DEPARTMENT OF STATE
WASHINGTON

May 23, 1939.

Dear Colonel Friedman:

Referring to our conversation of yesterday and the telegram I received from Mr. Doty, I am enclosing for your perusal the letter and exhibit referred to in the telegram. Kindly return it to me at your convenience.

Sincerely,

David A. Salmon

Enclosure:

From C.R.Doty
with enclosure.

Lieutenant Colonel William F. Friedman,
Office of the Chief Signal Officer,
War Department,
Washington, D. C.

INTERNATIONAL BUSINESS MACHINES CORPORATION

GENERAL OFFICES,
590 MADISON AVENUE
NEW YORK

DIVISIONS:
ELECTRIC BOOKKEEPING AND ACCOUNTING MACHINE DIVISION
INTERNATIONAL TIME RECORDING DIVISION
INTERNATIONAL SCALE DIVISION
INTERNATIONAL ELECTRIC WRITING MACHINE DIVISION

May 22, 1939

Mr. David A. Salmon
Dept. of Communications & Records
State Department
Washington, D. C.

Dear Mr. Salmon:

Regarding my telegram of this date: In order that none of the fine points of the coding device which we discussed last week will be neglected in your consideration of the proposition I have taken the time to encipher a test message by hand in several different ways.

I believe you will find the attached sheet self-explanatory. In the first instance the same message is encoded by means of the same card used in the four possible positions. In the second case the same message is coded with the same control card (always in the same position) with only a change in plugwires.

If the above is not sufficient evidence of the flexibility of the device, there are other means of further changing the card-sensing means by plugwires which will further scramble the result.

It is still my opinion that a very few cards are all that would be required for your point-to-point communication.

I would suggest that you carefully analyze the attached from a cryptographic standpoint so as to satisfy yourself regarding the security of the device. I feel that the likenesses which appear are merely coincidental and that they are no more frequent than would appear in a similar amount of copy encoded with any other device.

If there is any further information which you require, or if I can be of any further assistance to the Department in Washington, please do not hesitate to let me know.

Sincerely yours,

C. R. Doty
Comm'l Research Dept.

CRD:CWS

Assume the alphabetical keys on a punch were operated in the following order for 45 random characters and that the holes indicated were punched in a control card:--

H A D J O Q U K P T S E I C N R Z X B G L W Y M V F Z Y C I J N B F S M E Q L A H K U X T

A B B C D E A C D B D C E A D C E A B D C E A E X B E A A E C D B B D E C E C B A C A A B
1 5 3 2 1 5 4 1 3 1 4 4 4 2 2 5 2 5 4 5 3 1 3 3 2 2 3 2 4 2 2 4 2 4 3 4 5 3 5 1 1 4 5 1

Using this card as control, leaving plugwires as shown in the folder diagram, the following test message has been coded for all four positions of the card in the following order:--

(1) Front -- columns 1 to 45
(2) " -- " 45 " 1
(3) Back -- " 1 " 45
(4) " -- " 45 " 1

STATE DEPA-RTMEN-T WAS-HINGT-ON PA-RIS L-ONDON PERU

(1) XZIHY UFTHK IFIIG EXXHI UHQDT XLCTW FBZIC LZYBT EEGSE

(2) OUGQZ BQJXP AKTXF DPHUJ HXYFG SUAJD KYCHU KBAUS XHQTP

(3) NVMLC EJBDW ABWUG WTXHW UHYVT FHKFK JBZQU DVIBP UMKSQ

(4) CUCIJ FOZBX ICTXB PDZYB HFQFG EUANL KMOLC YFSQI TDMXZ

To illustrate the fact that a change in plugboard wiring does not merely result in letter substitution, three changes were made. The same message was coded with the same card in the position (front columns 1 to 45) for the four cases shown. The following shows the result:--

STATE DEPA-RTMEN-T WAS-HINGT-ON PA-RIS L-ONDON PERU

(1) XZIHY UFTHK IFIIG EXXHI UHQDT XLCTW FBZIC LZYBT EEGSE

(2) WLUJW BUSFY LANIP QMFOD FPTYT SHLUF ZKCAN PCELZ FXJPV

(3) QMMRQ MESSW FQOKU ZLLFC STVHT ZWRYH OHRHT JKZPD DCHPV

(4) HPHNR CPGMK AXLXJ CNCTX NDYLT FXAWV ZMKQC PTQSL UUWKI