colombia and Argentina. Stremlau mentions that the Biafrans discovered "a strong religious sympathy that had been aroused by the Catholic church."

6.4. *PR Activities*

One of the FRA messages, FRA3, is a message relayed from William Bernhardt, the Markpress executive in Geneva, dated 3 April 1968. Markpress was Biafra's public relations firm in Geneva, who organized and distributed media releases to various organizations (de St Jorre 1972, p. 305-307). The agency was described as "linked by telex to Biafra via Lisbon" and "distributing press reports, war communiques, briefings and photographs to five major news agencies and to 3,000 addresses". The Geneva headquarters was described as "a sort of unofficial embassy for the Biafrans".

In the message, IK asked O:

```
Regarding 25000000 pounds defence bond issue second April, appreciate
ask bank of ANNZEH [=Biafra] how this is selling, with some figures of
sales and maybe comment from bank chairman.
Thanks and regards, Bernhardt
```

The Bank of Biafra established its own currency, the Biafran pound, considered legal tender in the territory during the war. The first governor was Sylvester Ugoh, who signed the bank notes. Although we did not find Ugoh's name in the plaintexts we have, his name is present in Grahn's list. It is possible here that "IK" refers to Ochea Uduma Ikpa, Deputy Permanent Secretary in Lisbon; in other contexts, this might refer to Ignatius Kogbara.

Message BAL151 refers to a visa application for Robert Lotz and George Aczel, documentary filmmakers who were "`known friends and supporters of Biafra`". Their visas were to be approved after their recommendation of Dr Obonna in Frankfurt. We have been unable to find any trace of a documentary made by them.

Message BAL40 refers to the reception of books in the mass media, and mentions the writers Francois Debre and Jean-Francois Chauvel. Debre was considered by Heerten (2017) to be a pro-Biafra writer (like Forsyth) who wrote the book "Biafra An II" (Debré 1968) which won the 1968 Prix de la Critique Indépendante. Chauvel was a journalist from Le Figaro who wrote a series of articles in July-August 1968, comparing the conditions in Biafran camps to those of Buchenwald (Griffin 2015). He was also a "honorable correspondent" of the SDECE, which means an unofficial informer and assistant. (Bat 2018, p. 96)

During the war, the Foreign Broadcast Information Service (FBIS) of the US Central Intelligence Agency (CIA) was also monitoring the Biscaia traffic. Telegrams from 29 August and 17 September 1968 note that the station was transmitting from "Luanda" to "Biscaia" in Lisbon and that one of the items transmitted was referred to in a Reuters item. Reuters noted that the "press service" was operated through "a Geneva public relations firm receiving its news from the front via Lisbon"; that is, Markpress (Kriebel (1968a,b,c)).

6.5. *Expenses*

Message BAL25, 4 August 1969 from Dr (Aaron) Obonna in Frankfurt, refers to members of the delegation bringing Biafra into disrepute by not being able to pay their hotel or telephone bills. This is one of the first two messages we were able to decrypt, as the second part of both BAL25 and BAL26 used the same key and began with "`PART TWO BEGINS`".

There is a strong irony in these messages as we read about the "Arthur" from the messages, Arthur Mbanefo, who always stayed at one of the most expensive hotels in Paris, Hotel Lutetia, "whenever he was in Paris" (Mbanefo (2015)).

This was corroborated in Mezu (1972) where the initial action is set in the Hotel Lutetia and the delegates are given to expensive shopping trips, as in Iroh (1979).

Meanwhile, the leaders urged frugality: in message BAL74 (6 August 1969, for O from Chris, Lisbon), Chris was stipulating that officers could only be accommodated in hotels if the government guesthouse was full: “`We cannot afford to meet heavy hotel bills or Esta code which require immediate settlement.`”

In his pseudo-fictional book, Mezu explained: “Estacode is the living allowance paid to those in the diplomatic service while they are serving abroad. Very astute diplomatic servants can make lots of money this way.” UK Hansard (1968) defines it as “the Establishments code, or collection of rules and advice on staff management, for the non-industrial Home Civil Service.”

7. Conclusion

Transposition ciphers in a known language are easy to identify, but can be difficult to break if the transposition scheme is unknown. In the Biafran messages, a special variant of the columnar transposition cipher was employed, with a per-message key mechanism intended to avoid depths, i.e., multiple messages enciphered with the same key (historically, unknown transpositions could be solved via multiple anagramming on in-depth messages). As a result, the vast majority of the cryptograms could not be solved directly by traditional means.

We were able to recover partial plaintexts for a handful of the messages, using advanced attacks against regular columnar transposition ciphers (Lasry, Kopal, and Wacker (2016)), despite the fact that a wrong key length was assumed. With a combination of manual and computerized methods, we were able to identify the encryption and key generation mechanisms, allowing us to decrypt all the five-letter ciphers. The Swedish FRA was also able to decipher those messages (Grahn (2019)), which leads to the conclusion that while creating some challenges compared to standard columnar transposition ciphers, the scheme used for the Biafran ciphers was not very secure. The five-figure ciphers were probably more secure, as we were unable to decipher them, and there is no evidence the FRA had any success with those either.

The contents of the deciphered messages shed new light into the relentless but often inefficient efforts by the Biafran authorities to secure diplomatic and financial support, engage international public opinion, and obtain weapons and other supplies.

Acknowledgements

We would like to thank Ed Hannon for his suggestions and Jan-Olof Grahn for his help with names. We are also grateful for the friendly help and advice we received from Heather Heywood, Head of ITU’s Information Management Service. We also thank Emeka (Eugene) Maduewesi for his assistance in identifying names.

This work has been supported by the Swedish Research Council, Grant 2018-06074, DECRYPT – Decryption of historical manuscripts.

