WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

OCSigO 201 Friedman, Wm.F.
(10-29-31)

November 17, 1931.

MEMORANDUM for the Administrative Assistant,
War Department.

1. Attached is Mr. Friedman's report on his investigation, for the Department of State, of the cipher machine submitted for their consideration by the International Telephone and Telegraph Company. Draft of letter of transmittal for the signature of the Secretary of War is also inclosed.

C
O
P
Y

For the Chief Signal Officer.

G. E. Kumpe,
Colonel, Signal Corps.
Executive.

1. Incl.
Draft let. trans. report.

SIS FILES

W.P.& T.DIV.

WAR DEPARTMENT
alm
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

November 16, 1931

MEMORANDUM TO: Executive Officer.

Attached hereto is Mr. Friedman's report on his investigation, for the Department of State, of the cipher machine submitted for their consideration by the International Telephone and Telegraph Company. It is recommended that this report be forwarded to the Department of State, and that the following be used as a basis for a letter of transmittal to be signed by the Secretary of War:

> Reference is made to your letter of October 29, 1931, and this Department's reply of November 9, 1931, with regard to the assistance to be rendered by Mr. W. F. Friedman, Cryptanalyst in the Office of the Chief Signal Officer, in your investigation of the cipher machine submitted for your consideration by the International Telephone and Telegraph Company. The Department is pleased to forward herewith the report rendered by Mr. Friedman as a result of his investigation of the degree of cryptographic security afforded by this machine.
>
> Should any further assistance or advice in this connection be necessary or desirable, this Department will be very glad to cooperate with your Department in whatever manner possible.

D. M. Crawford,
Major, Signal Corps.

Attached:
Report

Report on Investigation for the Department of State of the cipher machine submitted for their consideration by the International Telephone and Telegraph Company.

---

1. Pursuant to authority contained in the 2d Indorsement, dated November 4, 1931, to a letter dated October 29, 1931, from the Department of State to the Secretary of War, a study was initiated to determine only the degree of cryptographic security afforded by the above-mentioned cipher machine.

2. A theoretical method of solving cryptograms produced by this machine, without possession of either the machine or a knowledge of the particular key settings employed in their production was quickly established.

3. Two sets of cryptograms were requested for test, as set forth in the attached Exhibit 1. The messages were delivered to this office under sealed cover and were received at the times indicated on the photostatic copies, Exhibits 2 to 9, inclusive.

4. As regards the first set of messages, the only information given by the State Department was that each message had been enciphered by a different 10-letter keyword. Attached hereto, labeled Exhibits 10 to 13, inclusive, are the solutions to Messages 1, 6, 7, and 8, of the set of 12 messages furnished as Set A. There seemed to be no point in solving all the messages of this set, it being deemed satisfactory to demonstrate, by solving any four of them, the possibility of solving any messages of this category, all with independent initial key settings. It may be stated that, with practice, any message of this type may be solved within an hour or less.

5. As regards the second set of messages, Set B, the only information given by the State Department was that these four messages were the 3rd, 4th, 5th and 6th of a series enciphered from an initial setting known only to them. Attached hereto, labeled Exhibits 14 to 17, inclusive, are the solutions to all four messages thus furnished. It may be stated, as regards this method of employing the machine, that if a series of 10 or more messages is available, the determination of the proper initial setting for the series can be reached within 24 hours, possibly only 12 hours. From that point on, however, all messages can be deciphered as rapidly as the legitimate correspondents can decipher them, providing a duplicate machine is available. If no duplicate machine is at hand, then the question of quick translation becomes one merely of available clerical personnel.

William F. Friedman,
Cryptanalyst,
Chief of Signal Intelligence Section.

Attached:
Exhibits 1 to 17, inclusive.

OCSigO - November 16, 1931

REF ID:A4148811

EXHIBIT 10.

MESSAGE NO. 1 of SET A

RIGA

DATED NOVEMBER 6, 1931.

