~~CONFIDENTIAL~~

10 August 1983

MEMORANDUM FOR THE RECORD:

SUBJECT: Comparison between Chapter II, of To Keep A Secret, by Deavours and Kruh (DK) and Part I and II of Analysis of a Mechanico - Electrical Cryptograph by William F. Friedman(F).

1. F has none of the history contained in DK.

2. Both F, Part I, and DK describe the manner of operation of the 1923 Hebern machine.

3. The five rotor alphabets "1" through "5" listed at the bottom of page II-3 in DK are the inverses of the five alphabets "Alphabet 1." through "Alphabet 5." listed near the bottom of page 4 of F, Part I.

4. Table 6 on page 37 of F, Part I, is equivalent to the table on page II-20 of DK.

5. DK gives a method for recovery of the plain based on the wiring of the rotors being known. F, Part I, first presents a method of analysis when only the knowledge of the mechancis of the machine is available, and then presents a method of analysis when the "left fixed sequence" and the "right fixed sequence" are known.

6. The DK solution is based on one message 240 long. The F, Part I, solution is based on 10 messages ranging in length from 303 to 333 characters.

7. While F, Part, I has a section on Mathematical Theory of Analysis, he does not use the term "I.C." statistic, while DK uses "I.C." and attributes the concept of I.C. to Friedman.

8. While both F, Part I, and DK give solutions to the parameters of the machine, they do not have the same notations or development. For example, DK uses letters to represent permutations and combinations of permutations to represent the machine; F uses no such representation. DK uses more statistical evidence and while F uses statistical evidence, he also has a great deal of intuitive explanation on how things work and why the available choices are limited at various stages of solution.

9. In summary, I do not think the DK solution was based on the reading of F. I recommend that we keep F classified CONFIDENTIAL even though DK, Chapter II, appears in the public domain.

RALPH W. JOLLENSTEN
Chief, P12

DISTRIBUTION:

P1
T5413, Russ Fisher
A5
Q43
S6

~~CONFIDENTIAL~~