20 April 1955

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

Dear Frank:

Here is the follow up on my letter of 1 April in connection with the cryptosystem you sent me via Colonel Brown recently. As I indicated we would in my letter, we gave the thing a pretty thorough scrutiny.

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 electro-mechanical and 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. 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 telecommunications.

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

At the moment I am recovering from a minor heart attack but they put me in the hospital nevertheless, where I have already been

for over two weeks. However, I'm making good progress and should be out of here in a couple of hundred years -- at least it will seem that long.

Sincerely,

WILLIAM F. FRIEDMAN
Special Assistant