DUD-BUSTING

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’. In all the texts this has been written without capitalization. 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, © May 1998

Source:

Addendum to Captain Walter J. Fried’s report No. 40 of 23 May 1944. National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 880, Nr. 2612.

COPYRIGHT

DUD-BUSTING.

A dud is any message whose setting is unknown and which we try to get out on the assumption that it is on a known machine key (i.e. wheel order, ringstellung and Stecker known). Occasionally we may wish to try on a partially known key; the Stecker must be known, (or limited to one of a few possible sets, e.g. when there is an unknown slide on it) but the wheel order and/or ringstellung may be unknown. These cases, however, are exceptional and for the great majority of duds the complete key is assumed known.

This paper is a description of the various types of duds and of the different methods of attacking them. It is written (1) to inform all interested parties of the various methods available and the types of job for which they are suitable (2) to find out what use is being made of the available facilities and how far they are adequate (3) to discover how useful improved methods would be and what type of improvements are desirable. We hope there[fore] that everyone concerned will express their views as the amount of effort put into attempts to produce new machinery must depend on the probable gain to be achieved.

A. Types of DUD.

1. Complete key with the indicators of all messages unknown. This occurs on naval traffic at 6 - 12 monthly intervals when the bigram tables change. The object is to get as many messages as possible out as quickly as possible, and it does not matter if the method is one which fails a number of messages, since these will come out later when the tables are built up. Moreover should the same problem arise for any reason on air or army traffic (e.g., through adoption of an indicator book) this requirement (a lot of messages quickly rather than 100% success) would probably still hold.

2. Limited set of messages with specially disguised indicators. The typical example of this is Offizier messages on naval traffic. Each Offizier key (there are 6 main keys of this type) has 26 settings, denoted by A to Z, which remain in force for a month. Here it is important to find every setting so we require a method giving a high chance of success, but it is not essential for it to be very fast, since in practice there will probably not be more than 80 or 90 settings a month to be found and a number of these will be very easy by hand methods.

3. Ordinary duds. These are messages whose indicators are corrupt or missing altogether. They might be subdivided into 3.1 duds of great cryptographic or intelligence importance, which must be got out if in any way possible and for which speed may also be important; 3.2 common or garden duds, which one would like to get out if it can be done without undue labour. This problem is largely a Hut 6 trouble as owing to multiplicity of keys and

the different indicator system about 10% of readable traffic is dud, whereas only about 1/5th of one percent as in this category for Hut 8.

4. Messages whose key is doubtful. This is almost entirely an air and army headache. Now that discriminants have gone it is frequently difficult to tell whether a message that fails to come out has failed because the message is a genuine dud or because it is on a different key. With such messages it is important to determine definitely which of these explanations is correct and therefore we require a method giving the highest possible chance of success if the message is an ordinary dud.

5. Messages on a key partially identical with, or connected with, a known key. This is mainly a Hut 6 problem. It arises when there is evidence that one key is repeating the Stecker of another, or possibly Stecker and wheel order. Sometimes it is certain that such a repeat is taking place, in which case it is a question of getting out one message on the key in question and therefore if there are a number of messages one can use a method which will give a reasonable chance on each separate message, or if there are one or two peculiarly favourable messages (e.g., cribbable messages) these can be attacked by methods giving a high chance in the special circumstances. The other case is when the key repeat is not certain (may indeed be merely an outside chance), in which case one wants to fail a chosen message as thoroughly as possible. Here again, however, if there are a large number of messages on the key a method giving a fair chance on each message would be sufficiently conclusive if it failed to get a single success.

Theoretically any or all of these problems might be met on three wheel or four wheel keys. In practice only 2 is met with on any appreciable scale as a four wheel problem; 1 might have to be faced in the future and 3 occurs on a very small number of messages.

B. Methods of Attack.

1. Twiddling. This is the straightforward trial and error method used when the indicator is partially known, e.g. has all letters but one correct and all possible alternatives are tried for this.

2. Hand rodding. This method is used when there is a crib in a known position in the message (e.g., ANX at the beginning of the message). It can also be used for cribs in unknown positions, but unless the crib is fairly long or the choice of positions very limited it is so tedious that it is better to use some form of machinery.

3. Click Machine. This is a machine for testing a crib (preferably 7 or 8 letters and certainly not less than 6) in a large number of different positions; it is essentially a mechanical method of rodding and its results have to be further tested by hand, much as in the case of bombe stops.