RECEIVED 12:40 P. M.

SECRETARY OF STATE,

WASHINGTON.

WHILE NO FIGURES ON THE SIZE OF RUSSIAS THIS YEAR GRAIN

CROP HAVE YET BEEN RELEASED, OFFICIAL SPEAKERS CITED IN PRAVDA

OF NOV 2ND AND 3RD ANNOUNCED THAT THERE HAS BEEN A SERIOUS

DROUGHT ...

COLE

(Solving time; 40 minutes to get first word "WHILE".)

EXHIBIT 11.

MESSAGE NO. 6 of [illegible]

NOVEMBER 5, 1931.

6 P.M.

AMLEGATION

MONTEVIDEO (URUGUAY)

ARE FLOOR DRAINS IN BATH AND TOILET ROOM REQUIREMENTS

STIMSON

(Solving time: 30 minutes)

EXHIBIT 12.

MESSAGE NO. 7 of DET A.

NOVEMBER 3, 1931.

6 PM.

AMERICAN CONSUL,

TOKYO (JAPAN)

INSTALLATION OF GRILL AUTHORIZED IF PLACED ON NORTHEAST WALL IN JAMB OF ARCH LEADING TO STAIRWAY FROM THE NORTHERLY CORNER OF LOBBY NO. 17, GRILL TO SWING INTO LOBBY.

STIMSON

(Solving time: Approximately 1 hour for complete reading.)

EXHIBIT 13.

MESSAGE NO. 3 OF SET A

NOVEMBER 5, 1931

5 P.M.

TO ALL AMERICAN DIPLOMATIC AND CONSULAR OFFICES:

PRESIDENTS PROCLAMATION NOVEMBER SECOND DIRECTS DISPLAY

UNITED STATES FLAG ALL GOVERNMENT BUILDINGS ARMISTICE DAY NOVEMBER

ELEVENTH. TAKE ACTION ACCORDINGLY.

STIMSON

(Solving time: First word in 30 minutes; for complete reading 1 hour and 20 minutes.)

EXHIBIT 14.

MESSAGE NO. 3 of SET B

OCTOBER 30, 1931

7 P.M.

AMEMBASSY,

SANTIAGO, CHILE

ONE. CONTINGENT EXPENSE ALLOTMENT INCREASED $305 TO PROVIDE FOR REPAIRS RECOMMENDED YOUR DESPATCH 974. TWO. YOUR DESPATCH 952 ANSWERED BY MAIL INSTRUCTION OCTOBER 6.

STIMSON

REF ID:A4148611 EXHIBIT 15.

MESSAGE NO. 4 of SET 5

OCTOBER 30, 1931

7 P. M.

AMLEGATION,

ASUNCION, PARAGUAY

EMBASSY AT RIO DE JANEIRO REPORTS THAT VASCONCELLOS WAS ON BOARD

STEAMER SOUTHERN CROSS WHICH LEFT THAT PORT ON OCTOBER 29 FOR NEW YORK.

STIMSON

REF ID:A4148811 EXHIBIT 16

MESSAGE NO. 5 of SET B

BERGEN

DATED OCTOBER 30, 1931.

RECEIVED 6:29 P.M.

SECRETARY OF STATE,

WASHINGTON.

NAVTOVA* MARSTEINEN* LIGHTHOUSE AND BACK TO BERGEN TODAY.

WEATHER DID NOT PERMIT TRANSFER OF MEN IN BOW BOAT BUT GOT TUGBOAT

AND SUBMARINE.

SMITH

* These names are not certain.

EXHIBIT 17.

MESSAGE NO. 6 OF SET B

PERNAMBUCO

DATED OCTOBER 31, 1931

RECEIVED 7:34 A.M.

SECRETARY OF STATE,

WASHINGTON.

ALL AMERICAN RESIDENTS AND KNOWN TRANSIENTS IN PERNAMBUCO

SAFE AND WELL.

VAN DEN AREND