

Method for Testing “Holmes Hypothesis” for U.D.

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 Stationery 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

Crown copyright is reproduced with the permission of the Controller of Her Majesty's Stationery Office.

Method for Testing “Holmes Hypothesis” for U.D.

1. The Holmes hypothesis I take as implying the following:–

(i) That U.D. is made up of two components – a fixed plugwheel and a rotatable Umkehrwalze.

(ii) That there is a fixed pairing, BO, and two types of other pairings. An example of the first type (normal) would be from A on right hand side of the plugwheel to J on the left hand side, J paired to U through the Umkehrwalze and U paired to K back through the plugwheel, giving an AK pairing through the complete U.D. An example of the second type (circumference strip) would be from E on right hand side of the plugwheel to Q on the left hand side, Q paired to B and thence via O to S (see Holmes’ diagram) through Umkehrwalze and S paired to L back through the wheel, giving an EL pairing through the complete U.D.

2. Now suppose amongst the various wirings of U.D. (9 at present) we have two corresponding to positions 13 apart of the rotatable component (Babbage pointed out to me how alphabet 13 apart would give the quickest way of finding the wiring of a normal type new wheel, given sufficient alphabets, which suggested that a similar attack in this case might be feasible). (i) Suppose AC is a normal pairing at the first of these positions, and HQ a pairing at the second position. Then, if A is thirteen ahead of H on the upright of the rod square, it follows that C must be thirteen ahead of Q. For suppose A is wired through the plugwheel to J and that J and R are paired through the rotatable component and R wired back to C, giving AC. Then, when [the] rotatable section has gone round 13 places, the JR connection will have become WE: when the current goes in at H it comes through plugwheel to W (since A is 13 ahead of H on rod square upright) and therefore will come back to E and then through plugwheel to Q (HQ being paired), therefore C must be 13 ahead of Q. We can write this $AH_{13} \rightarrow CQ_{13}$. (ii) Suppose AC is a circumference strip pairing. Then it is still true that $AH_{13} \rightarrow CQ_{13}$ if HQ is a pairing at the 2nd position. For suppose A comes through the plugwheel to J and J and B are connected, and also O and R connected, and R wired back to C, giving AC. Then when rotatable section has gone round 13 places we get, instead of J – B – O – R, W – O – B – E. From H we go through plugwheel to W, then via O and B to E and back to Q through plugwheel, therefore again $AH_{13} \rightarrow CQ_{13}$.

3. We are now in a position to examine any pair of alphabets to see whether or not they can be 13 apart. Take D_1 and D_2 for example.

$D_1 = AL, CM, DG, EZ, FR, HY, IX, JN, KU, PW, QT, SV, BO.$

$D_2 = AK, CR, DN, EV, FS, GW, HP, IZ, JU, LX, MQ, TY, BO.$

Assume AC_{13} , say. Then $AC_{13} \rightarrow LR_{13} \rightarrow$ (via CA and RL) MK_{13} and $FX_{13} \rightarrow UQ_{13}$ and $IS_{13} \rightarrow TJ_{13}$ and $VZ_{13} \rightarrow NY_{13}$ and EE_{13} . Impossible. (It is fairly obvious that the

hypothesis $AR_{13} \rightarrow LC_{13}$ can be simultaneously failed). In this way it can be shown that D_1 and D_2 cannot be 13 apart.

If we try D_1 and D_3 we get a more interesting result.

$D_1 = AL, CM, DG, EZ, FR, HY, IX, JN, KU, PW, QT, SV, BO.$

$D_3 = AJ, CK, DZ, EQ, FM, GT, HU, IW, LN, PX, RS, VY, BO.$

$CV_{13} \rightarrow MY_{13} \rightarrow SK_{13}$ and $HF_{13} \rightarrow UR_{13}$ and RU_{13} }
 $DQ_{13} \rightarrow GE_{13} \rightarrow TZ_{13}$ and ZT_{13} } Unique solutions.

And $AI_{13} \rightarrow LW_{13} \rightarrow XJ_{13}$ and $PN_{13} \rightarrow JX_{13}$ and NP_{13} with three alternative results AP_{13} , LX_{13} , WJ_{13} , IN_{13} , or AW_{13} , LI_{13} , XN_{13} , PJ_{13} , or AX_{13} , LF_{13} , WN_{13} , IJ_{13} .