4. Eins catalogue. Some common word (usually EINS) is encoded at all positions of the machine and the results compared mechanically with the contents of the messages, thus getting out all messages containing an EINS somewhere in them.

5. Jones Dudbuster. This drags a 4-letter crib (e.g. EINS) through a message testing 33 positions at a time. It uses a modified bombe; either a 3-wheel or a 4-wheel machine can be used.

5 (a) Grenade. This is an attachment to the Op 20 G machines enabling a 4-letter crib to be dragged through a message testing 4 positions at a time. The Jones dud buster is a development from this. Although the Jones 3-wheel dud-buster does 8 times as many positions at a time it is doubtful whether it is any faster, if as fast, as Grenade is attached to a 4-wheel machine and therefore runs much more quickly.

6. Hypo. This is a photographic method which compares a film of the cipher message with a film of the encodes of one or more (usually 5) common letters at all possible positions of the machine and looks for a position where there are a very large number of agreements between the two films.

7. Arlington Dud-buster. This is a modification of a bombe to do in a different way the same sort of job as Hypo. It has the drawback that it can only use one letter of text per enigma involved, so that the full message can not normally be used. This method has now been abandoned as not a sufficiently profitable use of the Arlington machine.

8. Test Plate 7 letter decode. The first seven letters (or more - seven is usually sufficient) of the message are decoded at all possible positions of the machine and the results listed alphabetically and then examined to see whether any of the answers are German.

C. Uses of Different Methods.

A chart showing approximately the time taken on the various methods, the trouble involved and so on, is attached at the end of this paper. This section is a discussion in general terms of the merits of the various possible attacks in the different circumstances listed in Section A.

Method 1 (twiddling) is only applicable when the message setting is almost completely known. When it works it is the simplest and probably the quickest way. 2 and 3 imply some knowledge of the content of the message, 2 of a crib (2 letters or more) in a fixed position, 3 of a longer crib (7 letters) somewhere in the message (e.g., a time, name or an address). They are both methods working on the right-hand wheel only, and therefore suitable for cases where the W.O. is unknown, since there are then only 5 (or 8 on naval) alternatives instead of 60 (or 336 on naval) as would be the case for methods using all three (or four) wheels. Methods 4 and 5 do not need any special knowledge about a particular message, but simply a general knowledge of what 4 letter word or words are likely to occur in traffic of that general type – the essential difference from Method 3 is that there are 4 letter words (e.g., EINS) with a high chance of occurring in any sort of traffic but there are no 7 letter words of a similar character.

Method 4 has the special advantage of being a wholesale method and dealing with a large number of messages simultaneously. Methods 6 and 7 assume nothing about the traffic except that it has normal language properties; 6, which uses the whole message, is an extremely powerful method and almost certain of success if the message is over 100 letters long - 7 can only use a portion of the message and is correspondingly weaker. Method 8 is the clumsiest and most laborious of all the methods but in some ways the most powerful; given a very short message with rather unusual content all methods 1 to 7 will probably fail, but (provided the beginning of the message is not corrupt) 8 must be successful if the decode of the first 7 letters is recognisable German.

For Type 1 duds (complete key with all indicators unknown) the EINS catalogue is far and away the best method, as it deals with all the messages simultaneously. When it is only necessary to get out half or less of the messages considerable time can be saved by only running half (or smaller fraction) of the EINS catalogue; this still gives half (or proportionately reduced) chance on messages containing one EINS and three-quarters or more on messages containing 2 or more EINS. This is assuming a 3-wheel key; no really adequate solution is known for the case of a complete 4-wheel key with unknown indicators. At the moment, if the key were several hundred messages, a partial EINS catalogue would still be best, but too slow to be satisfactory.

For Type 2 3-wheel duds one tries (1) any good initial crib (e.g., EINSKK) by hand (2) a really good crib on the Click machine (3) the Jones dudbuster (4) Hypo. Hand rodding is the quickest method if there is a good crib but it is not worth trying mediocre shots; the Click machine is only worthwhile if there is a practically certain crib; the Jones dudbuster is slower than Grenade or Hypo and has a smaller chance than Hypo, but it is less trouble and quicker in practice owing to saving transmission time to Washington. Moreover its time should improve when operators have had more experience. If there were half a dozen or more messages on the same key, (which does not very often occur) an EINS catalogue would be the best method as it would deal with all messages simultaneously. For 4-wheel duds of this type the same procedure should be used except that an EINS catalogue is impracticable.

