24 February 1945

MEMORANDUM for Mr. Friedman

1. This note is being written in response to your inquiry as to my opinion on the degree of confidence we can have that the Germans are not reading our high-grade machine cipher traffic.

2. The nature of the problem is such that there is slight likelihood of finding any direct evidence bearing on it. The little direct evidence that exists ⟵ isolated statements by prisoners of war that no success was attending efforts to break "the big machine" - cannot be relied on because they were probably not in a position to know and their evidence is pure hearsay. The principal basis for the belief that the Germans are not reading the traffic in question is indirect and inferential.

3. The indirect evidence is based upon the intelligence derived from reading German E and Fish traffic. Several million high--echelon German secret messages have been read in the past few years. In them has been found information on every conceivable subject. German confidence in the security of their cryptographic systems appears so great that no restrictions have apparently been imposed on the type of information that may be passed in E and Fish traffic. Strategic as well as tactical plans are freely discussed. Messages to and from Hitler himself are not infrequent. Y service reports pass freely, in fact one E key (Mustard) is exclusively devoted to Y service traffic. Reports of cryptanalytic success on M-209 and other traffic have been found on numerous occasions. It is difficult to imagine, in the light of this evidence, that there is one subject and only one which may not be mentioned in E or Fish messages. And if such a rule existed, it is hard to believe that the Germans would draw a line of demarcation between the M-209 and what we consider high-grade machines.

4. Other sources of intelligence add to the accumulation of indirect or negative evidence. Prisoner of war interrogations and our own espionage have uncovered no hint that the Germans have ever read a single message enciphered in any of our high-grade machine systems. Furthermore, we know of no case where the Germans have appeared to know our plans and the circumstances implied that the source of their information was successful cryptanalysis.

Although we have frequently heard of German use of IBM
equipment in cryptanalysis, there is no evidence whatever
that they possess any high-speed machinery of the type
that would be essential even to attempt solution of some
of our machine ciphers.

5. The inferential evidence is based upon German
cryptography. We know so much about their cryptographic
practices that we can deduce their cryptographic theories
and thus determine the stage of development they have
reached in cryptanalytics. The overwhelming evidence is
that they are far behind us and have no appreciation of
solution techniques which we now regard as commonplace. We
can see from their security precautions just what they are
trying to guard against and can thereby reconstruct their
cryptanalytic theories. A recent change in the method of
selecting E indicators (designed to prevent the possibility
of cillies) shows a very belated appreciation of the dangers
inherent in the old system. The "CY" procedure indicates
that they are blissfully unaware of the cryptanalytic
techniques that have proved most succesful in reading E
traffic. In the case of Fish, the introduction of the auto-
key feature shows that they may have appreciated that machine
settings could be entirely reconstructed from messages in
depth. The introduction of daily-changing wheel patterns
in the summer of 1944 indicates that they may have finally
realized the possibility of statistical solution despite
their careful efforts to make the generated key completely
random. But at the same time, it shows that they have no
conception of the possibility of rapid statistical solution
with the aid of high-speed machinery because they continued
(and still continue) to send transmissions thousands of
groups long without changing settings. Numerous other
illustrations could be cited - the foregoing are merely
isolated bits of evidence.

6. If the Germans were reading our high-grade traffic
they would inevitably realize that we are reading theirs.
They would know this both from the content of the messages
and from the techniques which they had themselves employed.
In such event, even though they were unable to adopt improved
cryptographic systems and procedures, they would certainly
impose drastic restrictions on the topics permitted to be
discussed in wireless messages.

7. Never having participated in any studies made on
our high-grade machines, I cannot, from any personal know-
ledge, venture any opinion as to their inherent security.
If, by any chance, the Germans have developed methods of
analysis wholly beyond our conception they might, after the
capture of some of our machines, be able to read traffic
enciphered on them. But if we assume that they are so far
ahead of us, we must also assume that they have been able to

ascertain the nature of these machines by cryptanalytic
means and to recover the wiring of the rotors.   I am sure
that all security studies made on our machines have
assumed that they were in the possession of the enemy and,
therefore, see no cause for undue alarm because they may
now possess a few machines.