4. If we assume that these alphabets, D_1 and D_3 , are 13 apart it is easy to show that no other pair of alphabets from D_1 to D_9 are also 13 apart. For we have the following "13 apart" pairings:– $CV, MY, SK, HF, UR, DQ, GE, TZ$ and 4 sets of alternatives for the remaining pairs. Now consider D_2 : it has a pairing CR and since the letters "13 ahead" of C and R are V and U any alphabet 13 ahead of D_2 must have a pair UV . No alphabet has a pairing UV , therefore none of the other alphabets are separated by 13 from D_2 .

5. To discover all pairs of alphabets that could be thirteen apart it is not necessary to go through the rather laborious process of trial and error described above. Suppose we wish to test D_1 and D_2 . Box the alphabets and we get

(ALXIZEVSFRMCMQTYHPWGDNDJUK)
 1 2 4 6 6 4 2 1 3 5 5 3 . Now in the example we took $AC_{13} \rightarrow LR_{13} \rightarrow$

MK_{13} and $FX_{13} \rightarrow UQ_{13}$ and IS_{13} etc. and it can be seen that starting from an AC we are moving through the box as shown by small figures. If we have only one box compartment of a given size between 2 alphabets it is fairly easy to see that we get a solution if and only if it has $4n - 2$ letters in it. Within the box one alphabet is represented by letters 1 and 2, 3 and 4, 5 and 6 etc. and the other alphabet by letters 2 and 3, 4 and 5, 6 and 7 etc. Now make an assumption (e.g. AC in the example above) involving two letters separated by an odd number of letters i.e. pairing the 1st letter with the second $(2n + 1)$ th. Then 1st and 2nd letters belong to one alphabet and the 2nd and $(2n + 1)$ th to the other. Therefore starting from such an assumption we shall work in opposite directions from the basic letters and, since there are an odd number of letters between, the basic letters must reach a contradiction through a letter being paired with itself. Secondly make an assumption – e.g. "AE" in (ALXIZEVSFRMCMQTYHPWGDNDJUK) – with two letters separated by an even number of letters, i.e. 1st letter paired with the 2nd. Then we work in the same direction from the basic letters (see example) and are bound to get a contradiction unless the 1st and 2nd have equal intervals between them in either direction, i.e. unless there are $4n - 2$ letters together. On the other hand if there are $4n - 2$ letters we shall always get such a solution. Finally, if there are two compartments of the same size in a box between two alphabets we can always get a solution by pairing off the two compartments in any way, i.e. any letter in one compartment can go with a given letter in the other and once this original choice is made all the other pairings follow.

6. The nine alphabets so far recovered box in the following ways amongst themselves:– 12 24's, 6 22-2's, 5 16-8, 2 20-2-2, 2 12-12, 2 12-8-4, 2 12-8-2-2, 1 each of 20-4, 18-6, 12-6-6, 10-6-6-2, 10-6-4-4. Of these the only possible[/s] are 6 22-2's, 2 12-12's 18-6, 10-6-6-2, 10-6-4-4. The 22-2's and the 18-6 give unique solutions, the 12-12's give 12 each and the 10-6-6-2 and 10-6-4-4 give respectively 6 and 8 pairings uniquely and 7 and 4 solutions respectively for the remaining pairings. So we have in all 33 substantially different solutions. No two of these 33 solutions are compatible with each other (see Appendix), therefore there is at most one pair of alphabets 13 apart in the first nine.

7. Now suppose (a) that the rotatable section of the Umkehrwalze has a wiring joining two points 13 apart. Then if there are two of the D's 13 apart they will either have a common pairing (i.e. be female to each other) or else the two points must happen to come at B and O for these two particular D's. In the former case all or all but one of the rest of the D's (this one being an alphabet for which the wiring joins points opposite B and O on the rotatable section – there cannot be two such or we should have another pair of alphabets 13 apart, already disproved) must have a pair in common with the set of 13 aheads which we are testing. In the latter case all without exception must have a pair in common with the set of 13 aheads and in either case all these pairs must be distinct from each other. Consideration of what the 13 ahead are will make it obvious that this must be true.

8. Suppose (b) that the rotatable component has no wiring joining two points 13 apart. Then we can only get a "13 ahead" pairing occurring if we have 2 pairings of the rotatable section each joining two points the same distance apart and also the 2 pairings themselves being 13 apart, e.g. on the rotatable component, i.e. on the left of the plugwheel a joined to d and n to q. If this happens then the circumference strip pairing will give a "13 ahead" pairing for four positions of the rotatable component e.g. in the case instanced (ad and nq) we shall get (1) b e and o r (2) y b and l o (3) o r and b e (4) l o and y b and these positions will fall into pairs 13 apart, each pair being "female" on a 13 ahead pairing. Moreover, if two pairings of this kind exist, any pair of alphabets 13 apart, for which the two pairings do not involve B or O, will be doubly female. In my example if a d and n q are joined, then, when the rotatable component moves round 13 places, we get n q and a d joined, i.e. the same pairs over again.

