

TOP SECRET

OT 75

SUBJECT: K Notes
TO : CC, SSA, War Dept.

Report #7 32
3 May 1944

1. Enclosed is copy of Part III of Hut 6 report for week ending 29 April 1944.

2. Cable was sent to you today advising that there had been no 1 May extension of UK D but that the thrice daily stecker change had gone into effect. There was some reluctance to make any suggestions as to the people you have been training on hand SEO. I think it is felt here that if these people now know how to do the job, further training and experimentation at A. H. is unnecessary. However, it is hoped that if they are transferred to other work they will still be available if the extension of UK D does occur before machine methods have been fully developed.

3. The thrice-daily change will introduce a real problem only in rare instances. If the first set of stecker are recovered, messages after the change will produce about 71% correct text (22/26 x 21/25) if there is no error in the indicator. This is substantial enough to enable the necessary corrections to be easily made. The chance of getting a correct indicator is about 35%. It varies slightly depending on whether or not the plain or cipher versions (or both together) contain repeated letters. If a number of messages are available the obvious thing to do is to try them until one is found with no indicator error. If there are only a few and none works "tiddling" can be tried, that is, assume each wheel in turn to be wrong and try it in all 25 other positions. This involves 75 trials and will work unless more than one wheel is off or about 30% of the time. However, 78 trials with an 80% chance of success which will yield only 71% plain text seems less desirable than trying all 150 change possibilities, this being sure to yield 100% plain text. Certainly the latter method is preferable for the 2300 change since this will involve only 54 trials. (Calculations are my own).

4. A decode indicates a prospective change in German Air Force medium grade systems. Its language, as usual, is cryptic and ambiguous. The following represents Hut 3 conclusions with respect thereto:-

"The general implication of this signal would appear to be as follows:-

- a. That the German Air Force intend to introduce a new hand cypher (which one must suppose is a replacement for Double Playfair). The date of introduction lies between the present time and August 1944.
- b. That the cypher involves some kind of specially prepared forms which are complicated to print and once completed cannot be reprinted.
- c. That the cypher is highly likely to involve transposition of some kind."

Encl. - 2 pages

(3)

Walter J. Fried
Capt. Signal Corps

TOP SECRET

ARMY

| |
|-----------------------------|
| DECLASSIFIED |
| Authority <u>NND 963012</u> |
| By <u>SB</u> NAVA, Dala |

20 June 1944

SUBJECT: Miscellaneous Items
TO : CO, SSA, War Dept.

1. Enclosed is microfilm (D-133) covering both paginations of the Tudi 5 book. This was requested in U. S. 174. The Near East section would appreciate receiving a set of blow-ups.

2. A second draft of the cryptographic dictionary is being typed and a copy should be ready for shipment to you within a few days. It is still considered only a draft.

3. In response to U. S. 166 I had a photostat made of the Dicionario Cryptographico (IL 3563). Mr. Exell, the head of the Berkeley St. Portuguese section, volunteered to have the necessary figures written in and to send it to you directly together with necessary charts, tables and instructions for reading all the Forteco systems about which you inquired. All of this material should have reached you before this.

4. Enclosed are a series of photostats covering captured training material on the "Rasterschlussel" together with British comments. As already reported, this system is to be used by both Army and Air Force beginning 1 August 1944. Nothing is known as to whether or not it will replace the Double Playfair in the police traffic. A training course designed to prepare personnel for working on this system was started this morning. It began with a 2 hour talk by Col. Tiltman who reviewed general methods of solving transposition ciphers, traced the history of German field ciphers from the beginning of this war, and concluded with a description of the "Rasterschlussel" and a discussion of possible methods of attack. The training program is to last about 10 days. Several of the people from Col. Bicher's London group are taking the course. It was interesting to note that the field cipher used by the Germans at the very outbreak of the war was similar in some respects to the "Rasterschlussel". It used a 13 x 13 matrix with 3 cells blacked out in each row and column and with a colored or shaded band running from lower left to upper right. Two keys were used, one for transcribing the unshaded portion and the second for the subsequent transcription of the shaded portion. The indicator showed the point at which inscription started and the columns first to be transcribed. These were different for the two keys but in each case transcription proceeded cyclically from the starting column chosen. Playfair superseded systems of this type on 1 February 1940 and with various changes and innovations has dominated the medium grade field ever since. The big unknown factor about the "Rasterschlussel" is the matter of distribution. If each stencil is widely distributed it will obviously be a great deal easier than if each division has its own. It now seems quite definite that the stencil will change daily.