Appendix A. A Personal Account of the Interception

The Biafran messages from the Lisbon–Biafra radio teleprinter (RTTY) link were intercepted by Frode Weierud, during the summer of 1969 from his parents’ home in Oslo. The following is a personal account written recently by him.

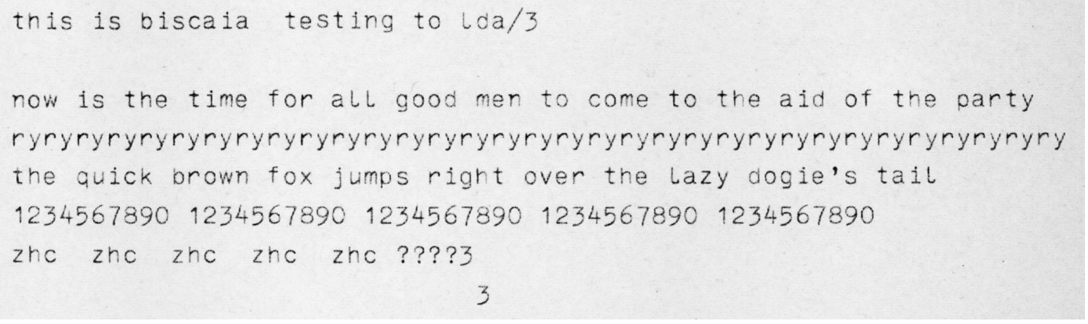
In 1967, shortly after I obtained my radio amateur license, the Norwegian telecommunication authorities, then named Teledirektoratet, decided to sell as surplus some of their older teleprinters that had been used in the national Telex network. The machines were offered at a very cheap price, 50 NOK per piece — equivalent to 7 USD, to the Norwegian radio amateurs, aka radio hams, and at the same time Teledirektoratet issued special permissions for Norwegian radio amateurs to use these machines on the radio amateur frequencies. Being very interested in all kinds of modern telecommunication techniques, I bought two of these page-printing teleprinters, model Siemens T-37, together with a Siemens paper tape reader and a Creed hand punching unit for making 5-level tape in the Baudot-Murray code, today better known as the International Telegraph Alphabet No. 2 (ITA-2).

At this time, I was ending the obligatory one year of practical industrial experience as a trainee in a Norwegian telecommunication company, NERA, before entering the engineering college in Oslo in the autumn. I therefore had both the time and the resources to start building the necessary radio teleprinter terminal equipment to allow the teleprinters to be interfaced to my ham radio receiver and transmitter. I decided to build the Mainline TT/L-2, a frequency shift keying (FSK) demodulator designed by an American radio amateur named Irvin M. Hoff and which was the state-of-the-art RTTY demodulator at the time. Its design was first published in the American RTTY Bulletin in September 1967 and with a subsequent publication in QST, the main publication of the Amateur Radio Relay League (ARRL), in May and June 1969. Special parts were ordered in the USA but to speed things up I also immediately started building a much simpler transistorised version with already available parts. This turned out to be a smart move, because in the end the TT/L-2 unit was not finished before the summer of 1970, well after the end of the Lisbon–Biafra link.

The simplified demodulator was very basic and did not perform very well, but in September 1968 Irvin Hof published yet another Mainline unit, the low-cost solid-state ST-3 with improved performance. I therefore quickly modified my simplified demodulator to reflect the design of the ST-3. Initially I used the new ST-3 demodulator with my main receiver, a commercial shortwave receiver called Hammarlund SP-600 JX-17, which was military surplus coming from the Norwegian army. This was an excellent receiver well suited for this type of application. Transmitting turned out to be a much more difficult task mainly due to the transmitter, which was a rather poor homemade construction and that I had bought from another radio ham. In the end I had to stop using this transmitter due to several complaints from other hams about the signal being both unstable and noisy, and subsisting on a small student loan a new transmitter was out of the question. Not being able to actively communicate from my ham radio station I instead spent my time listening to other radio amateurs, but I also listened to transmissions on frequencies outside the radio amateur bands. There were various press services, weather stations, commercial and government telegraph services and diplomatic and military communications. The diplomatic and military traffic was mainly in cipher or code. Very early on I discovered that all this traffic was generated by cipher machines and therefore impossible to break for a budding amateur cryptanalyst. However, even if the ciphers were unbreakable many of the messages had special characteristics which allowed me to recognise the traffic as originating from the Soviet Union, the Warsaw Pact countries or from the NATO countries. I found traffic analysis just as interesting as codebreaking and I therefore kept a log of all the traffic I intercepted together with a folder with sample message traffic. Sometimes the stations would use CW (Morse code) or just chatting in RTTY on the frequencies when establishing a link and then going into crypto mode. This allowed me to further identify the stations and their origin.

I had almost a year of experience in receiving radio teleprinter transmission when at the end of July 1969, I discovered an RTTY signal that transmitted cipher messages but in an unusual format. The signal was first discovered at a relatively high frequency – 19270 kHz – in the shortwave band. Signals at these high frequencies are usually strongest during daytime but in those days, with a period of solar maximum, the propagation was very good and many of the messages were also received in the late afternoon and the early evening. Unfortunately, the station logbook and some of the messages have been lost or destroyed during the 50 years that have passed since the interception of this traffic. It is therefore difficult to remember exactly when it became evident that this station was communicating with Biafra; however, I think I reached that conclusion at the beginning of August 1969.

