BP’s Notes on the Enigma Uhr

by

Sir Stuart Milner-Barry et al.

Introduction

These notes describe Bletchley Park’s (BP) discovery of the Enigma Uhr, an attachment for the German cipher machine Enigma. The notes have been found among the reports that US Army Captain Walter J. Fried wrote while he was at BP on liaison duty. The notes that are presented here are parts of the Fried Reports F-62, F-64, and F-112. The first two pages have been written by Captain Fried while the others have been compiled by the BP cryptographer Sir Stuart Milner-Barry. The last page is signed M.A.C. This is most likely Malcolm Alfred ("Mac") Chamberlain, who was in the Hut 6 Research Section from June 1943 to September 1944. The Hut 6 Research Section would have handled the Enigma security enhancements, Enigma Uhr and Umkehrwalze D (UKW D), that the Germans introduced during this period.

Source: Capt. Walter J. Fried Reports / SSA Liaison with GCCS,
RG 457, Entry A1 9032, Box 880, NR. 2612,
NARA, College Park, MD.
https://catalog.archives.gov/id/2809159

URL: https://cryptocellar.org/enigma/files/bp-enigma-uhr.pdf

Editor: Frode Weierud, Crypto Cellar Research

Copy 8 of 8 copies

IL 3619-A
Report #F 62
13 July 1944

SUBJECT: E Notes
TO : CO, SSA, War Dept.

1. Enclosed is Part III of Hut 6 report for week ending 8 July 1944.

2. Enclosed is document about the Red compromise, referred to under caption "General" in the foregoing report.

3. Enclosed are minutes of 17th meeting of UK D committee.

4. Enclcsed is Hand Duenna pamphlet referred to in paragraph 6.5 of the foregoing.

5. UK D ~~17~~ 19 (effective 11 July) is as follows:- A/D, B/O, C/T, E/X, F/N, G/Q, H/V, I/W, J/P, K/U, L/Z, M/S, R/Y.

6. The UK couplings set forth on the captured Red key referred to in my GCCS 3216 are not the same as those recovered here but are, of course equivalent. The fixed coupling which is not shown on the key is J/Y. The lettering used on the actual UK D apparently proceeds in a clockwise direction instead of counter-clockwise as had been assumed. If a normal alphabet (omitting J and Y) is written out for the true values, the English equivalents can be found in a reversed standard alphabet (omitting B and O) placed below it with A against A. It is planned to continue using English notation. The fixed coupling actually must connect points 13 apart and its contact points must lie between M and N and between Z and A on the true wheel. J and Y are simply 2 letters arbitrarily chosen for omission from the sequence.

7. A new device or procedure, which the Germans call "Enigma Uhr", has just been adopted on some of the Air keys. It was discovered because it is not yet in general use even on those keys which have started to employ it. Some messages were observed which decoded to yield a number and then nothing but gibberish. Through a re-encodement (after an exchange of messages which showed that one of the correspondents did not yet know the "Uhr" procedure) it was determined that the plain text following the opening number is first monoalphabetically enciphered with an alphabet which is usually non-reciprocal, that the resultant text is next enciphered on the steckered machine, and that the text produced by the machine is then monoalphabetically deciphered with the same alphabet (or enciphered with its inverse). The opening number seems to indicate the substitution alphabet to be used. Indicators decipher normally. It seems unlikely that a hand substitution process is employed. The effect could be obtained by changing the designations of both key-board letters and lights according to the same substitution or by introducing an additional non-reciprocal stecker (which is the same thing). With existing equipment it could not be produced by a mere change of stecker because the alphabets are generally non-reciprocal. The 6 letters

that are self-steckered in the key continue to be so, that is, they go to themselves in the substitution alphabet. A better way of putting it is to say that the substitution alphabet consists of only of the 20 steckered letters. This limitation certainly seems to indicate a mechanical or electrical procedure and that the substitution is based in some way on the key for the day. Efforts to find relations between the alphabets have yielded results but have not yet led to a satisfactory theory or a mechanical explanation. A multi-part message has been read which uses differed substitutions for the 2 parts. Enclosed is a note of Mr. Milner-Barry's on the new procedure together with instructions as to changes in routine. The procedure is too new to draw any conclusions as yet or to speculate on implications.