9. To sum up the position, suppose we are testing a set of 13 aheads, derived from 2 D alphabets. Then either (1) these alphabets are not female. In that case (a) no 13 ahead pairing must occur as a pair in any individual D alphabet or else (b) every alphabet except the 2 basic ones must contain one and only one of the "13 aheads", and each alphabet must contain a different one. (2) The alphabets are singly female. In that case every other alphabet, except possibly one, must contain one and only one of the "13 aheads" (or else – just possibly – all but one contain exactly two of the "13 aheads", and that one contains one) and these "13 aheads" must again all be different. (3) The alphabets are doubly female. In that case (a) one or two (not more) of the remaining alphabets may contain a pairing of the "13 aheads" or (b) every other alphabet except possibly one or two (not more) must contain exactly two of the "13 aheads", and this one or two must contain one.

10. These conditions are extremely stringent ones and none of the possible solutions in Para 6 satisfy it, so if the Holmes hypothesis is correct no two of the nine D's recovered can be 13 apart. Assuming the 9 to be randomly chosen the chance of this a priori is $\frac{24 \cdot 22 \cdot 20 \cdot 18 \cdot 16 \cdot 14 \cdot 12 \cdot 10}{25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18} = \frac{1}{8.5}$ (approx.), so that a factor of 8.5 has been put against the hypothesis.

C. H. O'D. Alexander.

14th April, 1944.

Distribution:

A.D. (Mch).

Mr. Milner-Barry.
Major Babbage. (2)
Major Manisty.
Captain Fried.
Lt. Eachus, U.S.N.
Mr. Alexander (2)
Mr. Fletcher.
Mr. Lawn.
File.

Appendix I.

Although in this particular case there was no hypothesis left for further testing it might have happened that we should have found a set of 13 aheads which would satisfy the conditions in Para 9, and it is interesting to consider how we could test it further.

First we will consider how we could deal with the problem if there were no circumference strip pairing, and second how we can reduce the actual case to this.

(a) All pairings normal. Consider any two alphabets, say AS, CM, DG, EZ, FR, HY, IX, JN, KU, PW, QT, LV and AK, CR, DN, EV, FS, GW, HP, IZ, JU, LX, MQ, TY, and a set of "13 aheads", say AC, LG, TP, EW, QK, XY, JI, MU, ZH, RN, DF, SV. Suppose these alphabets are distance k apart. Then suppose AR to be a "k ahead": then, AS being a pairing in the 1st alphabet, and CR in the 2nd, SC will also be a "k ahead". But since AC and RN are "13 aheads", then, if AR is a "k ahead", CN must also be a "k ahead": similarly $SC \rightarrow VA$. From CN and VA we now deduce MD and LK from the original pair of alphabets and so on. This process can be simplified by boxing each alphabet in turn with the set of "13 aheads". This gives us $\begin{matrix} (ASVLGDFRNJIXYHZEWPQKUMC) \\ 1\ 2\ 4\ 6 \end{matrix}$ and $\begin{matrix} (AKQMUJIZHPTYXLGWEVSFDNRC) \\ 4\ 6 \end{matrix}$ and the numbering shows clearly how the pairings go (if we assume AC we go through the 2nd box in reverse order). Unless these two boxes are the same size as each other we shall obviously get a contradiction wherever we start, since we shall get back to the start of one box before we get back to the start of the other. In this case the hypothesis that the set of "13 ahead" is genuine is immediately destroyed. If the boxes are the same size (as here) then we have the following very powerful test: take the case AG_k . $AG_k \rightarrow SW_k$ and so the boxes pair off like this:

$$\begin{array}{l} ASVLGDFRNJIXYHZEWPQKUMC \quad (1) \\ GWEVSFDNRCAKQMUJIZHPTYXL \quad (2) \end{array}$$

Therefore (boxing these) AG_k , GS_k , SW_k , WI_k , IA_k , therefore $5k = 26$ since 5 moves down the upright of k each bring us back to the start. This is impossible. Therefore position is failed. The only possibilities are as follows: – (1) k odd. Starting from A we reach C in 13 turns and get back to A in 26. (2) k even. We reach A in 13 turns and C is in the other compartment ("AC" is a 13 ahead pair). This implies incidentally of course that when (1) and (2) are correctly set against each other they must give a 26 box or two 13 boxes and we can see at once that the position shown is wrong, since we have two 2 boxes (RN) and (DF) which would only be possible if the alphabets were 13 apart, which is already known to be untrue.

