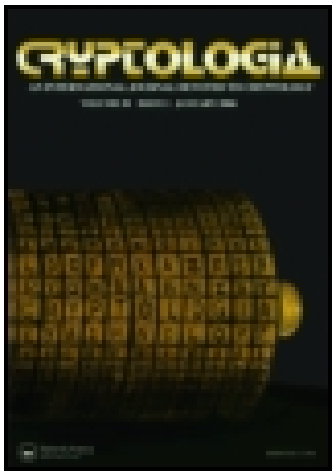

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

ALAN M. TURING'S CRITIQUE OF RUNNING SHORT CRIBS ON THE U. S. NAVY BOMBE

ALAN M. TURING

Published online: 04 Jun 2010.

To cite this article: ALAN M. TURING (2003) ALAN M. TURING'S CRITIQUE OF RUNNING SHORT CRIBS ON THE U. S. NAVY BOMBE, Cryptologia, 27:1, 44-49, DOI: 10.1080/0161-110391891748

To link to this article: http://dx.doi.org/10.1080/0161-110391891748

CRYPTOLOGIA January 2003 Volume XXVII Number 1

ALAN M. TURING'S CRITIQUE OF RUNNING SHORT CRIBS ON THE U. S. NAVY BOMBE*

ALAN M. TURING

We are rather surprised to hear that you are able to find the keys, given that a message when deciphered says VVVBDUUU . Our experience shows that with a 'crib' as short as 8 letters there are always far too many sets of keys consistent with the data, so that whatever method may be used for discovering the keys, the time required to test these solutions out further becomes prohibitive. To illustrate this I have enciphered VVVBDUUU with a random chosen key *viz* wheel order 457, English *Ringstellung* RWH, pre-start window position SZK and Stecker A/P, B/Y, C/L, E/Q, F/X, K/R, M/W, N/T, O/V, S/Z, giving YFZONMTY. I then imagined that

Y	F	Z	O	N	M	T	Y
V	V	V	B	D	U	U	U

was a crib that I had to solve, but that I knew the wheel order and *Ringstellung*: I tried out the hypothesis that the pre-start window position was the right one (SZK) and also the five which follow it (allowing correctly for turnovers) *viz* TAL, TAM, TBN, TBO, TBP, and found that with pre-start TBP there is a solution with V/J, F/G, Z/H, Y/E, U/X, M/L, T/K, D/P and either B/S and O/W or B/W and O/S. The 'unsteckered alphabets' for the relevant positions of the machine are shown in Fig 1, and the working in Fig 2. I hope that this working is self-explanatory. Each column of letters consists of steckers of the letters VFZYUMT which imply one another on account of the crib.

A continuation of this process would probably give about 3000 essentially different solutions per wheel order. Of course these solutions are not all equally likely: e.g. the solution with pre-start TBP is unlikely as the complete set of 10 Stecker has to be assumed to account for the whole crib, whereas with the right solution we can only deduce O/V, F/X, S/Z, Y/B, W/M, N/T, and D and U

In the previous paper, "A Small Treasure: Alan M. Turing's Interrogatories about the US Navy Bombe," Lee A. Gladwin introduces this work by Turing. We produce the paper with appropriate figures.

self-steckered. But there will still be a great many that look as good as this. A fairly simple calculation tells us the probability of this solution being the right one, under the assumption that the wheel order and *Ringstellung* are right. The total number of ways of setting up 10 Stecker is about 1.5×10^{14}, and the number of essentially different window positions is 16224, so that the total number of sets of keys in question is about 2.4×10^{18}. From this we can obtain the expected number of sets of keys consistent with the data by multiplying by 26^{-8}. We get 1.15×10^{7}. Now the solution in question can be made into a complete set of keys, by completing the Stecker in 51975 ways, i.e. it corresponds to 51975 of the 1.15×10^{7} solutions and therefore has a probability of $51975/(1.15 \times 10^{7}$, or 0.0045. We may therefore expect to have anything from say 50 to 1000 solutions to test further on each wheel order, even if we assume the *Ringstellung*, or, what comes to the same, the position of the turnover in the message. The examinations of these solutions is not very easy, especially in the case of likely looking solutions as in such cases we necessarily know comparatively few Stecker, and so can get