Walter J. Fried
Capt. Signal Corps

Encl. - 3 pages
1 page
2 pages
4 pages
3 pages

Copy of 8 cop

SECRET

IL 3619-A
Report #F 62
13 July 1944

ENIGMA UHR.

A new device for making life more difficult has suddenly been introduced by the Germans on some of the Western Front Air keys, particularly Jaguar and Cricket. It is not yet very widespread; about one in seven Jaguar messages seem to be affected, and fewer Cricket. We do not yet know very much about, but what happens is that a message starts with a number and then goes off into nonsense. We have broken into some of this nonsense, and have proved that some substitution table is employed in conjunction with the basic enigma key. The number with which the message starts off tells the Germans which particular substitution table is to be used; there seem to be at least forty of them every day, but may be more. It is thought probable that, rather than perform the substitution by hand, the Germans have some kind of gadget attached to their enigma machines, which can be adjusted to the right position for each table and perform the operation automatically.

We shall doubtless find out a lot more about this new development in the course of the next few days. The amount of traffic involved so far will not seriously diminish our output, nor should our chances of breaking be much reduced. If the bulk of any key or a complete key were to go over to Enigma Uhr, it would be a major complication:. there is however noreason at present to suppose that we could not cope with it fairly effectively, although breaking and decoding would inevitable be slowed down. In the meantime the first thing to do is to make routine arrangements for the orderly handling of the problem, and these are outlined in the attached note. Alterations of procedure will be published as necessary, together with more information as we acquire it.

P.S.M-B
12.7.44.

ARMY

Copy of 8 cop

IL 3619-A
Report #F 62
13 July 1944

ENIGMA UHR.

Routine for dealing with messages encoded with Enigma Uhr.

For the present the following procedure has been agreed upon:-

1. The D.R., upon finding that a message begins with a number and then goes off into nonsense, will

a) Mark the message with a "P".
b) Decode the rest of the message.

Note. It is important that this decoding should be done accurately, because this will be a great help for breaking purposes. Since what comes out will be nonsense, there is no means of checking readily that the decoding has been done accurately.

2. "P" messages will be passed through in the ordinary way to the R.R.l. tickoff girl. She, instead of writing "Dud", will write "P" against the blist number on the tick-off and pass the message through to the Duddery e.p.er.

3. The Duddery e.p.er will not e.p. the messages at this stage. She will keep them in a tray which will be collected for further registration by the Qwatch party.

4. "P" messages will be re-blisted by one or more R.R.l. girls in the Qwatch. There will be one "Plist", corresponding to each Blist. The Plist will contain the original Blist number plus all further details given in the original Blist. It will also have on the extreme left against the registration number the German number with which the decode starts off. This indicates which particular substitution table is being used.

5. Also in the Qwatch will be a party (at present two per shift by day and afternoon and one by night) who will be engaged in attempting to break the various substitutions. This party will consist of cryptographic or M.R. personnel. Since this unexpected development leaves us rather short of skilled personnel to deal both with our normal work and with the Enigma Uhr, it is important that the people who are not involved in the Enigma Uhr party should concentrate upon normal routine breaking, which must not be allowed to suffer. Captain Bundy will for the present be responsible for co-ordinating the work of the Qwatch party.

6. When the Enigma Uhr party breaks a substitution it will be possible to decode any other messages on that key on the same day, e.g., supposing that a Jaguar "P" message is broken, carrying the German number 27, then any other messages on the Jaguar Plist for that day carrying the number 27 can be decoded. These messages can then be taken back by the R.R. girls to the D.R. to be decoded. Having been decoded, they will be put through to the tick-off girl who will put a tick against the original "P" entry, to show that the message is out. The message will then go through to be e.p'd by the Duddery

and the Watch e.p.er in the ordinary way.