Normally we shall get no possible solution (there is none in this case) and then the sets of 13 aheads would be failed. If we do get a possible solution, then there will only be 13 possible values of k (odd or even according to the type of solution) each giving a complete upright from which the rod square can be reconstructed and the other alphabets compared with it which would be immediately decisive.

So when all pairings are normal we can fail a given "13 ahead" set fairly easily with two alphabets.

Now consider the actual case. A "Holmes alphabet" differs from a normal one got by having B wired through the plugwheel to B and O to O (or B to O and O to B) only in replacing pairs BJ and OK (say) by BO and JK, therefore to reduce a Holmes alphabet to an ordinary one interchange O with any of the other 24 letters, i.e. there are 24 possible "solutions". In the most difficult case (where none of the alphabets are female with the "13 ahead" set) box all of them with the 13 ahead alphabet. Choose the two boxes most unlike in shape. Now, since as shown above, the boxes for normal alphabets must be the same shape, if the set of "13 aheads" is right, the interchange of O with another letter must be made in such a way in the two alphabets as to produce boxes with the same shapes. Make the 24 interchanges for each of the two alphabets: these will obviously be very few if any pairs of alphabets with the same shape and they can be failed as described above. If one or more of the alphabets are female with the 13 ahead set the problem may be simplified owing to the circumference strip pairing being identified (see Para 8) and thus the letter to be interchanged with O being one of two.

Since writing the foregoing paragraph, I have seen that the problem is a great deal simpler than I thought. The only effect of changing, say, AL and BO into AO and BL is to insert OB in the original box between A and L: for instead of A to L we have A to O, O to B (from BO in the 13 aheads), B to L, therefore unless the box shapes of the original Holmes alphabets with the 13 aheads are the same or differ only in such a way that they can be made the same by adding 2 to one compartment of each (e.g. a 10/6 and an 8/8 can both be turned into 10/8) it is impossible for the corresponding "normal" alphabets to have the same box shape. So, except in the most unlikely event of all the alphabets producing the same or very closely similar box shapes when boxed with the set of "13 aheads", the hypothesis that the set is genuine can be failed at sight.

Appendix II.D Alphabets Boxed Together

Alphabets	1	2	3	4	5	6	7	8	9
	AL	AK	AJ	AL	AF	AY	AF	AV	AE
	CM	CR	CK	CD	CG	CK	CJ	CP	CI
	DG	DN	DZ	ET	DR	DF	DI	DW	DY
	EZ	EV	EQ	FN	EQ	ES	EP	ER	FK
	FR	FS	FM	GP	HN	GR	GQ	FN	GX
	HY	GW	GT	HU	IU	HZ	HS	GM	HJ
	IX	HP	HU	IY	JX	IW	KV	HX	LV
	JN	IZ	IW	JM	KY	JU	LY	IT	MT
	KU	JU	LN	KW	LT	LV	MT	JS	NS
	PW	LX	PX	QX	MZ	MQ	NW	KZ	PR
	QT	MQ	RS	RZ	PW	NX	RX	LU	QU
	SV	TY	VY	SV	SV	PT	UZ	QY	WZ
	BO	BO	BO	BO	BO	BO	BO	BO	BO

12. (ALXIZEVSFRMQTYHPWGDNJUK)
23. (AKCRSFMQEVYTGWIZDNLXPHUJ)
34. (AJMFNL)(EQXPQT)(CKWIYVSRZD)(HU)
45. (ALTEQXJMZRDCGPWKYIUHNF)(SV)
56. (AFDRGCKY)(EQMZHNXJUIWPTLVS)
67. (AYLVKCUJZHSEPTMQGRXNWIDF)
78. (AFNWDITMGQYLKZKV)(CJSHXREP)
89. (AVLUQYDWZKFNSJHXGMTICPRE)
91. (AEZWPRFKUQTMCI XGDYHJNSVL)
13. (ALNJ)(IXPW)(DGTQEZ)(CMFRSVYHUK)
24. (AKWGPHUJMQL)(CRZ IYTEVSFND)
35. (AJXPW IUHNL TGCKYVSRDZMF)(EQ)
46. (ALVSETPGRZHUJM QXNFDCKWIY)
57. (CGQEPWNH SVKYL TMZUIDRXJ)(AF)
68. (AYQMGRESJULV)(CKZHXNFDWITP)
79. (AFKVLYDICJHSNWZUQGXRPE)(MT)
81. (CMGDWP)(HYQTIX)(AVSJNFREZKUL)
92. (AKFSNDYTMQUJHPRC IZWXGLVE)
14. (CMJNFRZETQXIYHUKWPGD)(SV)(AL)
25. (AKYTLXJUIZMQEVSF)(CRDNHPWG)
36. (AJUHZDFMQESRGTPXNLVY)(CK)(IW)
47. (ALYIDCJMTEPGQXRZUHSVKWNF)
58. (AFNHXJSV)(IULT)(CGMZKYQERDWP)
69. (AYDFKCIWZHJUQMTPRGXNSE)(LV)