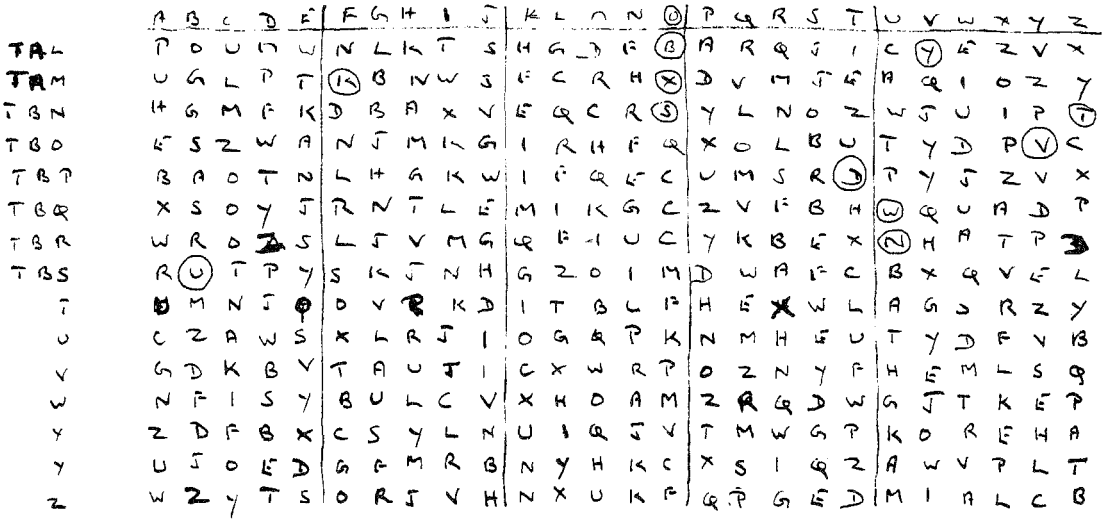

Figure 1. Alphabets for V V V B D U U U / Y F Z O N M T Y

The working shown in Fig 2 is not given as a suggested method for solving these cribs. It is part of an *a fortiori* argument to the effect that even if all solutions had been found by this method or some other the remaining work to be done would still be too much.

Leaving aside this general aspect of the problem I should be interested to be sure that I understand your method correctly: the argument given above depends

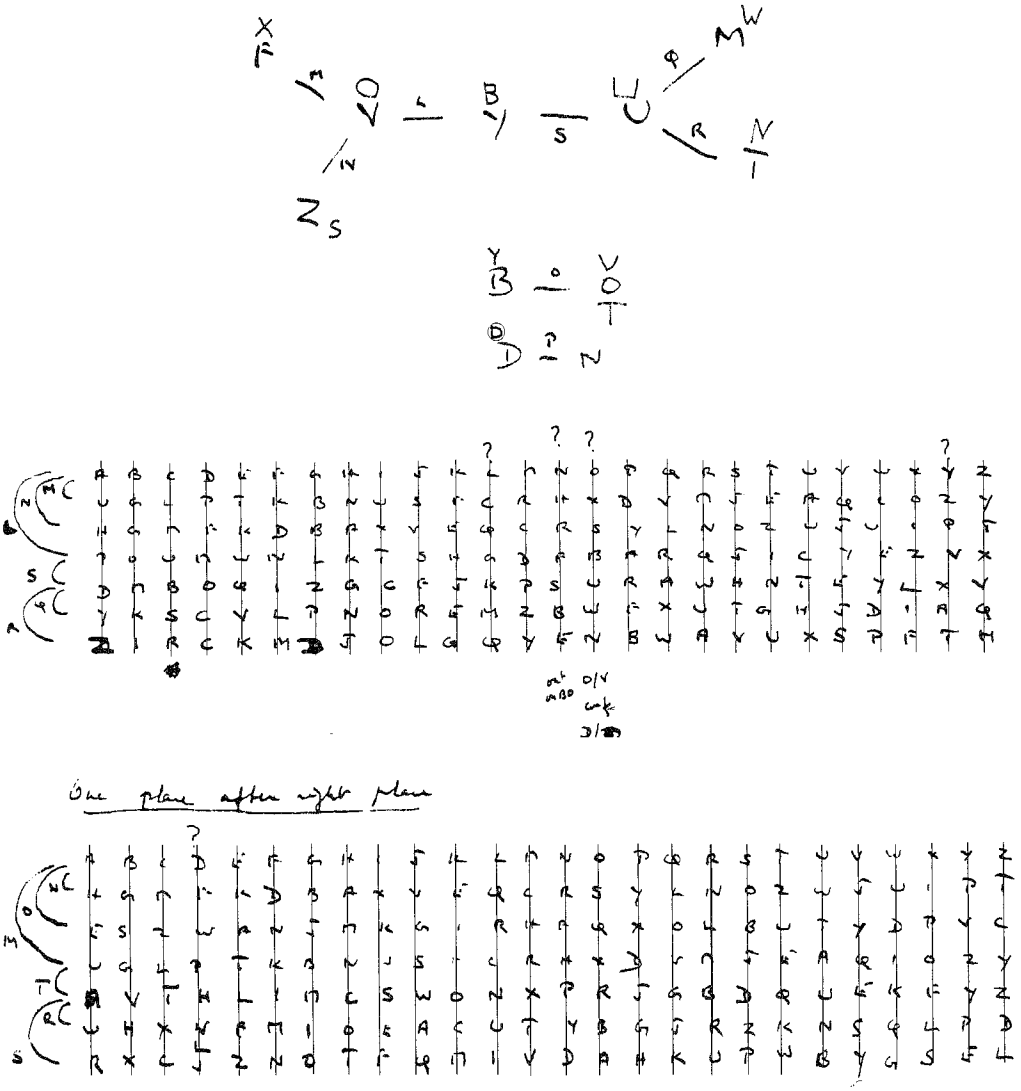

Figure 2. Part of the workings to solve

L	M	N	O	P	Q	R	S
Y	F	Z	O	N	M	T	Y
V	V	V	B	D	U	U	U

essentially on the length of the crib, and it may well be that you have a method which will deal with rather longer cribs.