7. It will be the responsibility of the Qwatch party to see that the D.R. are given the substitution key in an unambiguous form.

Enigma Uhr Research.

It is necessary that in addition to the routine breaking of each substitution key by known methods (R.E's and Cribs) special research work should be undertaken in order

a) to determine the most practical technique for breaking without cribs.
b) to investigate the relationship between the various substitution keys, and to examine all other relevant evidence.

Arrangments will be made to free one cryptographer at least for this work, either from Watch or Research.

T.I.S.(1). Analysis and Records.

It is the responsibility of T.I.S.(1) to analyse the "P" messages in order to discover the distribution and use of the Enigma Uhr. These results as they become available should be reported by T.I.S.(1) to the Qwatch part.

P.S.M-B

Distribution:

G.B.
Heads of Rooms.
D.O.
Captain Fried.
3L.

ENIGMA UHR

Hut 6,
Block D.

A short non-technical account of this episode may be of some interest to the layman. A proper technical paper is being prepared and will be available in due course to anybody who would like to go further into its intricacies from a scientific standpoint.

The most surprising feature of the story is that this new gadget - apart from the short-lived Uncle Charlie and Uncle Dick, the only alteration in the actual Enigma machine introduced by the enemy during the whole course of the war - was sprung on us with no warning whatever. With the exception of the change in the indicating system brought in during May, 1940, this is the first occasion on which we have received no prior notice of a major change from source - though on several occasions the warnings have been either fragmentary or highly ambiguous. The first we knew of this new horror was the actual receipt of a number of messages on July 10, which began with a number and then went off into nonsense; together with a decode which referred to certain messages being encoded with "Enigma Uhr", whatever that might be.

It was clear at once a) that the nonsense represented a code within a code, i.e. that some process of re-encipherment had taken place, and b) that a number of different codes must be in use, the particular one applicable to a given message being given by the number encoded at the beginning. The first thing to do was to try and break into one or more of these nonsense messages and see what kind of a code was involved.

This proved not to be very difficult. It soon appeared probable from an examination of the decoded nonsense that the substitution which had been imposed was not complete. The Fusion Room were prompt in producing a reencodement between a message which had been encoded in plain enigma and a version transcribed in Enigma Uhr, and with the assistance of this it was a relatively simple matter to break into that particular message and get out the code represented by the number at the beginning. It was then found, as would be expected, that any other message carrying the same number would decode on the same substitution, and also that the self-steckered letters in the fundamental enigma key remained unaltered.

So far, so good. The next question was whether the substitutions were performed by hand, according to a series of tables which would be printed beforehand, and which might well be changed every day and possibly even be different for each separate enigma key; or whether the Germans had fitted some extra gadget to their machines which would produce the substitutions automatically.

For a number of reasons the latter hypothesis appeared far the more likely. First, the name "Enigma Uhr" in combination with the numbers suggested some kind of clock face or dial, possibly with a hand or knob which one could set to the desired position. Secondly, the leaving alone of the unsteckered letters, together with the fact that only forty codes were in use (the highest number seen was thirty-nine) indicated pretty strongly that there was some intrinsic connection with the ten pairs of steckered letters. Thirdly, if the substitutions for encoding and decoding had to be performed by hand, it would be an intolerable nuisance for the German operators and must seriously delay the handling of messages.

This again was not very difficult to prove or disprove. If it was a hand process with arbitrary substitutions based upon tables, then one could not expect to find any relationship between one code and another. This would have been a serious matter, for it would have meant trying to break forty different tables per key per day (assuming different codes for each key, and a different edition every day), with no hope of ever shortening the process. If on the other hand some mechanical device was responsible, one would expect to find certain relationships between the various codes. One might hope, further, in due course to accumulate sufficient knowledge of these connections to be able, given one code or a number of codes, to deduce the remainder. Finally, one might be able to work out what kind of an apparatus it would have to be to produce just these peculiar patterns, and in due course to reconstruct and build for ourselves a model of the Enigma Uhr itself.