The intercepted station called itself Biscaia, a fact that became apparent very quickly because during periods of no traffic it would transmit a test tape saying: "`This is Biscaia testing to LDA/3`" (see Figure A1).



```
this is biscaia  testing to lda/3

now is the time for all good men to come to the aid of the party
ryryryryryryryryryryryryryryryryryryryryryryryryryryryryryryryry
the quick brown fox jumps right over the lazy dogie's tail
1234567890 1234567890 1234567890 1234567890 1234567890
zhc  zhc  zhc  zhc  zhc ????3
                         3
```

Figure A1. Testing message (Source: Frode Weierud)

Initially I believed `LDA/3` was a radio station callsign, even though that would indicate that the station operated illegally due to the fact that `LDA` is in a series of callsigns permanently assigned to Norway. However, only in 2014 did I learn that that `LDA/3` stood for "Luanda 3." Both Luanda 3 and Biscaia, which is the name of Biscay in Portuguese, seem to have been named so as to hide the exact location of the stations and only indicate approximately where they were situated. The names also lead one to believe that this is a Portuguese radio link with stations in Portugal and Angola, which in those days was a Portuguese colony. Personally I believed Biscaia operated from a ship in or close to the Bay of Biscay; however, it is now known that Biscaia operated from a villa in Lisbon and Luanda 3 from various locations inside Biafra.

Radio teleprinter stations usually operate on different frequencies such that they both can transmit at the same time and therefore operate in what is called full duplex. I also tried to locate the `LDA/3` station, but I was not able to receive transmissions from this station in Oslo on my twin dipole antenna for the 14 and 21 MHz radio amateur bands. Another problem was that Biscaia did not always use the same frequency and on several occasions, it was impossible to find it. Sometimes after an extensive search of the most likely frequency bands the station Biscaia could be found again. Altogether it was using at least three different frequencies in August and October 1969, the already mentioned frequency 19270 kHz, as well as 20890 kHz and 23800 kHz. When FRA discovered this traffic in late summer 1967, they first detected the station `LDA/3` at 17320 kHz and a few days later the station Biscaia at 20877 kHz. This frequency is very close to 20890 kHz which might indicate this was one of Biscaia's main frequencies.

Looking back now at the dates when I received these messages it seems that I mainly did the intercepts at the weekends. Towards the end of August, I started the third and final year of my engineering studies and I think this is the main reason why there are no messages from the end of August and September. I simply was too busy to play with my radios. The messages from October 1969 have been received on another teleprinter, a Siemens T-68d strip printer, that I had repaired for the radio amateur club in Oslo and then was testing out before returning it to the club. Due to all these activities I unfortunately did not have the time to maintain a more thorough and continuous interception of the Lisbon–Biafra traffic, something that I regret today.

Many of the messages were repeated one or more times to ensure correct interception by the station Luanda 3 in Biafra. Some of these repetitions were also printed by me; however, to save on the rolls of teleprinter paper that was a scarce resource for a poor student, many of the repetitions were not printed. Also, when a message did not look sufficiently interesting the printing was stopped manually to save paper. This probably means that several messages were lost or missed due to these cost cutting measures.

Another problem was the unstable medium of radio waves that depends on so many factors to achieve good propagation of the signals. Even if the radio propagation in 1969 was relatively good, the signal strength would on some days fluctuate heavily and a complete loss of signal was not unusual. Under those circumstances the teleprinter would lose synchronisation and it would print garbles, or worse, it would suddenly receive a carriage return and overprint an already perfectly received line. Atmospheric disturbances and locally generated noise also made the reception of these signal difficult at times.

Already in August 1969 was I intrigued by the curious block structure of the five-letter cipher messages. A frequency analysis of some of the messages with the minimum of garbles showed that the distribution was similar to that of the English language and that these messages most likely were transposition ciphers. Both then and somewhat later I tried to break these messages by using the methods known to me at that time and which were mainly based on what I had learned from Helen Fouché Gaines' book of 1956. I tried both columnar transposition and some other variants but without achieving a break. Because the messages were divided into blocks, which I already then had noticed were delimited by a count of the groups in a block followed by the day of the month, i.e. 71/4, I tended to believe that different grilles or stencils had been used for the transposition and that a solution therefore would be difficult to achieve.