8. I feel it advisable to replace all compromised
rotors but do not believe this must be looked upon as an
emergency measure which must be accomplished post-haste.
There are two reasons why I feel a change advisable.   In
the first place, it is simply an additional precaution
preventing the possibility of cryptanalysis even of an
occasional isolated message.   But more important, if some
key list were compromised, traffic on the captured models
would be readable for the period covered by such list,
whereas a change in rotors would reduce this danger.

W J F
(Fried)

1. Para. 3 says no reports from our agents that Germans are not reading our high-grade traffic. I feel this means more as indirect evidence - of Para 4, 2nd sentence of my draft.

2. Para 5. 1st sentence may be too broad since we are reasonably sure that they must have known some of our tactical plans from M-209 solutions. (or compromises).

3. Para 7. 3rd line - Suggest changing "message" to "messages". 5th line suggest changing "have to employ" to "would have to employ" or "had employed"

4. I think 8 b is too broad. The variable reflector is the principal, but not the sole, exception. Enigma Uhr, for example, has done more than make it harder to intercept and segregate the traffic.

5. Para 9 - 3rd line from the bottom of p. 7 - suggest changing "their" to "German".

_____

re Enclosure

6. Para 2 - There is some discrepancy on speeds. At 350 steps per second a 3 wheel run takes 50 seconds, not 40. Also - it's nearer 566 minutes than 565 and both are nearer 9 1/2 hours than 9 1/4. But the errors are on the conservative side and therefore perhaps intentional.

7. Para 3. The highest Colossus speed I ever heard mentioned was 5,000 per second - not 7,000

_____

General - I think its a complete story, well presented and very convincing.

W.J.F.

```
    18
    2
  360
   16
 2160
  360
 5760
   14

23040
 5760
80640
   12
161280
 80640
967680
8|
  120,960  hrs.

24) 120 960  (5040 days
    120
     96
     96
      0
```

```
 17 500

46) 17 500
    439
```

```
365.) 5040  (13
      365
      1390
      1095
       295
```

There are 967,680 reams

$$2\overline{)9'67'680} \quad 8$$
$$483.840$$

$$350$$
$$180$$
$$7\overline{)000}$$

$$967680$$
$$9.25$$
$$\overline{4838400}$$
$$1935360$$
$$8709120$$
$$2\overline{)8,951,040}$$

$$1000\overline{)4475,520}\,(4475.$$
$$4000$$
$$\overline{4755}$$
$$4000$$
$$\overline{7552}$$
$$7000$$
$$\overline{5520}$$
$$5000$$
$$\overline{520.}$$

$$24\overline{)4475}\,(186$$
$$\underset{192}{24}$$
$$\overline{207}$$
$$192$$
$$\overline{155}$$
$$144$$

$$2\overline{)365}$$
$$20\overline{)186}\,(9.3$$
$$180$$
$$60$$

456 q

26

2741856
913952

350) 11881,376 (33949

1050

1381
1050

33513
3150

1637
1400

2376
2450

2760

60
60

3600
1

60) 33946 (565.96
300

394
360

460

60) 565 (9.25
540

260
140

800

Navy 3-W run 40 sec. 17,576

$$\times \underline{\quad} \times \underline{\quad} \times \quad \frac{26}{105456}$$
$$\frac{3552}{456976}$$

003 - 30 imp/sec

Old Brit 3 W./20/sec

new " + Navy same 4 W run 22 min
@ 350/sec.

Rob ~~2000/sec~~

Col 10 000/sec theor, actually
7000/sec

IBM - 80/min for high

If ~~G ← I~~ were able to read
purple they would let it out
If I were able to read med g
they wouldn't also.

Germans pa

Ultra over air.

Secrey of matter passed
ey Fish + E is as
great or greater in value
than Ultra

Germans has passed Ultra
to Japs + we have
seen none.

Assume Ultra must go
by courier, how could
they go on using E +
Fish

If they could read ABA
ol CCM how would they
go on using another
machine.

Reason for

① reflectors

② could better guie
op as to rule for
not passing Ultra
by radio.

④ Jerm did pass Ultra
from Russian front
when adv.

26⁴ (4 w bombs) now ½ hr.