For Type 3.1 the procedure should be the same as for Type 2 except that one might send simultaneously to the Click machine and the Jones dudbuster if there was a sufficiently high degree of urgency. Type 3.2 we are unable to cope with at the moment owing to the large number of messages involved; the methods used should be as for 2 and 3.1 except that it might quite often be best to run an EINS catalogue owing to there being a number of messages, (say 6 or more) on the same key.

Type 4 duds, if expected to come out, should run first on the Jones dudbuster and then on Hypo, and if not expected to come out should be run immediately on Hypo. This is a small class of messages because if there are several messages on the same frequency, none of which will come out in the normal way, that is really sufficient evidence without any dudbusting that they do not belong to the key in question and therefore it is only isolated messages on a new frequency which are concerned. If there is a strong presumption that these messages will not come out and we wish to make certain that a new key is involved then an immediate run on Hypo is best; the Jones dudbuster is unlikely to get the message out, but its failure to do so will not be conclusive proof that a new key is being used; to get this proof Hypo is necessary and so might as well be used in the first instance. This of course is based on the assumption that the number of messages involved is not too great for Hypo to handle; if it is, then it is best to send the most important ones to Hypo and try the rest on the Jones dudbuster. It is difficult to see just what is the most profitable procedure with this group and the views of the Hut 6 duddery would be very welcome; a great deal depends on the number of duds involved and their importance from the sorting point of view.

Type 5 duds are suited to a variety of different methods according to the circumstances. There are 2 groups (a) W.O. but not rings. [sic. ringstellung] known (b) neither W.O. nor rings. known and each of these subdivide into two according to whether we expect to succeed or to fail and are further subdivided according to whether they carry very few messages or a large number (the dividing line would be somewhere about 6). The simplest way to show the best procedures is in tabular form (S = success expected, F = failure, L = large traffic, S [sic. s] small).

	SL	Ss	FL	Fs
a)	1. Handrodding 2. Eins catalogue	1. Handrodding 2. Jones, Click 3. Hypo	Eins	1. Jones 2. Hypo
b)	1. Handrodding 2. Click 3. Jones	1. Handrodding 2. Click 3. Jones	(1. Handrodding (2. Click	1. Handrodding) 2. Click)

If there is a good hand crib it will always be the best method. With more than a few messages one is almost bound to contain Eins (unless it is a very unusual type of traffic) so that the Eins catalogue - provided W.O. is known - is the most satisfactory method whether one expects success or failure. With a large number of messages it is a waste of time to run a complete Eins catalogue; e.g., with 50 messages, a quarter catalogue run against all the messages would give a conclusive answer one way or the other. With only one or two messages if W.O. and rings. are known the procedure is the same as for previous types and the same arguments apply. With unknown ringstellung considerably more trouble is involved on Hypo and the chance of success substantially reduced; the Click machine and Jones dudbuster are unaffected as they ignore turnover in any case. It would seldom be worthwhile using Hypo in these circumstances. For unknown W.O. handrodding and Click machine are the best methods since it is only necessary to try all possible right-hand wheels instead of all possible wheel orders; if these fail and the key is of sufficient importance the Jones dudbuster could be run on all W.O.’s, but these would be an extremely long job and only worth doing in exceptional cases. I have bracketed the entries under “failure expected” here as I rather doubt whether it would be worth doing anything in these circumstances.

In the description of methods used the Arlington Dudbuster has not been included as it does not seem worthwhile tying up a quarter of the Arlington bombe (‘Madam’) and a large number of staff in view of the alternative methods now available.

D. Limitations of Present Equipment.

With the facilities available we are able to cope fairly satisfactorily with the dud problem with the following exceptions: –

(1) Although we may be lucky we cannot relay on getting a dud out in under six hours; we could I think be fairly sure of doing it in that time if it was of vital urgency, but there might be rare occasions on which it was very undesirable to be faced with such a delay.

(2) We cannot deal completely with the ordinary dud problem as there are too many messages in this case for us to be able to get them out at present speeds.

(3) We have no satisfactory way of dealing with a four-wheel key with the indicators of all messages unknown. If Dolphin (the chief naval key involved in this problem) were to go four-wheel and then the bigram tables were to change we should be considerably delayed in building up the new tables. We could do it but it would be far too slow for us to regard the position as at all satisfactory.