It was plain after a very few codes had been broken that there were, in fact, various kinds of peculiarity that would be accounted for by a mechanical device. The discovery of the exact nature of the connections and their precise significance, however, was far from being easy. It was an ideal problem from the cryptographer's point of view, and must have been fascinating to solve. It was also entertaining for the spectator, since the outcome could be awaited without anxiety: for it was evident that, whatever the exact nature of the new horror, and whether or no the cryptographers would be able to get completely to the bottom of it, it was not of a character to threaten us with disaster, or with anything more serious than acute inconvenience.

For about 48 hours, the Qwatch, where the operations were being conducted, presented an appearance reminiscent of a rugger scrum, or alternatively of an assembly of chess masters conducting a post-mortem after an important game. Most of the participants (who included a strong contingent from Hut 8) appeared to play non-stop throughout the period, and several of them deserve an international cap. Eventually a completely satisfactory solution was found, which puts us in the happy position that we have now to break only one of the forty codes in order to deduce all the rest; and that, all being well, it should not be too difficult to build and attach to the D.R. machines mechanical contrivances which will do just what the Germans' does. This will save the necessity, under which the D.R. at present labour, of having to plug up to forty sets of stecker boards every day for each key. This is bad enough for Jaguar only, but would be intolerable if a large number of keys were involved.

CONCLUSION.

The only key seriously affected is Jaguar, on which about half the messages are encoded with Enigma Uhr. There is a little on Cricket, and even a Red message combining Uncle D and Enigma Uhr has been seen, which seems a gratuitous complication. We nowknow on Jaguar exactly who has this toy and on what messages it will be used, which is a great convenience for identification and breaking. There is clearly no reason why its use should not be widely extended to other keys, but it is also most unlikely that it is the kind of gadget that could be attached to the ordinary hand enigma. One may expect, therefore, that the use of Enigma Uhr will be confined to main stations possessing big electrical machines. In that case it is unlikely, though not impossible, that a key would go complataly over to Enigma Uhr.

Finally, the effect on the breaking position. At present, though a number of Jaguar cribs are now encoded with Enigma Uhr, there are a sufficient number still encoded in the straightforward way to enable us to break in the normal fashion. It is, however, quite possible to break on the bombe using cribs that have been re-enciphered. The main difference is that cribs have to be longer and menus stronger, and that there is considerably more difficulty about completing the key after the bombe has given the correct stop. There is also the nuisance that the unknown number encoded in front has to be allowed for, which means in effect allowing for a wahlwort of from three (e.g. Zwo, aqt, elf) to ten (e.g. einssieben) letters. However, a crib of the required length would hardly go through in more than one or two positions, so this is not a serious additional complication. And recovering the wirings of Uncle D by Duenna or hand Duenna is unaffected. Even, therefore, if a whole key or all keys were to use Enigma Uhr, we ought still to be able to break any of them on which reasonably long cribs were available.

P.S.M-B.
17th July, 1944.

Distribution:

Director.
D.D.1.
Professor Vincent.
A.D.(Mch).
G/C Jones.
Lt. Col. Taylor.
D.O. Hut 3.
Major Leathem.
W/Cdr. Rose.
Mr. F.L. Lucas (2)
No. 1 ABCD, Hut 3.
No. 1 E "
No. 1 F "
3L (2).
C.B. Hut 6.

All Rooms, Hut 6.
D.O., Hut 6.
Sixta.
Captain Fried.
Lt. Machus, U.S.N.
Mr. Hinsley.

HUT 6 REPORT

Week ending Saturday, November 4th, '44.

There is not much to add to the summary which I issued on November 3rd. The Air section took the turn of the month in its stride, and the three keys unbroken on the 3rd, Gadfly, Yak and Beetle are now also well in hand. In fact the general Air position is for the moment so satisfactory that there is little call for detailed comment. The following are a few points of interest.