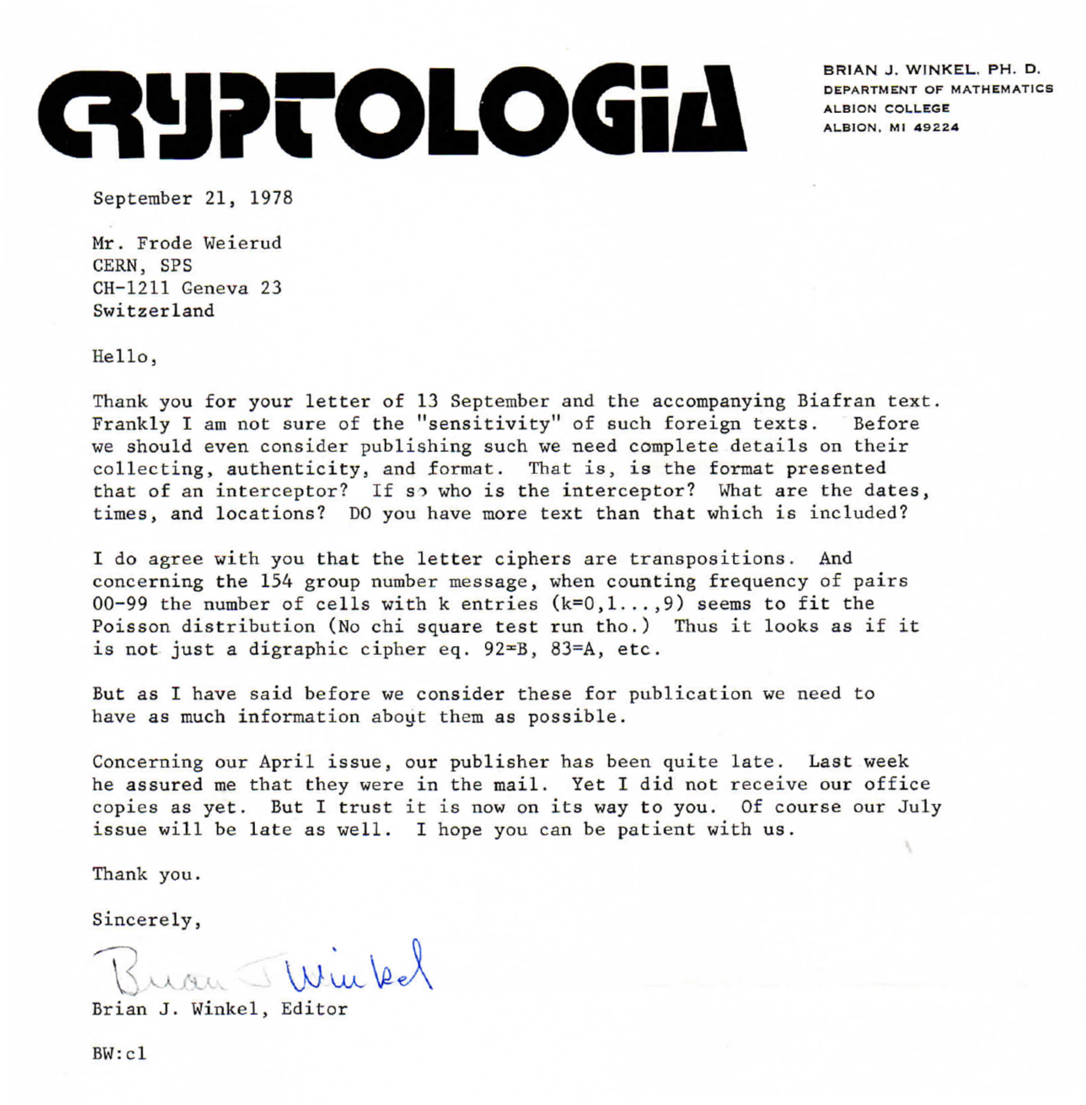
Nothing seems to have been done with the messages before April 1974 when I was employed as an electronics engineer by the European Organization for Nuclear Research (CERN) in Geneva, Switzerland. It is possible that one my colleagues there made me look closer at the messages again. My colleague had previously been employed by the Radio Corporation of America (RCA) and had worked for them in Lagos, Nigeria on the federal government's broadcast transmitters. He gave me several detailed maps of Nigeria and other information about the country and its people. I see from my notes that I then performed more detailed statistical tests on several of the messages. I was especially studying the messages BAL25 and BAL26 from 04 August 1969 because I had spotted the repeated group `BICTR` in both of these messages. Perhaps if I had persisted with my investigations in those days the messages might have been broken already then, 45 years ago.

The next part of the saga took place on 13 September 1978 when I wrote a letter to Dr. Brian J. Winkel who was one of the founding editors of the newly started publication Cryptologia. The first issue of Cryptologia was published in January 1977 and in February 1978 I received a letter from them asking me to publish if I had anything of interest. In my September letter to Dr. Winkel I presented the Biafran ciphers to him and sent him copies of a few of the five-letter and five-figure ciphers. I clearly stated that unfortunately I was very busy professionally at that moment and I would therefore have difficulties in preparing something for publication. However, I hoped that perhaps with his help or somebody else something could be prepared for publication about the Biafran cryptograms. My sales pitch in those days was the following:

"Personally, I find the cryptograms very interesting as they have their origin in a war where the so-called bush-war developed into modern large-scale guerrilla war. The Biafran diplomacy with representatives in most western countries is to my knowledge also a first, and I therefore think it is of interest to study in detail how modern telecommunications and cryptography were used by the Biafrans to communicate with their envoys."

Perhaps I would phrase this slightly differently today; however, in essence it is still what I feel about these messages.

Dr. Winkel replied already a week later on 21 September (see Figure A2). He was clearly interested but with a caveat, as he wrote: "Frankly I am not sure of the "sensitivity" of such foreign texts. Before we should even consider publishing such we need complete details on their collecting, authenticity, and format. That is, is the format presented that of an interceptor? If so, who is the interceptor? What are the dates, times, and locations? Do you have more texts than that which is included?" A great many questions which I tried to the best of my ability to answer in my next letter on 12 October 1978.



CRYPTOLOGIA

BRIAN J. WINKEL, PH. D.
DEPARTMENT OF MATHEMATICS
ALBION COLLEGE
ALBION, MI 49224

September 21, 1978

Mr. Frode Weierud
CERN, SPS
CH-1211 Geneva 23
Switzerland

Hello,

Thank you for your letter of 13 September and the accompanying Biafran text. Frankly I am not sure of the "sensitivity" of such foreign texts. Before we should even consider publishing such we need complete details on their collecting, authenticity, and format. That is, is the format presented that of an interceptor? If so who is the interceptor? What are the dates, times, and locations? DO you have more text than that which is included?

I do agree with you that the letter ciphers are transpositions. And concerning the 154 group number message, when counting frequency of pairs 00-99 the number of cells with k entries (k=0,1...,9) seems to fit the Poisson distribution (No chi square test run tho.) Thus it looks as if it is not just a digraphic cipher eq. 92=B, 83=A, etc.

But as I have said before we consider these for publication we need to have as much information about them as possible.

Concerning our April issue, our publisher has been quite late. Last week he assured me that they were in the mail. Yet I did not receive our office copies as yet. But I trust it is now on its way to you. Of course our July issue will be late as well. I hope you can be patient with us.

Thank you.

Sincerely,

Brian J Winkel

Brian J. Winkel, Editor

BW:cl

Figure A2. Dr. Winkel's letter from September 21, 1978 (Source: Frode Weierud)

There I explained in detail how I had intercepted the messages at my ham radio station in Oslo and that also I was unsure about the sensitivity of the messages and their publication so soon after their interception. I expressed that the message should not be published in their present form and that we should know the content of the messages to be sure that we did not publish any sensitive material. I added that personally I was not so much interested in publishing the messages as I was in seeing published a study of the crypto systems and the methods of communication.