Encl. - 1 microfilm
Photostats

Walter J. Fried
Capt. Signal Corps

**Difficulties in the Supply of Rasterschlüssel
to the German Forces.**

1. Raster, the new stencil handkey, which was to replace Double Playfair on August 1st as the standard handkey of the German Army and G.A.F., is both easy to work and difficult to break. From the first however the German authorities have been worried about the difficulties of manufacturing and distributing the cipher material.
2. During April, before the decision to introduce Raster was mentioned, a widespread investigation was held into the possibility of curtailing handkey requirements. The references intercepted were from Western Germany and France, but the survey may have been more general. An instruction from Luftgau XXX on May 1st that stations with only one cipher machine would continue to be allotted the handkey, would appear to be relevant.
3. The first explicit mention of Raster emphasized the supply difficulty. It was a Red message of April 26th, as follows:-

To Gen. Kdo. I Flakkorps Nafue,

1) It is not possible to provide a reprint of keys in the new handkey procedure (Raster) about to be introduced 2) A suitable stock is, therefore, to be maintained at Luftflotte and Luftgau Kdos in case of demand. 3) Handkey requirements according to the latest reckoning are to be reported on May 2nd. Indents at increased requirements rate, will owing to the special circumstances of production only take effect after a quarter ((three months)) e.g. an increase in an indent ordered in May cannot be supplied till August.

OKL, Gen. Nafue 2 Abt. IV C Marstall in 10229/44 geheim.

4. On May 9th a message from Luftflotte 3 to Fallschirm AOK 1 referred to the overburdening of the Geheimschriftstelle of Gen. Nafue caused by P AOK 1's large indents for keys especially handkeys. While there is here no explicit reference to Raster, the message is of considerable interest as indicating a possible bottleneck in the manufacture of keys.
5. The cipher material required for training seems on the whole to have been distributed adequately. One division in Italy, probably 3 Panzer Gren. Div., complained on June 29th that adequate training had been impossible. P/W's of the signals trupp of 709 I.D., captured at Cherbourg, said that they received no training in the use of Raster. But a large number of returns stating that training was completed were sent early in July mainly from G.A.F. stations in Germany, France and the Low Countries, but also from other stations including Army stations in the West and elsewhere. There is little doubt that, in general, training was completed up to schedule and practically all signals personnel will be ready to use Raster on August 1st.

SECRET

| |
|------------------------|
| DECLASSIFIED |
| Authority NWD 96 30 12 |
| By SB NAVA, Dala |

SECRET

IL 3628-A
Report #7-64
Page 11

6. To all appearances, the distribution of operational Rasterschlüssel was progressing satisfactorily early in July. From various references on Western G.A.F. networks it appeared that keys were already with Luftgau or Korps and were being handed out to their ultimate users. On Italian army networks divisions were asking at the end of June for their business Raster keys. The usual dates for key distribution are from the 15th of the month preceding use. P/W evidence suggested that the keys for August, September, and October had in some cases been distributed to divisions in Normandy before the middle of June. However there were hints that distribution difficulties had not been entirely overcome. An instruction from OKL authorized these Luftflotten and Luftgaue, which had been in the habit of preparing special handkeys for certain subordinate networks in their area, to continue preparing them in the old form for August, as it would be impossible to supply the stations concerned with Rasterschlüssel before September.

SECRET

| |
|-----------------------|
| DECLASSIFIED |
| Authority NND 96 3016 |
| By SB NAVA, Dala |

7. The signs of serious supply difficulties appeared quite suddenly. On July 7th an instruction from Jagdkorps II stated that where Schluesselblocks ((the transparent form sheets on which the messages are encoded)) could not be delivered in sufficient quantity through the usual supply channel (Nachschubweg), stations were to obtain through stationery office, (Verwaltung Nachschubweg) transparent paper to be used for the same purpose. On July 10th a department of Feldkommandantur Rouen sent a message in Nightjar to a department of Befehlshaber Nordwest, asking where Schluesselblocks could be obtained. On July 11th Flakkorps III asked Gen. Hafue Marstall for 400 Schluesselblocks, which Nachschubdienst could not supply before September. On the same day L.N. Abt. IV/212 told 2 J.D. that it was unable to get Raster (corrupt) for Raster cipher material before September 1st, and Militar Befehlshaber Frankreich stated that on the authority of Thekla (O.B. West) Raster would not come into force on the West till September 1st.

8. It is clear that the Germans from the first expected difficulty in the compilation, printing and distribution of Rasterblocks and the printing and distribution of Schluesselblocks and that it is this second problem that seems to have temporarily defeated both G.A.F. and German Army authorities.