As I understand it your method is to assume Stecker for certain letters thereby obtaining certain 'unsteckered' constatations. One then takes 26 separate hypotheses concerning the position of the R.H.W. and deduces, for each hypothesis the 'output' of the two left hand wheels and U.K.W. Assuming the wheel order one then looks up in a catalogue and finds the possible positions of the two wheels on the left. The whole effect of the process so far is to find the positions of the wheels consistent with the unsteckered constatations. Each position must be examined more closely afterwards, with a machine.

The process may be explained by means of an example.

S	D	D	Q	T	Y	M	D
V	V	V	B	D	U	U	U

This is a favourable one as the same constatation VD occurs twice over. Suppose now that we with to try out the hypothesis that V and D are both self-steckered on wheel order 457. Assume that there is no turnover between the two occurrences of VD. We lay down the 'Inverse rods' for V and D and wheel 7; the effect of this is shown in Fig 3.

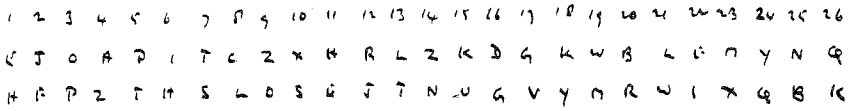

Figure 3. Inverse rods of wheel VII, for solving

V	V	V	B	D	U	U	U
S	D	D	Q	T	Y	M	D

The information we get from them is for instance that if VD were enciphered with no Stecker and with R.H.W. in absolute position (window position less English *Ringstellung*)17, then, if the R.H.W. were replaced by a 'straight through' wheel, and the other wheels kept the same and in the same positions, then find where, with wheel order "4 5 straight" we can get the pairings EH and JF, also where we can get JF and PO, and so on. We have catalogues in which we can look these pairs up. We find for instance that PO, AZ occurs in position 8 of the L.H.W. and 22 of the M.W. and therefore that without Stecker we get VD in absolute solutions 8, 22, 3 and 8, 22, 4. The complete set of solutions is shown in Fig 4. These solutions have now to be tested out on the remainder of the crib. Take the case of the solution 8, 22, 3 and suppose we are assuming there is no turnover in the whole crib. Then the DU will have been enciphered at 8, 22, 9 at which position D enciphers without Stecker to Z. Since we are assuming that D is self-steckered, we must have ZU. Now the UY constatation was enciphered at

8, 22, 6 where Z without Stecker enciphers to V. We therefore have V/Y contrary to the hypothesis that V was self-steckered.

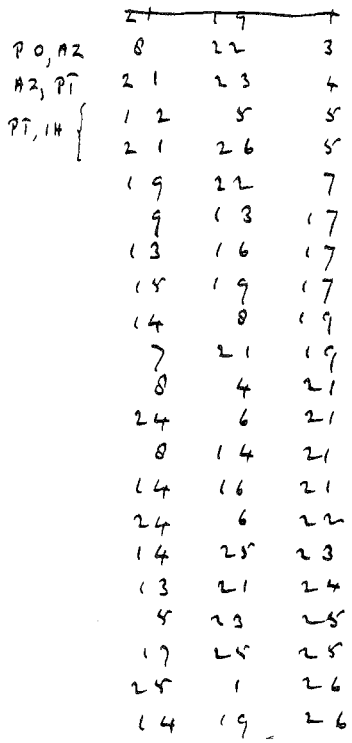

Figure 4. Position where we get $\begin{matrix} V & V \\ D & D \end{matrix}$ in wheel order 457.

The full examination of the possibilities of turnover takes some considerable time. Of course it is only worth while considering rather longer cribs than VVVB-DUUU: with cribs of length 20 it would be possible to deal with a wheel order on one assumption of Stecker for the letters taking the place of V and D in about five hours, of which about half an hour or less would be the looking up in catalogues. Suppose that we have a very large supply of cribs, 100 a day say, each with probability, $\frac{1}{2}$ of being right. The chance of the two letters being self-steckered is $\frac{3}{65}$, and therefore working on 336 wheel orders we should have on average $22^1/3 \times 336 \times 5 \times 2$ i.e. 72800 hours work to obtain a solution.

Would you mind telling us about your method

1. Does it give the keys starting from scratch, or does one need to start with the Stecker?

2. Is the above account substantially correct?
3. Do you work with cribs as short as VVVBDUUU? Have you any longer ones?
4. About how many hours work do you estimate would be necessary to obtain a solution on 336 wheel orders?