The absorption of Ocelot, a quite unexpected blessing, strengthened the crib position on Cricket, and, more important, on Jaguar, where the announcement that the Abdulla Fag (Gefechtsverband Hallensleben) was to use Uhr had caused some consternation: for last month's Jaguar was broken almost solidly on cribs from this unit. What exactly has happened to Hallensleben is far from clear. A number of possibilities have been disproved, and the two most plausible hypotheses remaining are a) that the key in use is Cricket with both Uncle D and Enigma Uhr and b) that it is using some key of its own, with Enigma Uhr and with or without Uncle D. Unless we can recover the Cricket Uncle by some other means (and this seems unlikely, since it is not at all clear that D is in use anywhere else in the Cricket field), the testing of the first hypothesis is very laborious and involves calling in Mr. Freeborn. The testing of the first part of the second hypothesis - a new key with Uhr and Uncle B - is in progress, though almost equally laborious.***

From our point of view Lily this month has taken the place of Snowdrop. The chief content of Snowdrop last month, and of Lily this, was the reports of a Recce Unit, F123. Last month these reports were sent in the key of Luftgau V, this month he has been told to use that of Luftgau XIV and is doing so. It is not clear why he does not use Red, like other Recce Units. The residual genuine Luftgau traffic on either of the Luftgaue is negligible, so we have probably said goodbye to Snowdrop for this month.

Daffodil alarmed us by producing a message which, in conjunction with a previous reference, seemed to suggest that the encoding of callsigns was coming into force on the 5th. On closer examination calmer counsels prevailed, and it was thought much more likely to refer to a local change of funkplan in the area concerned. This explanation received confirmation when the unit failed to appear on the 5th, presumably because of a change of frequency. There is also far too much talk of Uncle D on Daffodil, one subscriber indeed enquiring somewhat bitterly why his colleagues were not using D, as he had in accordance with instructions fitted up his machines with it; he was going back to B until further notice. Altogether Daffodil continues to keep us in a highly nervous condition.

It is clear, in fact, that a further widespread distribution both of D and Enigma Uhr is taking place, but apparently it is not yet complet

In the Balkans, the chronic key muddle still persists in November. Yak is using two keys, one new one (actually introduced at the end of October) and the September key in day for day order (last month this key was used backwards). This suits us very well, as there are always chances of reencodements between the September key which is automatically out and the new one. (Later). The Yak of this month is now found to be a partial repeat and rehash of the September key, which is better still.

Gadfly is using a fine variety of old keys; fortunately the great bulk of traffic is being sent in the key which was introduced about the middle of last month. A new key will replace this one on the 17th. The odd traffic is chiefly a headache to the Duddery.

Mosquito is now in very healthy shape, and there seems no reason why, if bombe time is free and more urgent calls on cryptographers' time permit, we should not make a fairly clean sweep of the missing October days. In this sector Ermine too (key of Fliegerkorps I) is coming along nicely, though it does not look like being breakable as a matter of routine. That leaves us with Skunk (Fliegerkorps VIII), which reemerged last month and on which the Qwatch is now beginning to cast a threatening eye. Its safest course would be to disappear again. Beetle (Luftflotte 6) gave a bit of trouble at the beginning of the month. Its standard and castiron crib said "Geraeteklarmeldung alles gruen", which started to go down and also to crash. Fortunately the first word is quite long enough to run in its own right, and when this was done it was discovered that "alles gruen" had been replaced by "wie gestern" in the same number of letters. After this piece of trickery had been exposed the other days came tumbling out.

In the Scandinavian area the chief cryptographer keeps plugging away at the General der Luftwaffe inDaenemark, still with no luck. As the investigation of callsign encoding may shortly become a full time occupation, it looks as though we shall have to change the bowling; but I hope he will take the General's wicket first.

*** Since these notes were written the mystery of the Abdulla fag has been solved. Neither of the suggested hypotheses was correct. A third, which had been considered but thought less likely, was that the messages were indeed in Jaguar and in Enigma Uhr, but that the use of Uhr had been indicated not, as formerly, by a straight enigma encode of numbers in the first two groups, but by some hidden means, so that the Uhr was switched to its appropriate position before the message began. This would be done easily enough, for instance, by various kinds of jiggery-pokery with the G.T.O.