It would, however, be unwise to assume that the postponement is general or even to put too absolute a trust on postponement in the West.

Distribution:

SIXTA 17/7/44.

Lt. Col. Blair-Conyngame, Main Building.
Major Brown, Block F.
Mr. Milner Barry, Hut 6.
T.I.S.2 (Mr Parker), Hut 6
W/Cdr. Ceser, Hut 3.
Mr J. Cooper, Block F.
Mr H. Edwards, Block F.
Major Gadd
Major Wills } SIXTA
Mrs Whitfield-2)
Prof. Vincent
Mr. Welchman
Major Babbage

SECRET

| |
|----------------------|
| DECLASSIFIED |
| Authority NND 963016 |
| By SB NAVA, Dala |

SECRET

IL 3571
Report #P-72
6 August 1944

SUBJECT: Miscellaneous Items
TO : CO, SSA, War Dept.

1. Cricket is the only GAF key which has thus far gone over completely from Playfair to Raster. One other GAF key has used some Raster but more Playfair. Repetition of old Playfair squares on other keys leads to the belief that they are just marking time, waiting for Raster to be introduced. There has been no appearance of Raster whatever in Army or Police traffic or on other Air keys except for practice messages which have been enciphered on the captured stencils. A few very satisfactory bits of intelligence have, however, been gleaned from this practice traffic.

2. There have, as yet, been no Raster solutions. Work is in progress on some re-encodings but the texts are doubtful due to variations in punctuation, abbreviations and use of cover names. A re-transmission of an unreadable message is also available for study. It shows significant repetitions but there are slight discrepancies in the letter count. Also, unfortunately, it seems as though the errors in the first transmission were substantial rather than trivial.

3. SSA 2499 has just been received. When a reference to Hagelin Cryptograph Type B 211 appeared in the traffic the ISK section studied Mr. Friedman's paper on the analysis of this machine. They are fairly definite, however, in their conclusion that the new machine (which is called # 41) is not the B 211 or an adaptation thereof. It is still being used only for practice traffic and the total material on hand is now about 12,000 letters.

4. I have finally had an opportunity to take up, with the head of the Near East section at Berkely St., Dr. Oliver's notes of 13 May 1944 (Annex A to Monthly Information Letter # 1). The only things that require comment are that Dr. Oliver is quite right in the correction he makes in paragraph 6 (his # 6) and that the French code used for SYA is an adaptation of "SITTIER". I understand that "SITTIER" is a well-known French commercial code containing 100 pages of 100 groups each. New values have been inserted throughout the book and as a result it has been expanded to 115 pages.

5. Supplement of 17 July to Monthly Information Letter # 3 states in paragraph 15 that I "have by now received the Edgerton book on French system identification" and that a new edition is attached as Annex K. The new edition is much appreciated but I never received any prior book.

6. The Bulgarian questions contained in Annex D to the foregoing supplement have been submitted and I will advise shortly as to what information is available.

7. The remaining paragraphs of this report deal with matters covered by Monthly Information Letter # 3.

SECRET

DECLASSIFIED

Authority NND 96 3816

SECRET

VI-3705
Port #P-76
15 August 1944

SUBJECT: Miscellaneous Items
TO : OO, SEA, War Dept.

1. The answers of the head of the Berkeley St. Bulgarian section to the questions contained in Annex D to Supplement to Monthly Information Letter #3 are as follows:-

- "(1) Discriminant 99911 is used in front of traffic between Sofia and Stockholm and Sofia and Ankara. Discriminant 01313 is probably a mistake for 31313 which is the same as 33311. Discriminant 20201 is used in front of traffic between Istanbul and Sofia and Edirne and Sofia. I know nothing of discriminant 82202.
- (2) Very often no discriminants are used in cases where the particular code in use is well known to both parties concerned.
- (3) The A pagination for 99911 is quite correct.
- (4) The discriminant 44422, as used recently in traffic between Sofia and Budapest, indicates a new code (with a different pagination from the old 44422). This has not yet been solved.
- (5) I cannot give any further information on this point."

2. Apparently you are studying some of the less important Bulgarian systems. My previous reports have covered only the 4 principal systems. Even though they are not reading the traffic I am sure the British have some information on the minor systems such as pagination sequences and probably some identifications. If you will let me know which discriminants you are working on or would like to work on I will try to send you whatever data is available.

3. The use of Master has not yet increased. One stencil has been reconstructed from 2 re-encodings and a few messages have been placed. The recovery of the row and column co-ordinates and indicator encipherment keys is laborious and is being done simply by setting messages which use the recovered stencil. Speedier setting techniques are being sought.