And there the matter rested. In May 1979 Dr. Winkel briefly mentioned the Biafran ciphers again in a correspondence about other unrelated subjects. He wrote: "I have gotten nothing on the Biafran ciphers I am afraid to say and of course we could not say very much about them even if we did, could we?"

And for the next 40 years the Biafran ciphers rested at the bottom of my filing cabinets and their existence has been unknown until now. Dr. Brian J. Winkel and my CERN colleague are to my knowledge the only two people I ever told about these ciphers. It is therefore with some pleasure and relief I see that they now are published and solved and that they finally receive their somewhat modest place in the annals of cryptologic history.

Appendix B. Channel Indicators

Channel indicators, as defined by the the International Telegraph and Telephone Consultative Committee (CCITT) Recommendation F.31 "Telegram Retransmission System" are a way of identifying telegrams sent over a telecommunication network from the beginning to the end. An extract from the International Telecommunication Union (ITU) Blue Book describing the Recommendation can be found in ITU (1988).

Paragraph 2.1.2 of Recommendation F.31, from the 1964 CCITT Blue Book (1964) defines the indicators in the following way:

2.1.2 Channel sequence number

Messages transmitted over a channel should be numbered according to a series of numbers for each channel. The channel sequence number will therefore be composed of a characteristic of the channel used (channel indicator) followed by a number showing the order of this message in the series of messages sent over this channel. A channel sequence number is composed of:

- *a space signal,*
- *three letters constituting the indicator of the channel,*
- *a "figures-shift" signal,*
- *three figures constituting the number in the series on the channel,*
- *a "letters-shift" signal.*

Service advices, including XQ, BQ, RQ, will be numbered like the messages unless agreed otherwise, by the Administrations concerned.

If several channels are used in tandem in a message relay system, the channel sequence number for each preceding channel is transmitted over the following channel; the new channel sequence number for the following channel will precede the channel sequence number for each preceding channel; the channel sequence numbers will therefore be in the opposite order to their order of transmission. The channel sequence numbers will be produced and examined automatically; the channel sequence numbers will be in sequence from 001 to 999 and change automatically from 999 to 001 at the end of a numbering cycle.

The following example shows the use of channel indicators for a telegram sent from London to Sydney in Australia:

```
ZCZC AOE262 LDB814 PLD606
AASD CO GBLD 018
LONDON / LD 18/16 22 1430

LX
HARRIS
2462 SOUTHERNHIGHWAY
SYDNEY

CONGRATULATIONS ON YOUR PROMOTION AND
BEST WISHES FOR THE FUTURE
           JOHN
```

```
NNNN
```

Here `ZCZC` is the start-of-message signal (SOM) and `NNNN` is the end-of-message signal (EOM); both are standard for all telegram transmissions and LX is the standard code for the deluxe form of the telegram. The first line of the header, also called the pilot line, starts with the SOM followed by the channel indicators, which here are `AOE262`, `LDB814`, and `PLD606`. We will return to channel indicators below. The second line starts with the destination indicator, `AASD` which is the official code of Australia (AA) and Sydney (SD), followed by a two-letter code, here CO, which indicates that the telegram is sent over a government service (C) and that it is an ordinary private telegram (O). The line ends with the origin indicator, `GBLD` which is the code for Great Britain (GB) and London (LD), and a three-digit number that shows the number of chargeable words. The third line, also called the preamble line, starts with the official name of the office of origin, `LONDON / LD`, followed by the number of chargeable and actual words, 18 / 16. The preamble line ends with the date and time of handing in the telegram, given by two numbers, the first indicating the day of the month and the second the time in 24-hour format.

The Biafran radio telex link did not follow the ITU recommendations, because it was not an official and international service but rather a private semi-governmental circuit. In a sense it was an illicit service using radio frequencies and callsigns unlisted in the ITU Master International Frequency Register; however, the telegram headers have some of the elements recommended by the ITU. The standard header of the Biscaia station have the following format:

```
ZCZC BAL30/4/8 BISCAIA - 04 1906
```

It starts with the SOM followed with the channel indicator, `BAL30`; however, unlike the ITU recommendations it is followed with the day of the month and month of the year, which means that taken together the telegram is uniquely identified within a given year. This is then followed by the full name of the originating station, Biscaia, which often would be abbreviated to just `BIS`, and then finally the day of the month and the time in 24-hour format. The number of cipher groups or words in the telegram is not indicated.

The Lisbon station, Biscaia, was the central telecommunication centre for the Biafran foreign communications. Biafran missions and offices in other countries in Europe and overseas would connect to the Lisbon station by the official telex service of the different countries. Sometimes the header of the original telex message arriving at the Lisbon office would be copied and transmitted with a `BAL` channel indicator as shown below.

```
ZCZC BAL50/21/10 BIS - 21 1441
UK
LDNTLX.14 48 7

FOR O FROM K REPEATED CHIJI
MIRHT TGEDF TWITW ICAER DOGCO LLDDK IOUUO TESNB YORDR AOEAR
---RL TEPAT RFHEI IERSO VERTD BOION EBOKS NAESP VRBMF CREOL
20/21 NMISO ERIZV JOITU ORTED YRSWO GIODS ETTSC OCNFH NBAPE
RLPOO TNTTO JEEIC NWNRE HCDAS IUOAT HSTWN SZEFA UMHTH SOEON
OOLEN 40/21
COLL 20/21 40/21
```

Here we can see the originating country, UK, together with the origin indicator LDNTLX.14, which indicates that the Biafran London office did not have their own telex machine but instead used the official London Telex Office, part of the international Gentex service, for their messages. If they had had their own private telex connection, then the origin indicator would have been the three letters TLX together with their telex number, e.g. TLX200745. The number following the origin indicator is the number of chargeable words, here 48, and the final number, 7, is the original date when the message was delivered to the London Telex Office. Either this number is wrong due to a transmission error or the message has for some reason been delayed at the Lisbon office. The plaintext of this message refers to a transfer of funds that will take place on the 21th October, on the day the message was transmitted to Biafra.