To test this hypothesis an Abdulla fag dud was taken and tried on all 40 positions of the dial. At position 28 it decoded, not however beginning straight away, but after the first four letters. Similar messages produced similar results, and it was clear that instead of encoding the number at the beginning the Germans were using some kind of substitution code, in which the first four letters always represented one of the forty possible settings of the dial.

Whether the motive of this device is to baffle us (on the grounds that we might be reading the enigma but be defeated by the disguised use of the Uhr) or whether it is an internal security device, it is providential that they did not start off in this way. If we had not had wind of the Uhr, we might well have been completely defeated; for the code, though simple enough once you know what to look for, has plenty of variety and is not of the kind that would strike one in the eye; and with the whole message dud there would have been nothing to direct one's particular attention to the first four letters. As it is, not for the first time, the engineer is hoist with his own petard; for should we now wish to run a crib encoded with Enigma Uhr we have no longer to allow for a beginning anywhere from the fourth to the eleventh letter, but can start off confidently in the fifth position.

As an offset against this, however, the D.R. will not be faced with the awkward riddle "when is a dud not a dud?" - which they can only solve by comparing their first four letters against the table of possible substitutions. This will not matter very much as long as we know which messages are likely to be encoded with Uhr; if any messages were liable to be, it would be a great nuisance. It is some consolation that the Germans must be in exactly the same position.

ARMY

In general it appears that with such of the Army keys - e.g. Albatross, Sparrow, Wryneck, Avocet - as boast cribs the cribs have sufficientl marked characteristics to be picked out without the use of callsigns. Provided, therefore, that interception and identification do not get into too much of a muddle it seems that the cryptographers should be able to get on much as before, if in certain cases with considerably greater expenditure of bombe time. In the case of Puffin, for instance, were there any appreciable volume of traffic, it would be desirable to distinguish between a Heeresgruppe G (good for "Dates-at-end") and OBW (good for "Geheim tails").

So far, at any rate, the stations have made a marvellous job of recognising their groups - not only W.O.Y.G., of whom we expected it, but the Overseas stations too, where it seemed too much to hope for. This makes one wonder whether the leading Air stations, in spite of their greater size and the wider field to be covered, may not after the initial shock be able to make a better job of doing without calls than they now anticipate.

The Army Watch last week broke five Falcon II (two of November) and three Falcon I (one of November). The Falcon II traffic disappeared at the end of the month, and though it has reappeared to some extent the regular routine reports are still missing. In the case of Falcon I, it seems that the log-readers can usually give us the Muenster callsign correctly, and with this we should be able to break at least occasional days. There is another possible line from an old Gannet crib, easily recognised when it comes. There is negligible traffic and no progress to report with other Western front Army keys.

The confidence of the cryptographers in the future of Albatross was fully justified, and no fewer than nine days were broken. Sparrow, too, has recovered well. Seven Sparrow I and three Sparrow II were broken. Sparrow II is the important key, but is more readily broken indirectly, by reencodement from Sparrow I.

The Research party had a thin week, but there is no indication, except in the case of Avocet, that prospects have deteriorated. The Avocet crib, as we feared it might, has incontinently disappeared. In the Balkans it looks as though Wryneck I and II are resuming their proper functions. This means that Wryneck II, the Staff key, will become difficult and expensive again.

The Police keys have not been in their usual form. Quince has hung fire this month, and there is something mysterious about Orange. The last two days decoded very little traffic, and it looks as though some kind of split may have occurred. Further drives on two Roulette days await bombe time in Washington which, now that the normal monthly hold-up on Naval keys has been overcome more quickly than usual, should become reasonably free. Roulette II, which of course decodes on Red, earned unexpected fame by providing a crib that broke an obstinate Red day.

