Further Note on Holmes Hypothesis

C.H.O'D. Alexander

Editor's Preface

This document is one of seven papers in a series of documents written by the late Conel Hugh O'Donel Alexander while he worked as a cryptanalyst at Bletchley Park during the Second World War. The documents have been obtained from the US National Archives and permission has been obtained from the Controller of Her Majesty's Stationary Office to publish the papers on the editor's personal Web Page. The documents have been faithfully retyped by the editor with help from Ralph Erskine. The original documents were typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the documents have been both left and right justified and a more modern type font has been used. Apart from these modifications to the layout the documents have the appearance of the original.

Where there are obvious typing errors these have been corrected in square brackets. There is one exception to this rule and that concerns the German word 'stecker'. The editor has decided to adopt the German spelling of the word Stecker with a capital, however, the constructed verb 'steckered' has been left in its original form.

The Editor,

Frode Weierud, © August 1998

Source:

Addendum to Captain Walter J. Fried's report No. 24 of 20 April 1944. National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 880, Nr. 2612.

COPYRIGHT

Further Note on Holmes Hypothesis

1. The Holmes alphabet differs from a normal alphabet only in having the pairings BJ, OX (say) replaced by BO, JX, and could be reduced to a normal alphabet by exchanging B or O with one of the 24 other letters, which letter is correct being unknown. (see Appendix 1 to the original paper on Holmes hypothesis: the normal alphabet in question would be one arising from a wheel with cross-wirings B to O and O to B instead of a fixed BO pairing). This paper deals with the modifications such an alteration produces in box shapes and some deductions that can be made from that.

2. Box together two Holmes alphabets, e.g., D1 and D2[1] which give

(ALXIZEVS…FRCMQTYHP…WGDNJUK) (BO).

Imagine that the change needed to reduce these to normal alphabets is to replace PW and BO by PO and BW in D1 and FS and BO by FO and BS. This splits the original box at the places shown by the dotted lines and we get

ALXIZEVSB-OFRCMQTYHPO-BWGDNJUKA

which joins up as (BWGDNJUKALXIZEVS) and (OFRCMQTYHP). If instead of FO and BS we had taken FB and OS we should have got

ALXIZEVSO-BFRCMQTYHPO-BWGDNJUKA

which rejoins as one big box (ALXIZEVSOPHYTQMCRFBWGDNJUK).

It is easy to see also that we can "insert" the BO's in such a way as to join together two compartments if the original box shape contained more than one compartment, e.g., (A LNJ) and (DGTQ EZ) becomes AB-OLNJA and DGTQO-BEZD giving

(ABEZDGTQLNJ)

Finally if one of the Holmes alphabets has no circumference strip pairing, i.e., is a normal alphabet already the alternation in the box is simply to insert BO or OB somewhere in it.

3. The transformation from Holmes alphabets into normal alphabets can therefore only alter the box shapes in one of three ways (1) Enlarge one of the original compartments by 2 (2) split a compartment of size 2 into any two compartments of size 2a and 2b such that a + b = n + 1. We can only have a or b = 1 by leaving the original alphabet unaltered. (3) Join any two compartments of sizes 2a and 2b into a single compartment of size 2(a + b + 1). In no case can the number of compartments (excluding BO) in the box formed by the Holmes compartments be increased or decreased by more than one.

4. It follows at once that the D's have not been equally spaced out. For D1,D2 boxes as a 24 and D3,D4 as 10-6-6-2, and these cannot be made the same by transforming the Holmes alphabets into normal alphabets. The distance between D1 and D2 is different from the distance between D3 and D4.

[1] D1 = AL, CM, DG, EZ, FR, HY, IX, JN, KU, PW, QT, SV, BO.
D2 = AK, CR, DN, EV, FS, GW, HP, IZ, JU, LX, MQ, TY, BO.

5. To apply an exhaustive test of the Holmes hypothesis would now be theoretically possible, but far too laborious to be a practical proposition. The method would be to consider all the possible box[es] that could arise from modifying the Holmes alphabets and test pairs of those that agreed on the theory that they correspond to a repeated distance. This is the analogous method to that used for testing after adding up in the normal use of a fixed Umkehrwalze and moveable fourth wheel.

6. A list of possible box shapes got by modifying the Holmes alphabets is appended.

List of possible box shapes got by modifying Holmes alphabets.

Actual Box Shape.	Possible Box Shapes from Modified Alphabets.				
24	26	26-a/a			
22/2	26	24/2	24-a/a/2		
20/2/2	24/2	20/6	22/2/2	20/4/2	22-a/a/2/2
20/4	26	22/4	20/6	22-a/a/4	20/b-a/a
18/6	26	20/6	18/8	20-a/a/6	18/8-a/a
16/8	26	18/8	16/10	18-a/a/8	16/10-a/a
12/12	26	14/12	14-a/a/12		
12/8/4	22/4	18/8	14/12	14-a/a/8/4	12/10-a/a/4
					12/8/6-a/a
12/6/6	20/6	14/12	14-a/a/6/6	12/8-a/a/6	
10/6/6/2	18/6/2	14/6/6	14/10/2	10/10/6	12/6/6/2
				10/8/6/2	10/6/6/4
	12-a/a/6/6/2		10/8-a/a/6/2		
10/6/4/4	18/4/4	16/6/4	12/10/4	10/10/6	12/6/4/4
	10/8/4/4	10/6/6/4	12-a/a/6/4/4	10/8-a/a/4/4	
	10/6/6-a/a/4				

Editor's Notes

1. The document is not dated but it is known to have been written in the period 14 - 20 April 1944.
2. For an explanation of boxes and boxing, the forming of chains, see the article by David H. Hamer, Geoff Sullivan and Frode Weierud, "Enigma Variations: An Extended Family of Machines," *Cryptologia*, 22(3), July 1998, pp. 211-229.