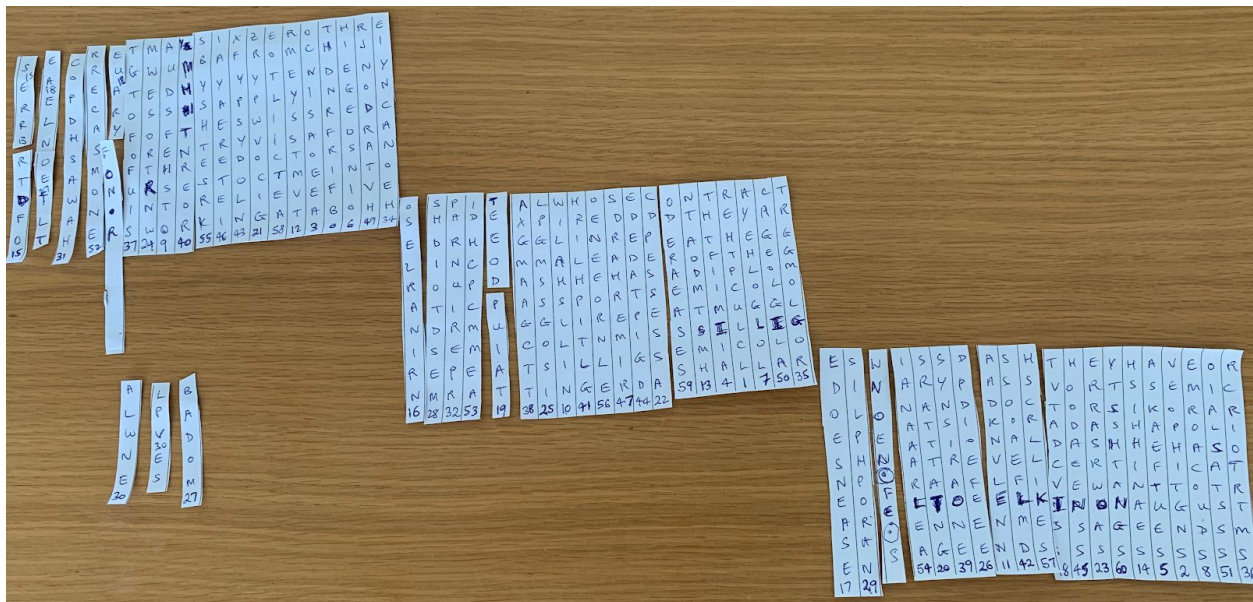


Solving Ciphers from the Biafran War

The ciphers published by Frode Weierud in <https://cryptocellar.org/Biafra> have been solved by a team composed of Richard Bean, Frode Weierud, and George Lasry. Here are the steps of the decipherment:

1. The messages had already been identified as some type of transposition cipher, as the letter frequencies match the frequencies expected in an English text. But it was not clear what type of transposition was employed.
2. The messages were transcribed using Google Docs OCR and manually corrected.
3. On November 24, two short messages were deciphered, assuming a regular columnar transposition cipher, with a complete rectangle of 22 columns and five rows. It turned out that two of the columns could be discarded.
4. Trying the same process failed for other messages, despite the use of advanced algorithms that otherwise are able to solve columnar transposition ciphers with long keys.
5. Various attempts were made for anagramming multiple messages from the same day and using the same key, without any results.
6. No progress was made until December 12, when it was found that when assuming a column height of 10, some word fragments could be seen, such as visa, certificate, message, in one of the messages.
7. Assuming similarly long keys, more fragments could be found in five other messages. Using a pen, paper, and scissors, the team was able to reconstruct the full text for those messages. An example is given here. Two sets of five letters were left unused (NLSMR, WEDKS - those might be dummies or some indicator), and some adjustments had to be made manually to correct the computer solution.



8. The same process could not be successfully applied to any of the other messages. So the team analyzed the various pen-paper-scissors results, to try and establish some

pattern. It was observed that there was a similarity in the reordering of the columns of the two or three parts of each cryptogram. An assumption was made about how the cryptograms may have been created:

- a. Write some plaintext in a transposition rectangle, of width 20 or 21.
 - b. Apply a standard columnar transposition, and obtain an interim ciphertext. Split the ciphertext into two blocks.
 - c. The twist: Take the first 30 letters of the ciphertext, and move them to the end of the first block.
 - d. Insert an indicator at a distance of five from the end of the first block, and another one at a distance of 25.
 - e. Transmit the modified ciphertext.
9. Based on this assumption, the team was able to decipher most of the cryptograms. For those, the key length was either 20 or 21, and the transposition rectangle was complete. An example, BAL151(b):

Key: 8,0,15,20,10,9,6,4,1,14,16,2,13,12,17,18,11,5,19,3,7,
PARTTWOBEGINSOFTWOUNN
AMEDGERMANFILMCOMPANI
ESSSSTHEYALSOCLAIMTHE
INTERESTOFAMERICANAND
FRENCHTTTTVVVSTATIONSS
SSBOTHGENTLEMENAREKNO
WNSUPPORTERSANDFRIEND
SOFBIAFRAAAWHILETHER
EISNOLOCALOBJECTIONTO
THEIRVISITCOMMABUTINT
HEIGHTOFTHEINSPECTOR
GENERALOFFPOLICELETTER
REFERENCESSONEZEROTW
OSTROKEONESEVENNINEON
EOFONESIXAUGUSTONENIN
ESIXEIGHTCOMMAYOUCONS
IDERTNEIRVISITNOWOPPO
RTUNEDANDINTHEINTERES
TOFDALFONPLEASECONVEY
APPROVALEARLIESTTTTTT

10. The same key lengths were tested for the remaining cryptograms, which turned out to be incomplete columnar transpositions. An example, BAL30:

Key: 6,0,10,16,7,11,9,2,12,17,14,13,8,18,3,5,15,1,4,19,
SECRET PAR FIVE NINENIN
E FOR UG WUMBA FROM CC PAR
ARE F YOUR MESSAGE FAFFI
VE ZERO FIVE EEECKECKED
WITH DIKE AND AMOUNT INV
OLVED IS ONE FOUR ZERO ZE
RO ZERO REPEAT FOURTEEN
THOUSAND DOLLAR NOT RE
PEAT NOT FOURTEEN HUNDR
EDDDD THIS IS QUIUE CONS
IDERABLE FOR MY PUCKETT
TTE ILL ADVISE THFT MATT
ER BETAKEN UP WITH MTAGBO
WHO WILL BE HOME SLONSOT
HAT HE CAN PICK UP THE BCL
LLLLL

11. We were able to reconstruct the indicator system. There is a base key, consisting of 15 or 16 letters, valid for a certain period, and a message key, used only for the specific message. The message key consists of five random letters, sent as part of the cryptogram. This message key is appended to the base key, to create a keyword from which a transposition key is built. This system explains why anagramming on multiple cryptograms failed, as the keys for different cryptograms are similar but not identical.
12. We are in the process of analyzing the contents of the messages, which include codewords, and topics like travel arrangements, shipments of material including weapons, and logistics for foreign aid staff. We plan to publish the full results of the research in a joint paper.