The message above has also an external routing address, which in this case is: FOR O FROM K REPEATED CHIJI. This is understandable as it allows the ciphertext to be routed to the final recipients before being deciphered; however, the way it has been implemented leaves a horrendous security hole. The problem is that the external routing address is almost the same and, in some cases, identical to the internal routing address. It means the external address is almost a perfect crib or probable word that can be used to break the cipher. In this case the internal routing address is: FOR O FROM KOGBARA REPEATED CHIJI. The start of the internal address is also relatively easy to determine as all the telegrams start with: SECRET followed by an internal channel indicator that would be three letters followed by three numbers spelled out; in the case above it was LNB ONE ONE ZERO. The only unknown factor here is the offset created by the spelled-out numbers. This offset will in most cases vary from 9 to 15; however, the Biafrans did not follow the ITU rules of always using a three-digit number here. They would use both single- and double-digit numbers, which of course will modify the offset accordingly. Knowing that the transposition width or number of columns gravitates around twenty only a relatively small number of trials is necessary to find the correct placement and hence the correct order of the columns. This is yet another example of how important it is to train the users in the correct usage of a given crypto system.

The Biafran station, Luanda, will also have used a channel indicator for their messages to the Biscaia station. What this indicator is we do not know for sure, but one message, BAL227, from 3 August 1969 refers to "your LAB193." It therefore seems that Luanda simply used BAL in reverse, LAB, as a channel indicator, which again seems to indicate that BAL stands for "Biscaia to Luanda." Channel indicators are an entity that is not officially listed by ITU and therefore they are not globally known. Each telegraph station makes up its own channel indicators and allocates them to the available telegraph channels. The stations operating in a given network will probably over time get to know the various channel indicators of their correspondents; however, they have no need to know anything specific about the indicators. If they want to question something about a given message, they will simply contact the station they received the message from and quote all of the channel indicators. This station will, if it is the originator of the message, be able to resolve the question; however, if it is a retransmitted message, they will again contact the station they received the message from and so on.

The BAL and LAB channel indicators were used in a similar way on the Biafran radio telex link. The indicators allowed the two stations to acknowledge the reception of the messages and also to ask for the retransmission of corrupted messages. However, one interesting thing is that internally, in the hidden plaintext, there is also a channel indicator. These channel indicators were made up by the various Biafran missions or offices that corresponded with each other and with Biafra in a similar way to the indicators used by the international telegraph offices. Like the official channel indicators, the Biafran indicators are made up of three letters and a number going from 1 to 999. The three letters are in most cases an abbreviation of the city or country where the Biafran mission or office was placed such as `FRA` for Frankfurt, `LDB` for London and `PAR` for Paris. The exception to this rule is the indicators used by the offices in Lisbon and the home office or government in Biafra. Lisbon housed several Biafran missions and offices and it appears that for this reason the message traffic was divided into at least two channels, one with the indicator `LNB` for the more general traffic and another `LSO`, that was used for communications about weapon procurements and transport to Biafra. The Biafran government used the channel indicators `FAF` and `FAH` in August and October 1969. Because the traffic over these two channels appear to be similar, we suppose that they are not different message channels but the same channel that use an incremental type of indicator. Originally it may have started as `FAA` and when reaching `FAA999` it would increment to `FAB001`. For the Biafran government office, which would have communications of long-term importance, such an incremental system with unique channel indicators has many advantages.

However, the system with internal channel indicators appears to have been introduced only in 1969 or in the second part of 1968. Unfortunately, we only have three messages from Spring 1968, so we are on thin ice drawing conclusions; however, it appears that then the overseas offices did not use proper channel indicators, but only a message number linked with the originator of the message. The Biafran home office on the other hand used a proper channel indicator of the form `MFAxxx`. If the Biafran foreign communications were handled by their Foreign Office, it is possible that `MFA` stands for Ministry of Foreign Affairs. When it later was decided to move to an incremental system of indicators it is possible that MFA simply was shortened for FA, Foreign Affairs.

Table B1 shows all the internal channel indicators that appear in the messages we have deciphered. One indicator is different, `MAR603`; however, we believe that this is an error for `PAR603`. The reason is that it fits nicely in the sequence after the indicators `PAR601` and `PAR602` and it has also been sent by Chijioke I. Dike, Biafra's special representative in Paris.