71. (ALYHSVKUZE PWNJCMTQGDIXRF)
 82. (AKZITYQMGWDNFSJULXHPCREV)
 93. (AJHUQE)(CKFMTGXPRSNLVYDZWI)
 15. (ALTQEZMCGDRF)(HYKUIXJN)(PW)(SV)
 26. (AKCRGWIZHPTY)(DNXLVESF)(JU)(MQ)
 37. (AJCKVYLNWIDZUHSRXPEQGTMF)
 48. (ALUHXQYITERZKWDCPGMJSV)(FN)
 59. (AFKYDRPWZMTLVSNHJXGCIUQE)
 61. (ALVSEZHY)(CMQTPWIXNJUK)(DGRF)
 72. (AKVEPHSF)(CRXLYJMQGWNDIZUJ)
 83. (AJSREQYV)(CKZDWITGMFNLUHXP)
 94. (ALVSNFKWZRPGXQUHJMTE)(CDYI)

<u>Box Shape</u>	<u>Number</u>
24	12
22/2	6
20/2/2	2
20/4	1
18/6	1
16/8	5
12/12	2
12/8/4	2
12/8/2/2	2
12/6/6	1
10/6/6/2	1
10/6/4/4	1

Possible Sets of U.D. "13 Apart" Pairings.

<u>Alphabets</u>		<u>Pairings.</u>											
3,4	1	CV	KS	WR	IZ	YD	HU and AF	JN	ML	EP	QG	XT or	
											(AJMFNL)	with (EQXPGT)	
4,5	2	AC	LG	TP	EW	QK	XY	JI	MU	ZH	RN	DF	SV
1,3	3	CV	MY	FH	RU	SK	DQ	GE	TZ	(ALNJ)	with (IXPW)		
2,4	4	AC	KD	WN	GF	PS	HV	EU	JT	MY	IQ	XZ	LR
	5	AZ	KR	WC	GD	PN	HF	US	JV	ME	QT	XY	LI
	6	AY	KI	WZ	GR	PC	HD	UN	JF	MS	QV	XE	LT
	7	AE	KT	WY	GI	PZ	HR	UC	JD	MN	QF	XS	LV
	8	AS	KV	WE	GT	PY	HI	UZ	JR	MC	QD	XN	LF
	9	AN	KF	WS	GV	PE	HT	UY	JI	MZ	QR	XC	LD
	10	AD	KC	WR	GZ	PI	HY	UT	JE	MV	QS	XF	LN
	11	AF	KN	WD	GC	PR	HZ	UI	JY	MT	QE	XV	LS
	12	AV	KS	WF	GN	PD	HC	UR	JZ	MI	QY	XT	LE
	13	AT	KE	WV	GS	PF	HN	UD	JC	MR	QZ	XI	LY
	14	AI	KY	WT	GE	PV	HS	UF	JN	MD	QC	XR	LZ
	15	AR	KZ	WI	GY	PT	HE	UV	JS	MF	QN	XD	LC
3,5	16	AG	JC	XK	PY	WV	IS	UR	HD	NZ	LM	TF	EQ
5,7	17	AF	CY	GL	QT	EM	PZ	WU	NI	HD	SR	VX	KJ
6,8	18	AP	YC	QK	MZ	GH	RX	EN	SF	JD	UW	LI	VT
	19	AI	YT	QP	MC	GK	RZ	EH	SX	JN	UF	LD	VW
	20	AD	YW	QI	MT	GP	RC	EK	SZ	JH	UX	IN	VF
	21	AN	YF	QD	MW	GI	RT	EP	SC	JK	UZ	LH	VX
	22	AH	YX	QN	MF	GD	RW	EI	ST	JP	UC	LK	VZ
	23	AK	YZ	QH	MX	GN	RF	ED	SW	JI	UT	LP	VC
	24	AC	PY	QT	MI	GW	RD	EF	SN	JX	UH	LZ	VK
	25	AZ	YK	QC	MP	GT	RI	EW	SD	JF	UN	LX	VH
	26	AX	YH	MK	GC	RP	ET	SI	JW	UD	LF	VN	QZ
	27	AF	YN	QX	MH	GZ	RK	EC	SP	JT	UI	LW	VD
	28	AW	YD	QF	MN	GX	RH	EZ	SK	JC	UP	LT	VI
	29	AT	YI	QW	MD	GF	RN	EX	SH	JZ	UK	LC	VP
7,9	30	AS	FN	KW	VZ	LU	YQ	DG	IX	CR	JP	HE	MT
6,9	31	AU	YQ	DM	FT	KP	CR	IG	WX	ZN	HS	JE	LV
9,3	32	AU	JQ	HE	CS	KN	FL	MV	TY	GD	XZ	PW	RI
4,8	33	AZ	LK	UW	HD	XC	QP	YG	IM	TJ	ES	RV	FN

