

Contract No. DA 18-119-sc-109
267-LYN-58 (Mr. William F. Friedman)

SIGPO

TNG

8 July 58
J. F. Cain/4057/dm

On 1 July 1958, Mr. William F. Friedman delivered Progress Report No. 1 to the Director of Training as provided in paragraph (1) b, Article V, contract No. DA 18-119-sc-109. This report meets the technical requirements of the Office of Training.

WILLIAM F. FRIEDMAN

310 SECOND ST., SE WASHINGTON 3, D. C.

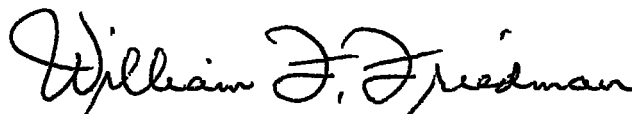
1 July 1958

Director
National Security Agency
Fort George G. Meade, Maryland
Attention: Director of Training

Sir:

Reference is made to Contract No. DA18-119-sc-109, 267-LYN-58, entered into as of 1 May 1958 by and between the United States of America and the undersigned. In accordance with provisions of Article I, paragraph d, of said contract, I submit herewith, in Inclosure 1, the first of the six bi-monthly Progress Reports outlining progress of the work on the items called for by said contract.

Very truly yours,


WILLIAM F. FRIEDMAN

Incl:
a/s

1 July 1958

1. Progress on Project 1 of Article I, Paragraph a(1) of the contract.

a. The item called for under this project is a manuscript of the text for a series of six (6) lessons containing unclassified data designed for the technical orientation of new NSA employees. However, after discussion with various high-level employees of NSA, it appears that the material and information to be included in this manuscript could also well be used with benefit, as collateral reading, by many NSA employees who, although now properly regarded as skilled specialists in their respective fields by virtue of their several or many years' practical experience, have never had the time or opportunity to glean by diligent research something about the history of the invention and development of cryptology. For it is a fact worth mentioning in this connection--but it is not a strange one--that there is in existence no adequate and authentic history of cryptology in any language. Such history as can be found scattered here and there in cryptologic literature is usually in foreign languages, is scanty, often erroneous, and gives evidence of having been prepared either by amateurs or by "literary hacks". That is why learning something about the history of cryptology is, for the beginner or even the experienced professional cryptologist, a job not many have the time or the willingness to undertake. Therefore, the manuscript of this text will not address itself strictly or only to beginners in the cryptological profession or practice of cryptology; it will be designed to be useful as well to the

INCLOSURE I

advanced students and skilled technicians mentioned above. Even when completed, however, the manuscript called for under Project 1 will constitute merely a broad outline of the history of cryptology; a definitive history will require much more space and time than is contemplated under the present project. Moreover, much research would be necessary to turn up the undoubtedly large number of cryptologic secrets which still remain hidden in the great libraries of Europe or have been so carefully buried, for security reasons, in the archives of the important governments of the world. A definitive history of this sort deserves, but will have to await, the attention of the slow, methodical and discerning scholarship of some future professional cryptologist who may be fascinated by the history and development of the science and art which lies at the foundation of his profession and may find the time and opportunity to embark upon the laborious but interesting job that would be involved.

b. For the purposes of Project 1 as broadly outlined above, a large amount of material has already been collected by the Contractor. The thousands of items contained therein are being carefully scrutinized and sorted. Attempt is being made to separate fact from fiction and where possible, evidence from one source is being weighed against evidence from other sources. But for the most part cryptologic incidents or events of cryptologic, diplomatic, naval, or military importance to be presented under Project 1 (except for those which happened long before he lived) will be such as have been experienced, witnessed, or lived through by the Contractor during his long professional life as a cryptologist. This

separation of fact from fiction may be exemplified in the sort of research which would be or is involved in trying to find answers to such an interesting question as this: Who or what cryptologic agency really discovered and applied the principles underlying the use of polyalphabetic cipher systems? Who or what agency really discovered and applied the principles underlying the solution of such systems? When was transposition first used? Who was first to combine substitution and transposition? Then there are many minor but also interesting questions such as these: What was the nature of the writing which an unseen hand inscribed on the wall of Belshazzar's banquet hall while that monarch was feasting? Why could not the Chaldean wise men and Babylonian soothsayers read it? Was it a cryptogram? How did Daniel solve the message it contained? Why does the Bible make the text of the writing in the first statement of it read "MENE, MENE, TEKEL, UPHARSIM" and in its second statement of it read "MENE, MENE, TEKEL, PERES"? Are the two words "UPHARSIM" and "PERES" variants in the sense of that word as used in cryptologic terminology, or in the sense of that word when we refer to "synonyms?" Of course, questions of this sort are not of any practical importance in modern cryptology; but to the professional cryptologist who delights in delving into the past and in musing along the byways as well as the highways of his science, questions such as these are not merely of academic or simply passing interest. They are of absorbing interest--or should be.

