TOP SECRET ULTRA "A"

IR4054
Fried Report #116
17 November 1944
CX/MSS

Subject: Fish Notes
To   : C.O., SSA, War Dept.

1. Enclosed is a seven page mimeographed report on Sturgeon-type ciphers. There is still a great need for a test to apply to cipher text to indicate positively when traffic encountered is Sturgeon. There is still a great need for a statistical method of solution of Sturgeon.

2. The week ending 12 November saw the following Tunny circuits broken:

Whiting - 7 Nov.
Codfish - 2,3,4 Nov.
Stickleback/shad - 1,2,5,7 Nov.
Gurnard - 3,4,5,7,8 Nov.
Bream - 4,7,8 Nov.
Lumpsucker - 5 Nov.

Newmanry rectangling and wheel-breaking broke 10 of the above, cribs broke 1, and depths 6. Total = 17. Of the 10 by Newmanry, 4 were out 3 days after interception; 4,4 days; 1,5 days; 1,6 days. Messages deciphered were:

Gurnard - Berlin, 255. To Berlin, 48.
Bream - Berlin 13, To Berlin, 32.
Lumpsucker - Berlin 12, Rotterdam 12.
Codfish - Berlin, 31. To Berlin, 64.
Stickleback - Berlin, 145. To Berlin, 7.
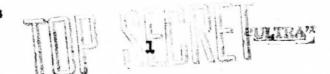Bleak - Berlin, 22.
Whiting - Berlin, 31.
Jellyfish - Berlin, 6.

Messages run were:

	Run:	Set on X wheels:
This week:	440	231
Last week:	231	166
Previous best week:	327	202

Albert W. Small
Cryptanalyst
U.S. Signal Corps

Encl.: 7 pages

1

STURGEON - TYPE CIPHERS

I   Cryptographic Evidence

The first traffic definitely known to be sent on the kind of cipher machine now referred to as "Sturgeon" was sent in the Summer and Autumn of 1942. Most of this passed between Sicily and Libya (the "Sturgeon" link). There was also another transmission from the Aegean to Sicily, which we refer to as "Mackerel."

Both these links had a habit of sending large numbers of cipher passages on the same setting of the machine. A short passage of cipher would be sent, and be followed by some operator's chat in clear. Then the signal "Um Um" would be transmitted, and the cipher message would be continued, with the machine brought back to its initial setting.

These depths enabled us to read a number of messages, and to discover the cryptographic processes carried out by the machine. The most notable characteristics of the machine which were thus revealed were the following.

> (1) There were 10 wheels, whose patterns seemed to be fixed. At any rate they were constant throughout September and October and in the first two days on November (after which the traffic came to an end). In the period before September interception was very bad, and no messages of this period were ever read. All subsequent "Sturgeon-Type" machines known have these same wheel-patterns.
>
> (ii) The periodic keys produced by the 10 wheels were combined, (usually in fours), according to a device known as the "Pentagon" which has been described elsewhere.
>
> (iii) The resulting keys were used to produce:-
>> (a) a subtractor letter Σ , which was added to the clear P to give $P + \Sigma$
>>
>> and (b) a "permutor" π, which determined a permutation of the impulses of $P + \Sigma$ among themselves to give the cipher letter C.
>> $$C = \pi (P + \Sigma)$$
>
> (iv) The "Pentagon" was cryptographically an inefficient device. Only four different subtractors could be associated with any given

permutation. Further, the subtractor letter was always even (i.e. its 5 impulses summed to zero), so that the plain language letter was known to be even whenever the cipher letter was even, and odd whenever the cipher letter was odd. When this was discovered it was of great use in reading depths, and setting cribs. The first "Sturgeon" depth to be read was a depth of 40, but a knowledge of the pentagonal limitations enabled depths of 4 or 5 to be read fairly easily.
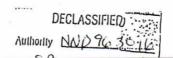
(v) The initial settings of the 10 wheels were constant for a given day. We imagine that this was arranged for the convenience of the operator, who thus had to set his wheels only once a day. We suppose that he could bring them back to the standard daily setting by moving a single switch. This limitation enabled depths of 2 or 3 to be read when the daily setting was known, and when half-a-dozen letters of clear could be guessed (with the help of (iv)) even single messages.

(vi) Different messages were however sent with different wheel orders. Some sort of stecker evidently existed between the wheels and the pentagon. The wheel order to be used was communicated by means of a five-letter indicator.