E. Possible Further Developments.

Of the points listed in D, (1) - which is the least important - could be met by the production of a dudbuster dealing with a message in half an hour or an hour. To solve (2) and (3) completely we should need a machine capable of dealing in about 5 minutes with a 3-wheel dud (for 2) and a 4-wheel dud (for 3). A machine capable (in practice, not in theory) of dealing with a 4-wheel dud in under half an hour would be valuable for (3) though by no means a complete solution; for (2) I do not think it would be worthwhile having a machine that averaged more than fifteen minutes per 3-wheel dud. This seems to indicate that the proper policy is (1) to try and speed up and improve in minor ways our existing equipment and methods (2) not to embark on any new machine unless it is going to work at a far higher speed than any of our existing machines – 10 or 20 times as fast in fact.

If this is accepted then the most profitable line of development seem to be (1) improvement in the Jones dudbuster, including assembly of the necessary apparatus to enable several 3-wheel and old type 4-wheel bombes to be used as dudbusters and also experiments on the new type 4-wheel machines (to run 3-wheel jobs fast). In this way we might both cut down times and provide ourselves with an adequate reserve should the dud problem increase in size. (2) the "one enigma" dudbuster which Arlington are working on and which might be able to do a 3-wheel job in 5 minutes and a 4-wheel job in under half an hour.

C.H.O'D. Alexander

(for U.D. committee)

Appendix. Table showing Performance of various forms of Dud-buster

Dudbuster	Chance of Success	Machine Time		Labour involved		Comments.
		a.3W	b.4W	Preparatory Work	Testing	
Click Machine	60% if crib correct	3 hrs.		Unsteckering message ¼ to ½ hr. per message	1 hr. per crib per message	With long crib that can be menued for T.O. chance probably 90%. Testing time is estimate for average girl. If a series of cribs are run they should come back at about half hourly intervals from Block C.
Eins Catalogue.	80% per message	8 hrs.		Alphabeting message. General instructions key, number of runs. ½ hr. to 1 hr.	Depends on No. of messages. 20 messages per hr. would be slow going.	Only running half the Eins catalogue would very nearly halve the machine time; reducing the number of messages makes very little difference. Times here and for Click machine assume that job has high priority. 4-wheel catalogue has never run; one would probably run (if driven to it) a quarter catalogue taking about 2 days.
Jones Dudbuster	75% per message on Eins	6 hrs.		Unsteckering message. ¼ to ½ hr. per message	Done by Bombe Hut	% chance put slightly lower than for Eins catalogue as Eins may be missed through turnover. Hoped to reduce time to 3 hrs. when operators are more experienced. 4-wheel time unknown at present but probably about half as much again.

Dudbuster	Chance of Success	Machine Time		Labour involved		Comments.
		a.3W	b.4W	Preparatory Work	Testing	
Grenade.		3 hrs?				Details unknown. Same general method as Jones dudbuster but rather faster as it is modified 4-wheel machine. Would be too slow for a 4-wheel drag on similar lines.
Hypo.	Almost 100% on messages of more than 100 long.	2 hrs.	4 hrs.	"Stripping" right-hand wheel in 26 positions. 1 hr.	Done as part of machine process.	If a series of messages on the same key are done the average time is reduced from 3 or 5 hrs. to about 1½ hrs. If the rings. is unknown the work involved is at least doubled and the chance of success considerably reduced (to about 90% on 200 letter message and worse on shorter message)
Test Plate Decode.	Almost 100% unless message is corrupt at the beginning.	8 hrs.		15 minutes	About 3 hrs. if rings. is known. Considerably longer if rings. is unknown.	If the rings. is unknown probably best to menu it by doing first the seven letters and if this fails the next seven (or more) assuming no T.O. in each case.

Editor's Notes

1. The document is not dated but it is known to have been presented at the 9th meeting of the U.D. Committee on 15 May 1944. The U.D. Committee, which presumably stands for "Umkehrwalze D Committee," was created to deal with the Umkehrwalze D and related problems and had its first meeting on 3 April 1944.
2. W.O. = Wheel Order. The order of the three moving wheels in the machine.
3. T.O. = Turn Over. The turnover of a wheel governed by its right-hand neighbouring wheel.