Walter J. Fried
Capt. Signal Corps

SECRET

SECRET

IL 3729

Report #P-79

28 Aug. 1944

SUBJECT: Rastorschlüssel
TO: GO, ECA, War Dept.

1. The GAF has gone over entirely to Raster both on the Western Front and in the Mediterranean theatre. The only Playfair still on the air comes from some units isolated in Brittany. Cricket started using Raster on 1 August. Snowdrop and Cockroach switched to it on 11 August and within the next few days all other keys gradually went over.
2. The Western Army will not start using Raster until 1 October. The plans of the Mediterranean Army are unknown. Police traffic is definitely going over to Raster also but the date is unknown.
3. The August stencil pad for Cricket has been captured. It reached here on 19 August but since a substitute pad was used beginning 17 August the date of capture was probably about the 16th. All Cricket traffic for the first 16 days of the month is being deciphered for the purpose of studying habits and errors.
4. Up to the time of this capture 30 messages had been set on the reconstructed stencil (Report #P-76). This was found sufficient to effect almost complete recovery of the row and column co-ordinates and the indicator encipherment table. All identifications were confirmed by the capture.
5. No additional stencils have been recovered. A few re-encodings are available and these are being worked on. Brig. Tiltman and the Research Section are now studying this problem. They are trying to develop methods for stencil recovery which do not rely on re-encodings.
6. Copies of your two papers on setting messages were received here a few days ago and I had a chance to read them yesterday. The crib method seems fairly rapid but this traffic is not stereotyped and the method cannot have a very wide application. The other method, in my opinion, is too slow to be practical. About 10 days ago I suggested a procedure which I feel would be a great deal quicker and simpler. It involves direct utilization of the spatial relations of the stencil whereas your method proceeds through an analytic approach to these relations. I enclose a brief description of my suggestions.

Encl.

Walter J. Fried
Capt. Signal Corps

SECRET

DECLASSIFIED

Authority: NND 96-3846

Method for Setting Easter Messages on Known Stencil

1. When stencil, transposition key and numerical key are known, there are 240 possible starting points with an average of $2\frac{1}{2}$ initial transcription columns for each. A rough estimate is that by the method described below a team of 2 people (one of whom must be able to recognize German plain text) should be able, after some practice, to test all positions in about 2 hours. The average time will thus be about 1 hour, or less if bad habits develop in the selection of starting points. Of course, if either starting row or column is known, the problem is comparatively simple. It is assumed that neither is known.

2. The method will first be described as a pure pencil and paper method. Assume the miniature stencil of Fig. 1 with the transposition key shown, an English message of length 37 the cipher text of which is written double length on the annexed strip, and a numerical key of 7. The rows of the stencil are lettered for purposes of reference and the red line shows the end of the message if it starts in cell a4.

3. The top row of Fig. 2 assumes that the message starts in cell a4 and shows the 12 stencil columns laid out horizontally. The lengths of the blocks represent the numbers of white squares and they are arranged in numerical sequence. The cells marked 1, 2, 3, 4 and 5 in red represent the positions of the plain text letters in row g. For this assumption column 6 must be the initial transcription column. If, therefore, the cipher strip is placed against the top row of Fig. 2 so that the cipher text begins at the first cell of the 6th block the letters opposite the numbered cells must come from row g. KRVID disproves the assumption.

4. We next test a2 as the starting point. The second row of Fig. 2 now represents the columns. The only change is that block 4 has been shortened by one cell and block 11 lengthened by one. However, either column 3 or 10 might now have been the initial transcription column so the initial letter of the cipher strip must be tried against the first cell of both of these blocks. REAIN and LNKLM are yielded and the assumption is disproved.

5. The third row of Fig. 2 represents the testing of a1 as the assumed starting point. Block 2 had to be shortened one cell and block 6 lengthened one. The top row of Fig. 3 is the sequence of columns containing white cells, from upper left to lower right. By sliding this sequence against itself, a number of places equal to the message length (bottom row) we produce a table which shows the blocks to be shortened (top row) and lengthened (bottom row) as successive assumptions are tested. When a block containing one of the red numbers is lengthened the additional cell must be added to the right of the number; when it is shortened the cell must be taken off from the left.