We observed that the letters used in this indicator were always members of the set P S T U W X Y Z. A letter might appear more than once in the five-letter group. (The indicator W W W W W was once sent.) When two indicators sent on the same day agreed positionally in n letters, then usually, but not always, 2n wheels had the same functions in the "Pentagon" for the two corresponding wheel orders. This regularity did not apply to messages sent on different days. One case is known in which two messages sent on widely separated days had the same wheel order. The indicator system was never broken cryptographically. But an indicating device which would show similar characteristics is, as is known from the Elba capture, used on a machine which is a combination of the types known as T.52 B and T.52 C.

"Sturgeon" and "Mackerel" traffic came to an end with the battle of el Alamein. One other message sent on the "Pentagon" machine later in the month was however intercepted. It was believed to come from the Caucasus. As usual it consisted of several cipher passages in depth. It was successfully attacked,

3

and was shown to have been sent on the "Pentagon" machine. The message referred to the Russian front.

With this message the "Pentagon" machine vanishes from the knowledge of civilized humanity.

In the first half of 1943 other teleprinter links having the habit of saying "Um Um" appeared. Some of these were shown to be "Tunny." In fact, from this time on it was often difficult to decide whether a particular new link was on "Sturgeon" or "Tunny-type" machines. Both types gave only a Q E P number for the indicator. The only exception to this rule is that some groups of letters were sent, apparently as indicators, on "Salmon." These were quite different from the "Sturgeon" indicator groups.

"Salmon" operated between Koenigsberg and Mariupol. Messages were intercepted from 11th. January to 6th. February. The machine operated much more simply than the "Pentagon" machine. There was no combinations of wheels. Five wheels constituted the subtractor key, and the othr five the permutor key. The message consisted of "operator's chat."

As a result of the absence of the "Pentagon," cipher breaking was made much more difficult. 960 different alphabets, instead of 60 as before, were in use, and the parity of a cipher letter was not necessarily the same as the parity of the corresponding clear letter.

Another link (called "Sardine") appeared in May. It operated between Sicily and Sardinia. This link was never broken. Later in the year two operators' log books referring to this traffic were captured. (Time, numbers and degrees of priority correspond in the log books and the intercepted messages.) The same type of addresses (Luftwaffe) as were used in "Sturgeon" appeared.

In July and August the link "Halibut" was in operation between Koenigsberg and Munich. It came to an end in August, but reappeared in a changed form in 1944. In the period July-August a few depths of 4, and one of 5 were found.

An August depth of 4 was read. It was found to have been enciphered in the same way as the "Salmon" depths. Like them it consisted of "operator's chat."

The depth of 5 (July) was recalcitrant. In about a year however it was broken, and was found to have been enciphered on a new type of machine. As in the cases of "Salmon" and the

August depth, there was no combination of wheels in the formation of the subtractor and permutor impulses. But each wheel moved irregularly, being driven by a "motor" as are the "Tunny" wheels. But in "Halibut" each motor was formed by the Boolean addition of the patterns of two other wheels (with possible reversals), these patterns being read off from a different part of the wheel from that used in forming the subtractor and permutor keys. And of course these two wheels moved irregularly. There were four wheels having the same motors, but the motors of the other wheels were all different.

The messages broken referred to experiments with a machine called T.52 D. Since then two German cipher machines labelled T.52 D have been captured. Both contain a motor mechanism agreeing with that deduced cryptoanalytically for "Halibut."

In September 1943 the link "Conger" appeared between Athens and Berlin. Hundreds of messages were sent, all in depth so that there was no difficulty in reading them. They contained only "operator's chat."
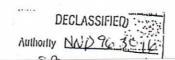
Reference to a captured machine (labelled T.52 B) showed that the initial setting of each wheel corresponded to that numbered 1 on the actual machine. (The numbering of the wheels as well as the patterns seems to be the same for all the machines.) The wheels were used in the order of their periods, and the operation of the machine was of the simple type encountered in "Salmon," and in the August "Halibut" depth. In November a similar "Conger" depth was sent, the wheels being now all set in position 2.

"Conger" and "Halibut" reappeared early in 1944. The new "Halibut" messages were all very short, (whereas the old ones had often been very long), but the "Conger" messages were often long. 'Depths,' that is sets of messages having the same QEP number, of up to 4 were found, but the lack of repeats in them suggested that an autoclave was being used. This hypotheses was supported by the occurrence in the logs of such phrases as "Mit KTF" and "Ohne KTF" (KTF = Klar Text Funktion.) One depth of two which was obviously "Ohne KTF" was found, but "Conger" depths of two are unreadable in England.