c. Again, take these questions: Which came first--"plain-text" writing, or "secret" writing? Should the cryptologist concern himself at all with the history and development of the alphabet? Or of writing of any kind, such as ideographic, pictographic and the like? What interest does

signalling in general and secret signalling in particular have for the cryptologist? Should he concern himself only with cryptography, i.e., secret writing; or, if he considers the many different modes of transmitting thoughts and information of various sorts, should he look into all forms of communication and, more specifically, secret communication--even those long ago outmoded? To review outmoded ideas and take a new look at them in the light of new techniques and of means not dreamt of when those ideas were first generated is frequently a not unprofitable procedure. Modern information theory and modern electronic digital computers, for example, make use of a "bilateral alphabet" first proposed, invented, or described by Francis Bacon. When put in this way it becomes clear that the professional cryptologist must or should concern himself with the old things as well as the new ones, and with all forms of secret communication, and not merely with secret writing, for are not ciphony and cifax currently in use and do they not now present problems of great interest and complexity? They are, strictly speaking, not forms of secret writing or cryptography. And then there is civision--and possibly telepathic communication--should these be included in the sphere of cognizance of the professional cryptologist?

d. It will seem, therefore, that even the gathering of the raw material for Project 1 involves a lengthy, painstaking and absorbing process. The sifting and digesting of the bits and pieces and their assimilation and condensation to make a well-rounded and interesting introduction to the cryptologic historical orientation of the professional

and would-be professional cryptologist represents an interesting and worthwhile problem. A good start has been made on this part of the Contract by this time. In the Contractor's personal collection of items of cryptologic interest are thousands of bits and pieces, including books, periodicals, articles in scientific and popular journals, newspapers-- and even cartoons and "comics" in which cryptograms play a role and which should not be discarded as childish, for they serve as mirrors reflecting the average person's absorption or interest in the subject of cryptography even today. There are, too, thousands of photographs, reproductions in the form of photostats, photocopies and the like, to be examined for points of cryptologic interest, to enliven the text and what is to come after it-- the recorded lectures. In short, there is no paucity of authentic, semi-authentic, and downright erroneous material to be studied; there is indeed a plethora, so that perhaps the problem will be to decide what to omit, or treat sketchily, rather than what to include or to treat in detail. For instance, a single episode of great importance in the history of cryptology, diplomacy and warfare--that involving the famous "Zimmermann Telegram" of World War I--well deserves lengthy treatment and a text all by itself, with two or three full-period lectures to accompany it. There are similar fateful cryptologic episodes of World War II awaiting similar detailed treatment because they are of absorbing interest and of great technologic value to the cryptologist.

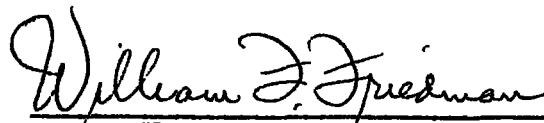
2. Progress on Projects 2, 3, and 4 of Article I, paragraphs (a)(2), (a)(3), and (a) (4) of the contract.

a. The contractor has already amassed a large file of photographic negatives and prints from which selections will be made to accompany the manuscript called for under Project 1, and which will serve as illustrative material for the data contained in the manuscript of Project 1. But many more photographs remain to be produced from material of more recent vintage, say from the period 1940 or thereabouts to the present date. Much of the basic raw material to be photographed has already been assembled; the portions to be photographed are still to be sought out and delineated for photographic processing.

b. For Project 3, the set of lantern slides for use in connection with a series of six lectures which shall be based upon and coordinated with the material called for under Project 1, the Contractor has already assembled a large collection of slides from which selections are to be made. But more slides will be necessary, depending upon what material is finally selected for Project 2.

c. Finally, on Project 4, the preparation of a voice recording of the material contained in the six lectures to be prepared for use in connection with the materials called for under Projects 1, 2, and 3, nothing has yet been done in the way of actual recording, of course; but a rough outline of text to be recorded, made in the form of notes on cards is well under way. From these cards a manuscript will be prepared, and then, in preparation for final recording, there will have to be some practice recording for primary editing and revision.

3. The Contractor believes that one-sixth of the work to be done under this contract will have been completed by the date of the submission of this report. There has been an interruption in work which was occasioned by the Contractor's having undertaken, in his capacity as a consultant to NSA, a special mission in behalf of the Director, NSA, and which necessitated making a couple of trips overseas after the contract was initiated. A further interruption of about one month will be occasioned by the Contractor's acceptance of an urgent invitation to attend the first month's session of the SCAMP program at the University of California in Los Angeles, to deliver some lectures thereat during that month, and to participate in other SCAMP activities.


WILLIAM F. FRIEDMAN