Pairings in Common Between D Alphabets and "13 Ahead" Sets.

1. IZ 2. DY 9. HU 3,4.
2. PT 6. HZ 6. DF 6. SV 1,4,5.
3. -. In subsidiary LX 2. JX 5. NX 6. NW 7. (Subs are AI, LW, XJ, PN/AP, LX, WJ, IN/AW, LI, XN, PJ/AX, LP/WN/IJ.
4. NW 7.
5. DG 1. QT 1.
6. AY 6. WZ 9. GR 6. CP 8. LT 5.
7. AE 9. LV 6,9.
8. KV 7. GT 3. UZ 7. CM 1. NX 6.
9. FK 9. EP 7. MZ 5.
10. CK 3,6. HY 1. LN 3.
11. AF 5,7. DW 8. CG 5. PR 9. HZ 6. IU 5. MT 7,9. EQ 3,5.
12. AV 8. QY 8.
13. HN 5. CJ 7. IX 1. LY 7.
14. KY 5. HS 7. JN 1. RX 7.
15. KZ 8. IW 3,6. PT 6. JS 8. FM 3.
16. CJ 7. EQ 3,5.
17. AF 5,7. QT 1. RS 3.
18. MZ 5. RX 7. FS 2.
19. TY 2. CM 1. RZ 4. JN 1.
20. MJ 7,9. GP 4. CR 2. HJ 9. LN 3.
21. EP 7. UZ 7.
22. FM 3. DG 1.
23. AK 2. FR 1.
24. QT 1. GW 2. DR 5. NS 9. JX 5. HU 3,4. KV 7.
25. KY 5. GT 3. LX 2.
26. HY 1. CG 5. PR 9. ET 4.
27. AF 5,7. QX 4. IU 5.
28. DY 9. GX 9. EZ 1. CJ 7. LT 5.
29. IY 4. HS 7. KU 1.
30. FN 4,8. KW 4. LU 8. QY 8. DG 1. IX 1. CR 2. MT 7,9.
31. QY 8. CR 2. HS 7. LV 6,9.
32. TY 2. DG 1. PW 1,5.
33. ES 6. FN 4,8.

Variations of 1.

1.1.	AF, JN, ML, EP, QG, XT.	AF 5,7. JN 1. EP 7. GQ 7.)
1.2.	AE, JT, MG, FP, NX, LQ.	AE 9. GM 8. NX 6.)
1.3.	AQ, JX, MP, FG, NT, LE.	JX 5.)
1.4.	AX, JQ, ME, FT, NG, LP.) All down
1.5.	AP, JG, MT, FE, NQ, LX.	MT 7,9. LX 2.)
1.6.	HG, JP, MX, FQ, NE, LT.	LT 5.)
1.7.	AT, JE, MQ, FX, NP, LG.	MQ 2,6.)

All 33 positions failed. None of the female pairings satisfy the conditions of Para 8-10.

Editor's Notes

1. U.D. stands for Umkehrwalze D, the pluggable reflector also called Uncle Dick at Bletchley Park, which was introduced on German Air Force nets in January 1944.
2. For an explanation of rods, rod squares, boxes, and boxing 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.
3. Female is a BP expression for a given constation to appear in two different places in the message usually at a relatively short distance. A constation is the association of a cipher letter with its assumed plaintext equivalent.