Channel	Indicator	From	City / Country	Subject
DAR	663	Austine	Dar es Salaam / Tanzania	UN politics
DAR	672	Austine	Dar es Salaam / Tanzania	OAU Conference
DAR	670	Austine	Dar es Salaam / Tanzania	Congo politics
FAF	71	Ojukwu	Biafra	OAU Conference
FAF	351	Ojukwu	Biafra	UN politics
FAF	459	Ojukwu	Biafra	Finance / Esta code
FAF	467	Ojukwu	Biafra	Expenses
FAF	505	Ugwumba	Biafra	Payment Mr. Chabert
FAF	508	Ojukwu	Biafra	About Mr. Chabert
FAF	566	Ojukwu	Biafra	Travel S-America
FAF	692	Ojukwu	Biafra	Congo politics
FAH	210	Ojukwu	Biafra	Finances / Chiji
FAH	280	N.U. Akpan	Biafra	Concerning Eronini
FRA	313	Dr. Obonna	Frankfurt / Germany	Expenses
FRA	314	Dr. Obonna	Frankfurt / Germany	Rome office politics
FRA	330	Dr. Obonna	Frankfurt / Germany	Commercial
FRA	331	Dr. Obonna	Frankfurt / Germany	Travel German TV crew
GAB	832	HY	Libreville / Gabon	Travel arrangements
GAB	833	HY	Libreville / Gabon	Uli transport
GAB	834	HY	Libreville / Gabon	Travel arrangements
LDB	97	Kogbara	London / UK	Office politics
LDB	98	Kogbara	London / UK	Concerning Mr. Eronini
LDB	108	Kogbara	London / UK	Air transport to Uli
LDB	110	Kogbara	London / UK	Payment to Chiji
LNB	762	Chris	Lisbon / Portugal	Finance / Esta code
LNB	788	CC	Lisbon / Portugal	Personal comm.
LNB	789	CC	Lisbon / Portugal	Office travel
LNB	790	CC	Lisbon / Portugal	Group travel
LNB	791	CC	Lisbon / Portugal	Notification
LNB	792	Chris	Lisbon / Portugal	Travel arrangements
LNB	793	Chris	Lisbon / Portugal	Travel South-America
LSO	289	Chris	Lisbon / Portugal	Uli transport
LSO	292	Onubogu	Lisbon / Portugal	Weapon/Parcel transport
LSO	293	Onubogu	Lisbon / Portugal	Transport notice
LSO	294	Chris	Lisbon / Portugal	Office politics
LSO	295	Emodi	Lisbon / Portugal	Uli transport
LSO	296	Chris	Lisbon / Portugal	Uli transport
LSO	297	–	Lisbon / Portugal	Uli transport
PAR	599	CC	Paris / France	Payment Mr. Chabert
PAR	601	Chiji	Paris / France	Concerning Mr. Chabert
PAR	602	Arthur	Paris / France	Uli transport
PAR	853	Chiji	Paris / France	French media
MAR	603	Chiji	Paris ?	Red Cross
MFA	37	Hamilton	Biafra (Spring 1968)	Question
MFA	143	HE	Biafra (Spring 1968)	Weapons

Table B1. List of internal channel indicators used in the Biafran messages.

References

Ângelo, Fernando Cavaleiro. 2019. *Os Falcões do Biafra.* Leya, Lisbon.

Bat, Jean-Pierre. 2018. "Les réseaux Foccart." *L'homme des affaires secrètes (Nouveau monde éditions, Paris)* .

Bauer, Friedrich Ludwig. 2002. *Decrypted secrets: methods and maxims of cryptology.* Springer-Verlag, Berlin. https://doi.org/10.1007/978-3-540-48121-8.

CCITT. 1964. *Telegraph Operation and Tariffs.* International Telegraph and Telephone Consultative Committee, Geneva. http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.254.43.en.1002.pdf.

Chen, Jian, and Jeffrey S Rosenthal. 2012. "Decrypting classical cipher text using Markov Chain Monte Carlo." *Statistics and Computing* 22 (2): 397–413.

Clark, Andrew J. 1998. "Optimisation heuristics for cryptology." PhD diss., Queensland University of Technology. https://eprints.qut.edu.au/15777/.

de St Jorre, John. 1972. *The Nigerian civil war.* Hodder and Stoughton, London.

Debré, François. 1968. *Biafra, an II.* Julliard, Paris.

Dimovski, A, and D Gligoroski. 2003. "Attacks on the transposition ciphers using optimization heuristics." *Proceedings of ICEST* 1–4.

Draper, Michael I. 1999. *Shadows: airlift and airwar in Biafra and Nigeria 1967-1970.* Hikoki Publications, Crowborough, UK.

Express. 1968. "Biafra - The End." *The Express* https://newsbeezer.com/morroco/the-express-of-october-7-1968-biafra-the-end/.

Freire, João Sérgio Gilzans d'Oliveira. 2017. "Portugal na guerra do Biafra. A diplomacia do Estado Novo em África: 1967-1969." PhD diss., Universidade Autónoma de Lisboa. http://repositorio.ual.pt/handle/11144/3409.

Friedman, William F. 1941. *Military Cryptanalysis, Part IV, Transposition and Fractionating Systems.* United States Government Printing Office. https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/military-cryptanalysis/mil_crypt_IV.pdf.

Gaines, Helen Fouché. 1956. *Cryptanalysis: A Study of Ciphers and Their Solution.* Dover, New York. https://archive.org/details/cryptanalysis00hele.

Getty Images. 1969. "Picture of Michael Ugboma in Rome." https://www.gettyimages.com/detail/news-photo/michael-ugboma-representative-of-the-secessionists-of-news-photo/141555916.

Giddy, JP, and Reihaneh Safavi-Naini. 1994. "Automated cryptanalysis of transposition ciphers." *The Computer Journal* 37 (5): 429–436.

Grahn, Jan-Olof. 2019. *Om svensk signalspaning : Kalla kriget (English: "On Swedish signal intelligence: The Cold War").* Medströms Bokförlag, Stockholm.

Griffin, Christopher. 2015. "French military policy in the Nigerian Civil War, 1967–1970." *Small Wars & Insurgencies* 26 (1): 114–135. https://doi.org/10.1080/09592318.2014.959766.

Hansard. 1968. "Hansard, 29 January 1968." Quote from Frank Beswick, https://hansard.parliament.uk/Lords/1968-01-29/debates/72c099ae-b576-4f4f-b099-3400077eeb69/Estacode.

Heerten, Lasse. 2017. *The Biafran War and postcolonial humanitarianism: spectacles of suffering.* Cambridge University Press, Cambridge, UK. https://doi.org/10.1017/9781316282243.

Ikejiani, Okechukwu. 2007. *The Unrepentant Nationalist.* Snaap Press, Enugu.

Iroh, Eddie. 1976. *Forty-eight Guns for the General.* Vol. 189 of *African Writers Series.* Heinemann, London.

