424 N. George Mason Drive
Arlington, Va.
12 January 1950

Dr. Julian P. Boyd
Princeton University Library
Princeton, New Jersey

Dear Dr. Boyd:

Receipt of your letter of 10 January is acknowledged.

The only suggestion I have for a possible change in the proposed statement is in respect to the footnote, with a view to clarification or rather the elimination of what might be an ambiguity. A quick perusal of the footnote gives the impression that the "second inventor in the field" is William F. Friedman -- an impression which is dissipated only on closer study. It might be better to make it perfectly clear that the quoted matter is an extract from a "communication to the editors." Therefore I suggest that the parenthetical portion of the footnote be made to read as follows:

> ... a second inventor in the field." (Extracted from a communication to the editors, 17 Nov. 1949, from William F. Friedman, Chief of the Technical Division, Armed Forces Security Agency, Washington.)

I trust that you will not deem my suggestion pedantic and that it will meet with your concurrence.

In closing I wish to say that I feel very much repaid for the bit of effort that went into the drafting of my commentary, since you have seemed it fitting to place Jefferson's cryptographic invention in such distinguished company with his drafting of the Declaration of Independence as evidences of his "elevated and even inspired intellect."

Sincerely yours,

WILLIAM F. FRIEDMAN

424 N. George Mason Drive
Arlington, Va.
5 January 1950

Dr. Julian P. Boyd
Princeton University Library
Princeton, New Jersey

Dear Dr. Boyd:

Receipt of your letter of 27 December 1949 is acknowledged.

It is not often that a man receives an apology which is so flattering in nature that he is truly glad to find himself in a situation calling for one! Under the circumstances ascribed in explanation of the delay in replying to my letter of 17 November, I am glad to share some of the responsibility therefor. I hardly expected that my commentary would meet with such approval and appreciation as you indicate.

I have, of course, no objection at all to your referring to my commentary in the Introduction to Volume 1. Indeed, I am more than pleased that you find it of sufficient interest and merit to mention it in what must be a very much attenuated birds-eye view of the whole project.

As to my title, although the general nature of my position has not changed in many years, the title of office has gone through a good many metamorphoses. Currently, I am Chief of the Technical Division, Armed Forces Security Agency. It would be proper to employ, if you wish, the title "Colonel" although I received my honorable discharge from active service way back in early 1941. I am on the honorary retired officers list.

If you have no objection, I would like to have the opportunity to review your proposed mention of my commentary, in passim, in the Introduction. I might add that I found it desirable to request permission from higher authority to prepare the commentary -- "security considerations, and all that sort of thing, you know." I am supposed to keep entirely out of print and to have a real passion for anonymity!

Thank you for your courteous invitation to visit the Library and to spend a few minutes with you. But I don't get around much these days. I'm hoping that this will not be the case for long, however, and that I can some day make up for several years of a somewhat vegetative mobility.

Thanking you for your very nice letter, I am

Sincerely yours,

WILLIAM F. FRIEDMAN

424 N. George Mason Dr.
Arlington, Va.
~~14~~ November 1949

Dr. Julian P. Boyd
Princeton University Library
Princeton, New Jersey

Dear Dr. Boyd:

A couple of years have passed since our exchange of letters on the subject of my preparing a brief commentary on Jefferson's "Wheel Cypher."

In your last letter, dated 11 September 1947, you indicated that it would be several years before you reach the volumes in which the cipher documents will be published. Although I felt that there was no urgency in the preparation of my commentary, I nevertheless at once set myself to writing the piece. In the course of doing so, two things happened. First, some questions arose as to the exact dates of conception of the identical device by two American inventors other than Jefferson. Since the gentlemen in question were both old friends of mine, and still among the living, I wrote to them, thus obtaining valuable, authentic data which were incorporated in my account. Not only that, but I then sent the draft of my commentary to both of them and profited by their review thereof.

The next thing that happened, soon after completing the piece, was that I had a siege of illness which made any "extra-curricular" activity a burden, so I put the piece aside. Now that I am recovering, I dug it out the other day and am enclosing it herewith, for your scrutiny.

I know that you wish to limit the commentary to five hundred words, preferably less. I fear I have failed rather badly in my attempt to stay within the limit set, and suggest that you may be in a better position to tailor the piece to your needs than am I. However, if you prefer that I do the trimming, please do not hesitate to return it and I will try my best.

