

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS,
CONCURRENCES, OR SIMILAR ACTIONS

1	NAME OR TITLE COL. HERRELKO	INITIALS	CIRCULATE
	ORGANIZATION AND LOCATION C/SEC	DATE	COORDINATION
2			FILE
			INFORMATION
3			<input checked="" type="checkbox"/> NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Please let me have results of
examination.

Col H I/A
41 (M.C) A

FROM NAME OR TITLE

ORGANIZATION AND LOCATION

DATE

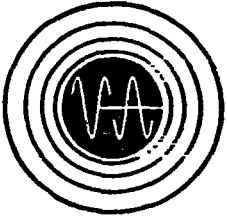
1 Apr 55

TELEPHONE

DD FORM 1 FEB 50 95

Replaces DA AGO Form 895, 1 Apr 48, and AFHQ
Form 12, 10 Nov 47, which may be used.

16-48487-4 GPO



VARIAN associates

RUSSELL H. VARIAN, PRESIDENT • H. MYRL STEARNS, GENERAL MANAGER
611 HANSEN WAY • PALO ALTO, CALIFORNIA • DAVENPORT 5-5631

March 21, 1955

Mr. William Friedman
National Security Agency
Washington, D.C.

My dear Billy:

For a long time you have not heard from me. My silence is now broken and I desire to convey to you what I consider an excellent possibility for a high degree cipher system.

For the past year I have been employed by Varian Associates, in Palo Alto. I have come in contact, during this period, with a number of fine, up-standing young men, one of which is a designer of the enclosed cryptograph system. He is Howard N. Smith, a graduate of Massachusetts Institute of Technology. Howard Smith is highly respected in our organization and has gone to great lengths in the development of this system. I have studied it and consider that it has excellent possibility for military usage, should it be possible to convert it electronically to automatic usage.

I consider your judgment in matters of this nature as the best obtainable in the United States, so if you will be kind enough to carefully analyze the possibilities of our Government's use of the enclosed system, and give us your recommendations, I will be extremely grateful.

The inventor's position is that he desires the system be completely analyzed by an expert to determine the extent of possible interest. Should there be merit, he would be willing to make it exclusively available to the United States' Government under some proper contractual arrangement. Mr. Smith also advises me that should you consider it as a possibility he would be glad to come to Washington to discuss the matter in detail with the appropriate authorities.



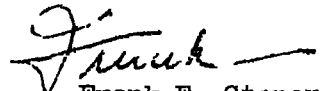
Mr. William Friedman
National Security Agency

- 2 -

March 21, 1955

I hope this letter finds you and Mrs. Friedman in good health and happiness, and Mrs. Stoner and I hope that, should you every come West, you'll plan to stop by to see us. Our best wishes also.

Sincerely,


Frank E. Stoner

Enclosure: Cryptographic System
Invented by Howard N. Smith
(Dated November 14, 1954)

P.S.: I am transmitting this System to you by my good friend, Colonel Walter B. Brown, our Washington representative. Colonel Brown served for many years in the Signal Corps, and I am sure you will enjoy making his acquaintance.

Suspense 15 Apr
REF ID: A70314

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS,
CONCURRENCES, OR SIMILAR ACTIONS

1	NAME OR TITLE COL. HERRELKO	INITIALS	CIRCULATE
	ORGANIZATION AND LOCATION C/SEC	DATE	COORDINATION
2			FILE
			INFORMATION
3			<input checked="" type="checkbox"/> NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Pse let me have results of
examination.

FROM NAME OR TITLE

J

DATE

1 Apr 55

ORGANIZATION AND LOCATION

TELEPHONE

Office Memorandum • UNITED STATES GOVERNMENT

TO : S/Asst (Mr. Friedman)

DATE: 18 APR 1955

FROM : DD/COMSEC (Col. Herrelko)

SUBJECT: Cryptographic System Submitted by Howard N. Smith

Reference: Confidential ltr from Maj. Gen. Frank E. Stoner, USA, Rtd.,
dtd 21 Mar 55

1. The system described in the brochure inclosed with the reference has been examined and found to incorporate no principles which are superior to those presently in use. It is a type of autokey (Vigenere) substitution wherein each key value is determined by the random selection of a letter, conversion of that letter to a displacement interval by a mixed component, and the corresponding displacement of the plain and cipher components from their preceeding alignment. Alternate letters of the cipher are the encipherment of the randomly-selected (indicator) letters.

2. It is suggested that your reply to Maj. Gen. Stoner include substantially the following:

"Unfortunately, the system designed by Mr. Smith does not exemplify any cryptographic principles not already known to us, and it has certain major disadvantages, compared to systems in current use. Although the combination of basic principles shows a keen and facile mind, and a flair for cryptographic manipulation on the part of the designer, several deterrents to its operational feasibility, for our purposes, may be cited. The inherent requirement that each cipher message be twice the length of the corresponding plain language is an uneconomical feature for large volume traffic. The fact that a single discrepancy between the correct cipher text and the version received may affect the intelligibility of the remainder of the message also introduces a highly undesirable factor. It is recognized that such errors may be corrected readily enough in hand operation of such a system; however, in electronic adaptations, present criteria require that automatic equipment be permitted to operate unattended, without the likelihood of unpredictably long stretches of unintelligible plain text resulting."

"It is interesting to note the thorough analysis, by the authors of the brochure, of the potential weaknesses of this system; their

electro-mechanical
an

I feel sure that your long background of practical experience in electrical communication technology will serve to corroborate the emphasis we lay upon the disadvantages of Mr. Smith's system for extensive official telecommunication.

18 APR 1955

independently conceived methods for averting these weaknesses represent a commendable achievement. I trust you will express our appreciation to Mr. Smith, and to his associate Mr. Lewis, for their patriotic interest and expenditure of time and effort in this matter."

The correspondence and the descriptive brochure are attached.

Copy furnished:
TEC (NSA-18)



F. E. HERRELKO
Colonel USAF
Deputy Director
Communications Security

1 April 1955

Major General Frank E. Stoner, USA, Rtd.
 Varian Associates
 611 Hansen Way
 Palo Alto, California

Dear Frank:

I was highly pleased to have a telephone call from Colonel Brown and to have news about you and Mrs. Stoner, for I had been wondering about how you are and what you are now doing.

This letter will be but a brief acknowledgment of receipt of your letter and its inclosure dealing with a cryptographic system proposed by Mr. Howard W. Smith of your organization.

You flatter me by your characterization of my judgment in matters of this nature but I will be glad, of course, to give my own attention to Mr. Smith's proposal after a thorough study and an appraisal of it has been made by our very competent technical staff and certain other of my associates.

Just as soon as possible I will write you of the results of our study and I hope both Mr. Smith and you will not be too impatient. From your own experience of former days you certainly are well aware of the fact that proposals of this sort come to us in a steady stream from patriotic citizens and inventors who find this field fascinating. Unfortunately, because they do not have access to the extensive but usually classified literature that exists in this field, the chances of their inventing something really new and useful are rather small. Nevertheless, because there is always some chance of this, we try to look at each proposal in as objective a manner as possible, and this does take time.

Your letter finds both Mrs. Friedman and myself in good health. I have just returned from over a month's absence in Europe on official business, to find that a manuscript we wrote on Shakespeare-Bacon cryptography was awarded the \$1,000 Folger Shakespeare Library literary prize. We hope to see it published very soon.

Sincerely,

WILLIAM F. FRIEDMAN