Iroh, Eddie. 1979. *Toads of war.* Vol. 213 of *African Writers Series.* Heinemann, London.

ITU. 1988. "Telegram Retransmission System, ITU-T Recommendation F.31. Extract from the Blue Book." https://www.itu.int/rec/T-REC-F.31-198811-I/en.

Jeffs, Nikolai. 2012. "Ethnic "betrayal", mimicry, and reinvention: the representation of Ukpabi

Asika in the novel of the Nigerian-Biafran war." *Revue LISA/LISA e-journal. Littératures, Histoire des Idées, Images, Sociétés du Monde Anglophone–Literature, History of Ideas, Images and Societies of the English-speaking World* 10 (1): 280–306. https://doi.org/10.4000/lisa.5051.

Kahn, David. 1967. *The codebreakers. The story of secret writing.* New York: Macmillan Co.

Kirk-Greene, Anthony Hamilton Millard. 1971. *Crisis and conflict in Nigeria: a documentary sourcebook.* Vol. 2. Oxford University Press, Oxford, UK.

Kriebel, Norman. 1968a. "Clark/Goodnow from Kriebel/Seely WA 918." Foreign Broadcast Information Service, https://www.cia.gov/library/readingroom/docs/CIA-RDP81-00770R000100100017-1.pdf.

Kriebel, Norman. 1968b. "Clark/Scheuer from Kriebel/Seely WA 751." Foreign Broadcast Information Service, https://www.cia.gov/library/readingroom/docs/CIA-RDP81-00770R000100100030-6.pdf.

Kriebel, Norman. 1968c. "Clark/Scheuer from Kriebel/Seely WA 923." Foreign Broadcast Information Service, https://www.cia.gov/library/readingroom/docs/CIA-RDP81-00770R000100100018-0.pdf.

Lasry, George. 2018. "A methodology for the cryptanalysis of classical ciphers with search metaheuristics." PhD diss., Kassel University. https://doi.org/10.19211/KUP9783737604598.

Lasry, George, Nils Kopal, and Arno Wacker. 2014. "Solving the double transposition challenge with a divide-and-conquer approach." *Cryptologia* 38 (3): 197–214. https://doi.org/10.1080/01611194.2014.915269.

Lasry, George, Nils Kopal, and Arno Wacker. 2016. "Cryptanalysis of columnar transposition cipher with long keys." *Cryptologia* 40 (4): 374–398. https://doi.org/10.1080/01611194.2015.1087074.

Lasry, George, Ingo Niebel, Nils Kopal, and Arno Wacker. 2017. "Deciphering ADFGVX messages from the Eastern Front of World War I." *Cryptologia* 41 (2): 101–136. https://doi.org/10.1080/01611194.2016.1169461.

Marks, Leo. 2012. *Between Silk and Cyanide.* The History Press, Cheltenham.

Matthews, Robert AJ. 1993. "The use of genetic algorithms in cryptanalysis." *Cryptologia* 17 (2): 187–201. https://doi.org/10.1080/0161-119391867863.

Mbanefo, Arthur. 2015. *A Fulfilled Life of Service.* Bookcraft, Ibidan. https://www.sunnewsonline.com/excerpts-from-mbanefo-a-fulfilled-life-of-service-2/.

Mezu, Sebastian Okechukwu. 1972. *Behind the rising sun.* Vol. 113 of *African Writers Series.* Heinemann, London.

Miersemann. 1944. "CSDIC (UK) S.I.R. 1106 'German wireless intercept and counterespionage activities'." *National Security Agency Record Group 457 Historic Cryptographic Collection* http://chris-intel-corner.blogspot.com/2013/10/soe-cryptosystems-german-view.html.

Onwumechili, Cyril. 2000. "Igbo Enew Eze: The Igbo Have No Kings." http://ahiajoku.igbonet.com/2000/.

Onyegbula, Godwin A. 2005. *The memoirs of the Nigerian-Biafran bureaucrat: An account of life in Biafra and within Nigeria.* Spectrum, Ibadan.

Russell, Matthew D, John A Clark, and Susan Stepney. 2003. "Making the most of two heuristics: Breaking transposition ciphers with ants." In *Evolutionary Computation, 2003. CEC'03. The 2003 Congress on*, Vol. 4, 2653–2658. IEEE. https://doi.org/10.1109/CEC.2003.1299423.

Sinkov, Abraham. 1968. *Elementary Cryptanalysis.* Random House, The L. W. Singer Company, New York.

Special Libraries Association. 1971. "Special Libraries, January 1971." *Special Libraries* https://scholarworks.sjsu.edu/sla_sl_1971/1/.

State Department. 1970. "Foreign Relations, 1969-1976, Volume E-5, Documents on Africa, 1969-1972." https://2001-2009.state.gov/r/pa/ho/frus/nixon/e5/55059.htm.

Stremlau, John J. 2015. *The international politics of the Nigerian civil war, 1967-1970.* Princeton University Press, Princeton. https://doi.org/10.1515/9781400871285.

Time Magazine. 1970. “The secession that failed.” *Time Magazine* 19–24. 26 January 1970, http://content.time.com/time/magazine/article/0,9171,878714,00.html.

Udekwu, Fabian. 2011. “The Civil War.” http://unknown-africanromancewriters.blogspot.com/2011/08/civil-war-apart-from-operating-daily-i.html.

Venter, Al J. 2016. *Biafra’s War 1967-1970: A Tribal Conflict in Nigeria That Left a Million Dead*. Helion and Company Ltd, Solihull, UK.

Weierud, Frode. 2019. “The Biafran Ciphers.” https://cryptocellar.org/Biafra/.

Winnipeg Free Press. 1970. “Biafra’s publicist winds up work.” *Winnipeg Free Press* 31 January 1970, https://newspaperarchive.com/ca/manitoba/winnipeg/winnipeg-free-press/1970/01-31/page-4/.