Of the peculiar keys, no more has been heard from the Rocket front. Culverin, which does not encode its callsigns, is healthy; Blunderbuss is not, though much is being tried. It is not helped by unpredictable calls, but had shown signs of deterioration before the first of November. Brown has failed to make its weekly break; it requires more than one message to make a cilli. Similarly Corncrake, pruned of much that was miscalled so, is found to be practically non-existant, though efforts have not been exhausted to break the shadowy remnants. Finally Mustard after a long run of prosperity has fallen on bad times again. The cribs, presumably as a result of the rapid developments in the Balkans, have disappeared; and it remains to see whether anything can be done with the Western Mustard, which unfortunately is all on Uncle D.

The D.R. output has fallen back slightly, and last week was rather under 2100. Actually they probably got through a greater volume of work. A new method of recovering Umkehrwalze wirings without the use of a crib has been discovered, based upon the fixed B/O pairing. This involves the manufacture of what are known as grass skirts by the D.R., a laborious proceeding which can easily cost about 200 messages per shift in decoding time. This week there has been rather a spate of new Uncles (with Mosquito 1/11 we scored our century) and hence the D.R. has been rather handicapped. In general it pays all round to recover Umkehrwalze wirings as quickly as possible, but the pressure on the D.R. is fairly heavy and we must be careful to avoid overburdening them with extraneous work.

D.R. FIGURES

	This Week.	Last Week.
Average No. of tle. decoded in a day ...	1814	1914
Highest " " " " " " " ...	2091	2273
Lowest " " " " " " " ...	1605	1697
Average No. of D.R.s attempted in a day ...	55	59
Highest " " " " " " " ...	109	91
Lowest " " " " " " " ...	22	42
Average No. of tries & Duds attempted in a day ...	988	1070
Highest " " " " " " " " " ...	1142	1425
Lowest " " " " " " " " " ...	905	940

D.R.S. FIGURES

Average No. of teile decoded in a day ...	265	224
Average No. of tries & duds attempted in a day ..	176	200

P.S.M-R.

ENIGMA UHR NUMBERING Mk. II.

After the Cricket-Jaguar-Ocelot tangle had been sorted out on the first, we were still left with some unexplained duds on 3836.

The Morning Erdlage from 5 Jagd. Division came out on Jaguar, but the Evening one and "Intentions" were dud (B and D). Shots were run on these messages as E/3836 without success.

When Abdulla fag was found on the 2nd, this also proved dud on Cricket and Jaguar, and while there was still the faint possibility of Cricket, Uncle D with Enigma Uhr, Abdulla was thought to have a key of its own.

Several cribs were run on E/3077A (Abdulla) and when these failed, a message was tried on all 40 positions of the Enigma Uhr on Jaguar 1st, this Uhr having broken on a straightforward H** message. This was tried in case a new method of indicating H numbers had been used, depending on T/O or some other external method.

This message came out on number 28 and showed up four dummy letters at the beginning which obviously had been used to indicate the number. All the first groups of Abdulla 1st were decoded and the first four letters listed.

From repeats, it was obvious that numbers were represented by bigrams. The second bigrams were all close alphabetically e.g. IJ, PR, ZX, while the first were more scattered, e.g. HM, TY. The idea was then tried of splitting the alphabet into four parts for the first bigram and ten parts for the second bigram.

A little decoding showed that this was correct, and gave the boundaries of each division.

There is no overlapping allowed and the final table is below.

** H = Uhr.

1st. Bigram.

	ABCDEF	GHIJKLM	NOPQRS	TUVWXYZ
No:	0	1	2	3

2nd Bigram.

	ABC	DE	FGH	IJ	KLM	NO	PQR	ST	UVW	XYZ
No:	0	1	2	3	4	.5	6	7	8	9

Distribution

All Rooms, Hut 6.	Capt. Fried
Prof. Vincent	3L.
A.D.(Mch).	Lt. Eachus
Sixta	File (5)

Examples.

BEQR = 06 = FARP.
OSJI = 23 etc.

M.A.C.
7.11.44.