I am planning to write a complete story of this device for Douglass Adair, in connection with a much longer article

for the William and Mary Quarterly. It was very good of you to suggest to Dr. Adair that he propose to me the preparation of an article on ciphers of the period ca. 1800, for the Quarterly and I am about to embark on that piece. It should be interesting to write; I hope it will also be interesting to read.

With cordial greetings, I am

Sincerely yours,

Encl. WILLIAM F. FRIEDMAN

Commentary on Jefferson's "Wheel Cypher"

Jefferson's invention of the Wheel Cypher represents a contribution to cryptographic science so far in advance of his time that at least a century had to elapse before a similar invention was independently made by a second inventor in the field. The ascertainable facts are useful in assessing Jefferson's ingenuity and perspicacity as a theoretical as well as a practical cryptographer.

Lacking specific information as to the genesis of his invention, we can only offer surmises. That Jefferson found numerous occasions for employing cryptography in his official correspondence, particularly when he was in France, is abundantly clear. In those days there were in general usage only about a half dozen methods of secret communication. In addition to their technical vulnerability, which he probably ascertained for himself either by speculation or by experimentation, Jefferson undoubtedly found such methods very cumbersome and tedious in practice. It appears logical, therefore, that a man endowed with a flair for invention would exercise his imaginative faculties in a search for better methods. It is probable that the Wheel Cypher came to him in a single brilliant flash of imagination and in a completely visualized embodiment, for the underlying

cryptographic principles are by no means obvious or such as would emerge gradually and naturally from working with the usual two sliding alphabets or with tables of alphabets such as those comprising the so-called Vigenere Square. Nevertheless, Jefferson's first description of his proposed device gives clear evidence of improving the invention as he was describing it. A second description, also found in his papers, is merely a clean copy of the first. It would be highly interesting to know whether Jefferson ever constructed or used the device; but on these points, too, the record is a complete blank.

The very earliest published description of a device almost identical with the one Jefferson proposed is found in a book[1] written by a French cryptographer, Commandant Bazeries, almost exactly a century after Jefferson wrote his description. Bazeries gives a rather detailed account of the events leading to his invention of le cryptographe cylindrique. It is quite certain that he could not have known of Jefferson's invention and it is equally certain that there was nothing in cryptographic literature which might have suggested the same basic ideas to both inventors. Not only are the cryptographe cylindrique and the Wheel Cypher identical in principle but also they are similar in their respective physical embodiments and instructions for usage. But Jefferson's device was more

1. Les Chiffres Secrets Devoiles. Paris, 1901, pp. 250-261.

secure because he proposed 36 "wheels," whereas Bazeries' device had but 20.

It is of interest to note that Bazeries' earnest endeavors to have his device adopted by the French Army were fruitless. It is equally interesting to note that in 1921 the U. S Army commenced using a device identical in principle and construction with the one invented by Bazeries, but the U. S. Army device had its origin in neither Bazeries' nor Jefferson's descriptions -- the same invention was conceived independently a third and, possibly, a fourth time, by two officers of the U. S. Army. By 1930, the Army device was being used by the other services of the U. S.

Jefferson's Wheel Cypher was an eminently practical device and to him belongs the credit not only for the first American invention in the cryptographic field but also for an invention which was so far in advance of the state of the art that it could be successfully employed over a century later by the armed forces of his country, not for a year or two, but for 20 years. It is safe to say that had U. S. communications employed his principle soon after he conceived it, they would have been far more secure against unauthorized reading than they were for at least a hundred years thereafter.

The eminent position Jefferson's invention occupies in the realm of cryptographic devices and in the history of

cryptography is well deserved. His astuteness in recognizing the weaknesses of the methods employed in his day places him far ahead of that other American genius for whom cryptography also had a fascination -- Edgar Allan Poe. The latter, so far as is known, never invented a cipher device or system but claimed supernormal ability in the solution of cryptograms; Jefferson, so far as is known, never solved any cryptograms but invented a cipher device and system satisfying the most important requirements of security, simplicity, and flexibility.

WILLIAM F. FRIEDMAN

Washington
17 November 1949