6. We finally get to c10 (fourth row of Fig. 2) and find plain text based on the assumption that column 2 is the initial transcription column. This means that c6 was the true starting point. 5 letters are probably too few with which to test for plain text but in the actual case

SECRET

IL 3729

F-79

Page 3

10 would be available from a single row. Only enough of them to disprove the assumption need be used. The reason row g was selected was that this involves a minimum of changing of the red numbers. Only after we start testing starting point assumptions in row g do we have to shift to some other row in which to look for plain text. In general it would seem best to start by taking the last full row although it may prove more useful to try to use beginnings or endings. This would involve a little more manipulation of the red numbers.

7. With some very simple equipment it should be possible to make these tests rapidly. All that is needed is a series of strips made of wood, glass or some other material, cut accurately to integral multiples of some unit length. The multiples should range from 1 to the maximum number of white squares in any column of the stencil. (Actually the maximum is lower because of the limitation of message lengths to 200 letters.) Presumably $\frac{1}{2}$ " would be the unit length selected so that the longest strip would have to be about 4" long. A channel would be needed to hold these strips and it should be marked off in $\frac{1}{4}$ " units so as to provide a check on the placement of the strips. Markers sliding along the channel would be useful to designate the block positions. A series of compartments to hold the wooden strips and possibly a frame, through which the cipher strip could be slid along adjacent to the channel, completes the list of necessary apparatus. The red numbers would be written directly on the strips and erased and rewritten whenever necessary.

8. The principal advantage of this method is the simplicity of the operations necessary to proceed to test the next assumption. The principal disadvantage seems to be that for long messages 4' of channel would have to be used and the cipher strip would have to be 8' long. Division of the channel into a number of segments would probably consume more time even though it would make the manipulation less awkward.

SECRET

DECLASSIFIED

Authority: NAD 96 3846

SECRET

L 3773
report #F-86
3 September 1944SUBJECT: Rasterschlüssel
TO : CO, SSA, War Dept.

1. Both Police and Italian Army went over entirely to Raster on 1 September.
2. About a hundred captured stencils have reached here and more are on the way from the field. Decoding traffic covered by these captures has proved quite arduous. The Germans make many mistakes and a lack of clarity in their original instructions adds to the confusion. In the illustrative example a black square was chosen as the starting point and inscription started on the next white square. When a white square is chosen inscription should start in the indicated square but some operators use the following white square. Not only does this add to the labor of reading on captured stencils but it also increases the difficulties of setting on reconstructed stencils, there being 840 possibilities instead of 600. Since the place name substitution alphabets are printed on the backs of the stencils it was expected that different alphabets would be used every day. However, the alphabets are the same for an entire pad, that is, they remain unchanged for a month. Furthermore, each user is apparently instructed which alphabet to use and employs one of them exclusively.
3. About 5 stencils have been reconstructed by cryptanalytic means. All solutions have been based on re-encodements. A single re-encodement is usually insufficient to give an unambiguous solution and methods are being developed of tying up crib messages with the re-encodements. Similar methods are being experimented with on groups of messages with good cribs in an effort to select pairs or larger groups of messages which start at approximately the same position. The Police traffic is not expected to produce as many re-encodements from other readable systems as are found in the Air Force traffic; on the other hand the crib situation is somewhat better.
4. Setting techniques are still in an evolutionary stage and a number of different procedures are being tried. Messages with only 1 or 2 Z's and W's can often be set using ZWO as a crib and this is about the most satisfactory method yet found.
5. A tendency to start messages in the upper left-hand corner portion of the stencil is clearly discernible. A study of the transposition keys shows that they are hand made and by a very lazy person. Many of them are nearly identical and there are a number of reciprocal pairs. However, by far the most important weakness of the system was discovered a few days ago. All stencils thus far seen (including the practice ones) employ only 36 different rows. Printing imperfections make it evident that only 36 master strips have been made. Each stencil is a different selection and permutation of 24 of these. The row patterns never contain more than 4 successive black squares except at the beginning or end of the row where the limit is 5 and they never contain more than 3 successive white squares. 23 lines of the stencil printed in the instruction booklet are taken

SECRET

SECRET

3778

Report #F-86

3 September 1944

Page 2

from this pool of 36. The other line contains 5 black squares in the middle of the line and was probably eliminated for this reason. It is not yet known whether the Police and Italian Army stencils are based on the same 36 patterns although it is significant that the Police practice traffic reads on the same practice stencils. It is also not yet known whether the September row patterns will be the same as August. This limitation should help substantially in stencil reconstruction and consideration is being given to the best methods of exploiting it. It may very well be possible to use IBM methods for trying combinations of rows and will almost certainly be possible to use IBM to construct various types of useful catalogues.

Walter J. Fried
Capt. Signal Corps

CLASSIFIED
WJF 9c 30-16
NADA, DIII