A RIVERBANK TROVE

David Kahn

ADDRESS: 120 Wooleys Lane, Great Neck NY 11023 USA.

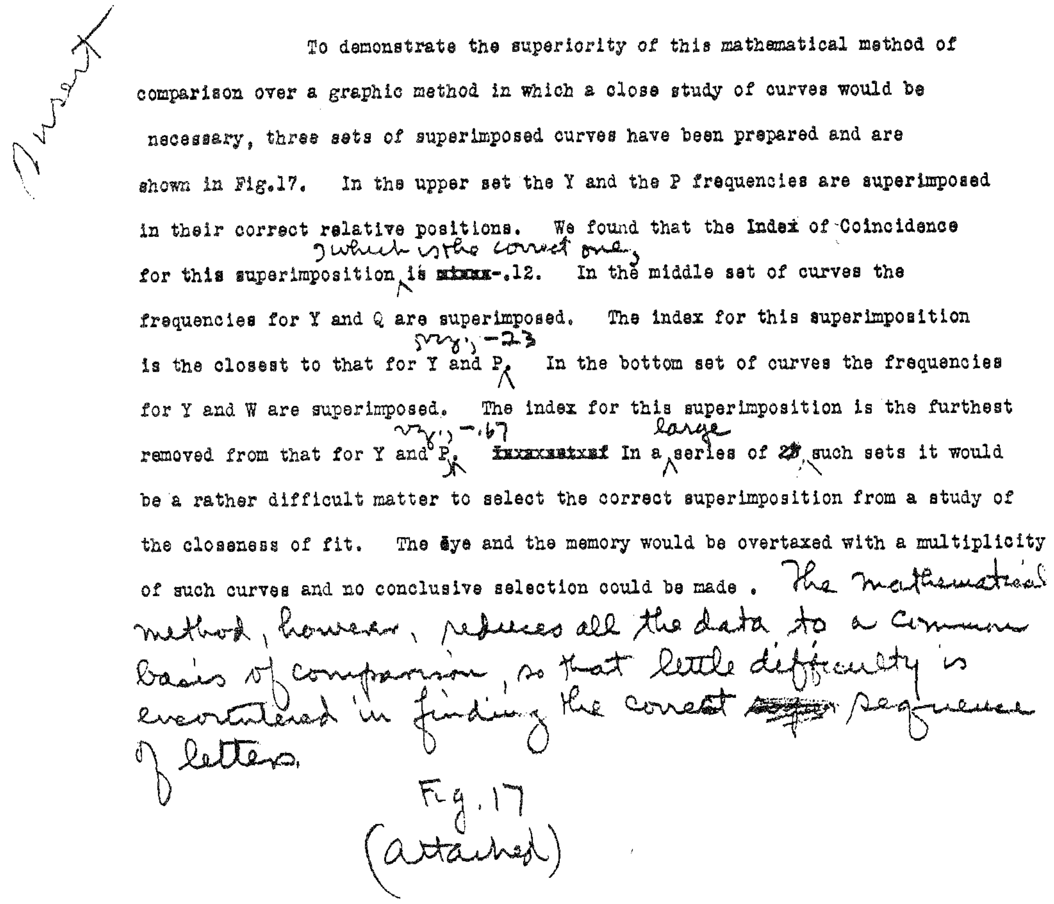
ABSTRACT: A proof with handwritten corrections by the author of William F. Friedman's Riverbank Publication No. 22, one of the most important documents in the evolution of cryptology, has been found at the New York Public Library.

KEYWORDS: Friedman, Riverbank, index of coincidence.

William F. Friedman's *The Index of Coincidence and Its Applications in Cryptography*, published in 1922, is universally regarded as one of the most significant publications in the history of cryptology. Friedman himself considered it as the most important of his many contributions to the field. It treated tables of letter frequency, not as collections of the counts of the individual letters, but, as Friedman said in its preface, as partaking "of the nature of mathematical or statistical curves." He stated correctly that "the occasions when such tables are regarded and treated as real curves having definite characteristics as entities, ... are rather rare; but when such a treatment is possible, it is one of the most useful and trustworthy methods in cryptography."