Soon after this the interception of these links was discontinued as being unprofitable.

Recently many "Tunny" messages have been sent without the autoclave, and E. messages have been found ordering its disuse in "T.52 D and T.52 E". A day's traffic on "Conger" was recently intercepted. Its study showed that the autoclave was not being used. (Evidence = repeat in depths of two).

II. Evidence from Captures

The first "Sturgeon-type" machine to be captured is labelled T.52 B. It was found in Tunisia. The wheels of this machine move regularly and do not combine. We do not know of any traffic which might have been sent on this machine.

Later a full technical description of a machine referred to as combining the functions of "T.52 A/B and T.52 C" was captured on Elba. The T.52 C machine therein described combines its wheels in fours. The ten combinations thus formed are not linearly independent. In fact two independent linear relations exist between them, so that the number of alphabets used is 256. This still compares favourably with the 60 of the "Pentagon" machine. The wiring diagram shows that the machine when acting as T.52 A/B does not combine its wheels. The "Salmon," August "Halibut" and early "Conger" depths could have been sent on a machine of this type.
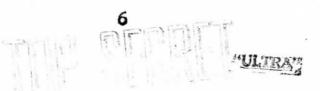
At the same time two key book pages, one for T.52 D and one for T.52 A/B and C were captured. One side of each page gave the table for June 3 1944, and the other side the table for June 4th. Each table consists of 25 rows (distinguished by the letters of the alphabet) and 10 columns (distinguished by the numbers 1 to 10). The entries in the nth. column are possible settings of the nth. wheel when the wheels are arranged in the orders of their periods. The evidence for this is that in each column the numbers range (roughly) from 1 to the period of the nth. wheel, and never exceed this period. Presumably the wheel setting of the message is given by a sequence of 10 letters, and the sequence of letters to be used is fixed by the QEP number. Thus the same QEP number will have different meanings on different days, even apart from the variation in the wheel order.

This completes the description of the tables for T.52 D.

The tables for T.52 A/B and C have two entries in each space of the first five columns. One is a wheel setting, and the other is one of the letters p s t u v x y z, which were met with in the "Sturgeon" indicators. These letters are indicators for a change of wheel order with each message. (Evidence described below.)

An interesting part of the "Elba" machine is its wheel-permuting mechanism.

There is a set of five levers each of which may be set in

TOP SECRET

"ULTRA"

any one of eight positions, distinguished by the letters P S T
U W X Y Z. Each lever controls 3 of a set of 15 switches. Each
switch interchanges two wheels in its active position, and leaves
their order unaffected in its inactive position. The switch is
active or inactive according to the position of its controlling
lever, but the correlation of switch positions with lever posi-
tions is not the same for all the three switches controlled by
a particular lever.

Besides this device there is a system of plugs (present in
all the captured machines), whereby the wheels can be steckered
in an arbitrary way. It seems likely that the indicator system
of the "Pentagon" machine depends on such a device. (See the
previous section.)

Since then an actual machine of the type described in the
"Elba" capture has been received from Naples. The system of
5 levers has unfortunately been removed. It is not present in
the first B machine, but there is room for it.

On another Naples machine the label, originally T.52 B
has been altered to T.52 D. This machine has a switch for
putting in or cutting out the autoclave. When the autoclave
is not being used, the wheels are motorized like those of the
July "Halibut" machine. When the autoclave is in use the
motor system becomes much more symmetrical, and the third im-
pulse of the clear is involved in it (driving two wheels with
(X), and two with (.)). We have not yet settled which of the
preceding clear letters contributes to the motor in this way.

Subsequently another T.52 D machine (altered from T.52 A)
was captured. From a comparison of the two machines it seems
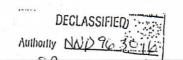that T.52 A and T.52 B must have been very similar machines.

III. Evidence from Decodes

References to T.52 traffic are often found in "Tunny" and
"Enigma" decodes. These messages in 1942 refer only to T.52 A/B
and T.52 C. There is also a captured hand book for cipher
officers, issued 1.12.42, which gives the machines in use as
T.52 A/B and T.52 C.

On 17.10.42 a message[1] from C.S.O. Luftflotte 2 to Flieger-
fuehrer Afrika speaks of T.52 C as having inadequate security,
and orders that "Secret" and "Secret Commands Only" messages
are to be enciphered on "Enigma" before being sent on Saegefisch
links.