He went on to say that "In this paper two examples of such a treatment, leading to the solution of rather complex ciphers, will be given in detail. In the first one it will be shown how a cipher system involving more than one hundred unknown, random mixed alphabets can be solved without necessitating a single assumption of plain text values. In the second example, it will be shown how a multiple alphabet cipher system, involving both substitution and transposition processes in a somewhat complicated method, can be solved from a single message of no great length." The systems were the Vogel cipher, which Friedman says was devised by E. N. Vogel, chief clerk of the American Expeditionary Force's code and cipher solution section, and the Schneider cipher, invented by France's Major E. L. E. Schneider, who described it in a 31-page pamphlet in 1912.

The Index of Coincidence, I have written, "connected cryptology to mathematics. ... When Friedman subsumed cryptanalysis under statistics, he likewise flung wide the door to an armamentarium to which cryptology had never before had access." Friedman, 28 when he wrote it, had returned from service in



Insert

To demonstrate the superiority of this mathematical method of comparison over a graphic method in which a close study of curves would be necessary, three sets of superimposed curves have been prepared and are shown in Fig.17. In the upper set the Y and the P frequencies are superimposed in their correct relative positions. We found that the Index of Coincidence for this superimposition, which is the correct one, is ~~xxxxx~~-.12. In the middle set of curves the frequencies for Y and Q are superimposed. The index for this superimposition is the closest to that for Y and P, viz., -.23. In the bottom set of curves the frequencies for Y and W are superimposed. The index for this superimposition is the furthest removed from that for Y and P, viz., -.67. ~~Ixxxxxxtxxf~~ In a large series of ~~20~~ such sets it would be a rather difficult matter to select the correct superimposition from a study of the closeness of fit. The eye and the memory would be overtaxed with a multiplicity of such curves and no conclusive selection could be made. The mathematical method, however, reduces all the data to a common basis of comparison, so that little difficulty is encountered in finding the correct ~~[illegible]~~ sequence of letters.

Fig. 17 (attached)

Figure 1. Part of a page of the typescript of Riverbank Publication No. 22 with corrections in Friedman's hand[1]

G. 2. A. 6, the American Expeditionary Force's cryptanalytic agency, and was working as a cryptologist for George Fabyan, a millionaire cotton merchant who wanted to prove cryptologically that Francis Bacon had written Shakespeare's plays. He lived and wrote at Fabyan's think tank, the Riverbank Laboratories in Geneva, Illinois, an exurb of Chicago. Fabyan had published some of Friedman's early World War I cryptologic studies, which have entered the literature as Riverbank Publications. Fabyan reserved numbers 1 to 14 for other studies - never published - so the cryptologic studies began with No. 15. *The Index of Coincidence* was No. 22, and Fabyan, to save money, had it printed in France

[1] Reprinted with permission from the Bacon Cipher Papers, Manuscripts and Rare Books Division, New York Public Library.