This message passed between the points served by the "Stur-
geon" link, so it suggests that this link used T.52 C. On the

"ULTRA"

other hand messages, apparently of some importance, continued
to pass on this link without previous encipherment on "Enigma,"
until the cessation of the traffic on November 2nd. Many
"Enigma" messages were sent on this link however.

From decodes of February 1943 it appears that the Germans
then discovered something seriously wrong with their Saegefisch
machines. A message from Madrid to Paris[2] says that T.52 is
very badly compromised, and enemy decipherment is possible. No
more "Secret" or "Most Secret" messages are, it says, to be
sent on T.52.

On the 18th. of February a new set of instructions[3] were
issued. These lay down:-

    (1) The indicator systems in use for T.52 A/B and C
        are cancelled.
    (2) Henceforth the ten wheel settings are to be
        given instead, and sent on a specified emergency
        key.
    (3) A new method of indicating the settings of the
        "five levers" is to be used.
    (4) The device for setting back all the wheels to
        the "so called zero position" is to be removed.

These five levers must be those which appear in the "Elba"
capture. (4) shows that part of the trouble is the frequency
of depths. But the reference in subsequent messages to altera-
tions in T.52 C show that more than this is involved.

There was more information[4] on the 19th. February.

    (1) T.52 A/B is not to be used for "Secret" or "Most
        Secret" messages, save when other means are not
        available.
    (2) If T/P links are used, there must be previous
        encipherment on "Enigma."
    (3) After "the alterations to T.52 C," and after a
        change in the indicator system, "Secret" and
        "Most Secret" messages may again go forward
        without previous encipherment on "Enigma."

In March there appeared a message[5] saying that traffic on
the "Aptierte" (i.e. "adapted") T.52 C need no longer be en-
ciphered on "Enigma."

After this there were references to T.52 CA.

"ULTRA"

Then, on 14.6.43, there was a message[6] to the Naval Communications Officer, Sulina, and "other addressees" saying "On the completion of the adaptation to SFM T.52 C, the designation T.52 CA will no longer be used. The designation T.52 C only is to be used from now on.

The first reference[7] to T.52 D in the decodes came in October 1943. Since then there have been frequent references to T.52 A/B, T.52 C and T.52 D. Since September 1944 there have also been references to T.52 E.

```
1    Red    121-2-3  17/10  6610
2    RSS    6713/2/43
3    Bullfinch II   1735/18/2/43
4    Merlin   19-2-43
5    Red    Nos. 322/4, 385/7 of 6th. March
6    14/6/43    77    Med.
7    Red    279/0    4/10/43
```

IV. Conclusions

Our views on the distinctions between the T.52 machines may be summed up as follows:-

(1) Cryptographically there is no distinction between T.52 A and T.52 B. For our captures show that machines T.52 A, T.52 B exist, but references to such machines in the decodes are very rare. We find, however, many references to T.52 A/B, a designation which we suppose to include both.

Secondly both A and B can be converted into D.

(2) The "Pentagon" machine was T.52 C. The evidence for this statement is:-

    (i) Decodes suggest that the "Sturgeon" stations had a T.52 C (message of 17/10/42).

    (ii) The "Pentagon" is a combination of wheels in fours and so resembles the combination system of the new T.52 C (see below).

    (iii) Simpler machines than the "Pentagon" are known, therefore the "Pentagon" is unlikely to be T.52 A/B. This is borne out by the fact that the modern T.52 A/B is of this simple type, and we have no evidence that the meaning of this designation has ever altered.

(3) The original T.52 C machine was found to be very
insecure and was altered. The altered machine was
known first as T.52 CA and then as C. CA probably
stands for C. Aptierte, and thus has no connection
with T.52 A.
        (Evidence from decodes)
This affords further evidence for (2) for the
cryptographic evidence shows that the "Pentagon"
machine was very insecure indeed.

(4) The new T.52 C machine is completely known (Elba
and Naples captures). Its chief characteristics
are its combination of wheels in fours, and the
regular movement of its wheels.

(5) T.52 A/B is completely known from the same captures.
Its wheels do not combine, and they move regularly.

(6) T.52 A/B is not now used for important traffic.
(Evidence from decodes). But it has often been
used for practice messages. (Cryptographic evi-
dence on "Salmon," "Halibut" and "Conger" links.)

(7) T.52 D is completely known (Naples captures). It
is an improved form of T.52 A/B in which the wheels
move irregularly, and an autoclave can be used.

(8) There exists a T.52 E which has been put into action
recently (evidence from decodes). Nothing else is
known here about this machine.

Research Section

NOVEMBER 1944