Fig. 17

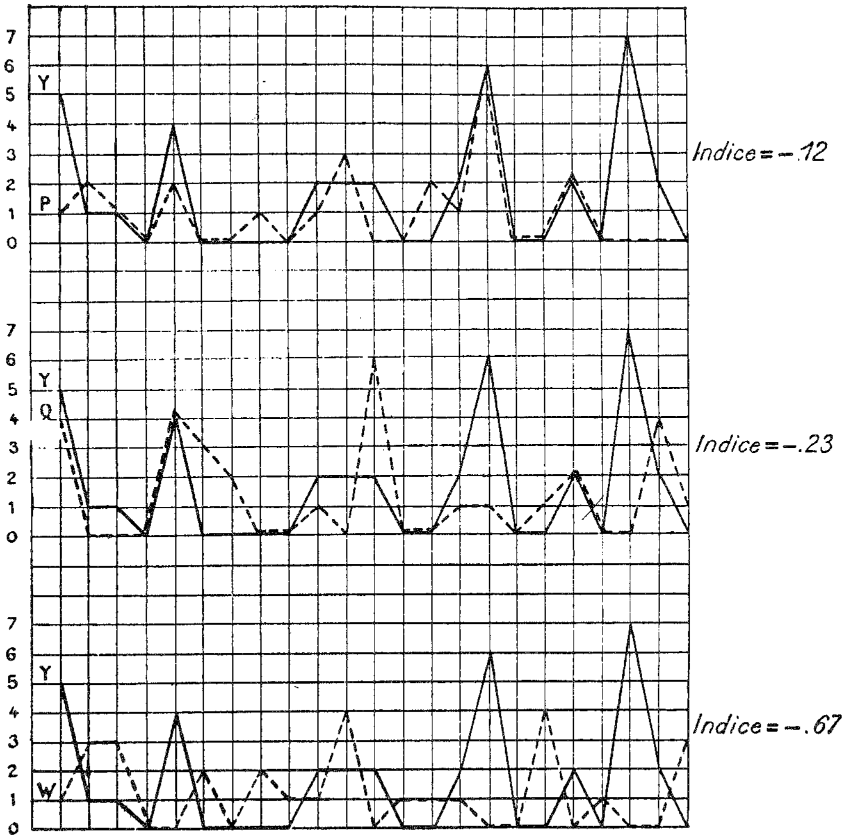


Figure 2. Figure 17 in the French translation of Riverbank Publication No. 22[1]

in 1922. General François Cartier, the head of the French Ministry of War's cryptologic agency, saw it, recognized its value, and quickly had it translated. He then had the military publisher Fournier, whose office was across the street from the war ministry on the Boulevard Saint-Germain, publish this translation, acknowledging it as such but falsely dating it 1921, as if the French had thought of this brilliant concept before the Americans. Fournier also published an English-language version, dated 1922. Neither credited Friedman as the author, but an edition published by Riverbank in 1922 did carry his name on the title page.

All this is well known in the history of cryptology. But nobody knew where the manuscript of this most important work was. It was not in Friedman's

[2] *L'Indice de Concidence et ses Applications en Cryptographie*, Publication No. 22. Paris FRANCE: L. Fournier. p. 40.

own collection, now in the George C. Marshall Library at the Virginia Military Institute in Lexington, Virginia. Nor had anybody - myself included - thought to ask where that original was. It is as important in cryptology as, say, James Joyce's manuscript of *Ulysses* is for modern literature.

One day, while working on my biography of Yardley in the Manuscript and Rare Books Division of the New York Public Library, I called for some files from the Bacon Cipher Collection. Cryptologists may imagine my astonishment and delight when, looking in Box 16 into folders marked "Schneider Cipher" and "Vogel Cipher," I saw typescripts of Riverbank Publication No. 22 with corrections in Friedman's recognizable clear handwriting. It was not the original manuscript, which seems to have vanished, not being either at Riverbank or in the Friedman collection. But it was as close as we are likely to get to it. A cryptologic treasure trove!

Friedman's corrections to the typescript all seem to be improvements in the clarity of the exposition. None change the basic idea. Though they are not substantive, and obviously not as significant as any changes Joyce might have made in his landmark work, they might interest historians of cryptology, and I therefore reproduce one here, with the kind permission of the New York Public Library.

ADDITIONAL REFERENCES

Oakley, Howard T. 1978. The Riverbank Publications on Cryptography. *Cryptologia.* 2: 324-330. This includes a memorandum by William Friedman to Oakley, in which he states that Fabyan sent the paper to Cartier, who had it translated and printed in French in 1921 and in English in 1922. It also includes the text of Friedman's inscriptions to Oakley on seven copies of the publications. These copies were donated by Oakley's widow, Marjorie, to the Special Collections section of the library of Georgetown University, where they remain.

Kahn, David. 1967 and subsequent printings. *The Codebreakers*. New York: Macmillan. pp. 374-384.

BIOGRAPHICAL SKETCH

David Kahn is the author of *The Codebreakers* and an editor of *Cryptologia.*