

DUNDAS PREBLE TUCKER
1829 SOLEDAD AVENUE
LA JOLLA, CAL. 92037
February 17, 1968.

Mr. David Kahn
c/o The Macmillan Co.
New York, N.Y.

VF110-1
Orig - Kan a/crow.
recently & thought it
might be of value to
you. Best,
Dave
P.S. Regards to all there

Dear Mr. Kahn,

I have just completed reading your well-researched and well-written THE CODEBREAKERS. Having been on the periphery of this subject professionally as a communication officer and cipher-machine designer, I can well appreciate the magnitude of your work in getting it out. Many of the U.S. Navy cryptographers you mention are known to me as friends or colleagues. I still keep up with Safford and Rochefort, having had lunch with the latter only a couple months ago, even though both of us have been retired from the Navy for a number of years.

In 1927 I served briefly under Safford in a U.S. Fleet Problem wherein I was able to crack the "enemy's" cylindrical cipher of the Jefferson type used by the U S Army. Later on in 1937-9 when I had the Research Desk in the Radio Division of the old Bureau of Engineering, I collaborated with Safford in producing the first design for the famous ECM which carried the Navy and many others safely through the war and afterward. One of the vivid recollections I have of that tour of duty is the day Safford and Friedman came into my office with a requisition for \$10,000 for me to sign. That was big money for my meager budget of those days, a budget which also had to take of radar and radio research as well as code and signal equipment. They announced they had cracked the new Japanese cipher machine and needed the money to build two models in our shop at the Washington Navy Yard. One was for us and one for Friedman's people. Although consumed with curiosity, because I was personally working on the ECM design with Safford and Reiber of Teleype at the time, I was reluctant to be privy to such an important secret and signed without question. That was my first and only contact with PURPLE. Shortly after that, I went to sea as U.S. Fleet Radio Officer under Richardson the year before the Pearl Harbor attack. Was never was active in cryptography again, because I was ordered to the Bureau of Ordnance in December 1941 to head up their new radar research section and finally wound up there as Program Director for Electronics, Guided Missiles and Nuclear Matters.

Having displayed some credentials in cryptology, rather modest ones to be sure, now I can offer you a few comments which you may find of interest and in return for the pleasure you have afforded me by your monumental work on cryptology.

One of the characters mentioned in your book I remember quite well: J F Byrne and his Chaocipher. I was the man who carried the burden of correspondence with him in the name of my Chief for the Navy. He was one of many crypto inventors which deluged Admiral Bowen's office after his incautious statement about the Navy's need for a secure crypto system. I was designated to take care of them in order to take the load off of Safford's overworked people. I was made no happier by Safford's comment that only one good idea had turned up from the public in the past 25 years, but had been well worth the effort of

keeping the door open all that time: the Hebern wired rotor. Hebern's designs were neither secure nor mechanically adequate for general service purposes, and the Navy spent large sums evolving a satisfactory machine based on the wired rotor principle. It must still be pretty good, judging from the paucity of your comments in its use. In fact, I am pleased at your silence regarding Navy WWII equipment and since, vis a vis the Army and State. It tells me the Navy has maintained its standards of quality and silence..

I have remembered Byrne because of his lifetime devotion to what he regarded as a major invention, his arrogant condescension towards we smug and unappreciative bureaucrats, and his utter dejection when I made him see its impracticability, something which apparently no one else had had the courtesy to do in rejecting him. Although he makes no mention of its basic weakness in his book, he also makes no mention of ever trying to market it again. Hitt could have saved him many years of hope and frustration had he pointed out its basic military weakness in the beginning. Byrne could then have directed his energies and resources toward applications where it might have been suitable.

Byrne's demonstration took place in the office of Jennings Dow, my immediate superior and my predecessor on the Research Desk. Wenger was there when I arrived and Byrne strode in shortly afterward, in shirtsleeves and with two obviously homemade articles under his arm. One was a box of wooden alphabet blocks as I recall, and the other looked like a big tambourine about 20 inches in diameter.

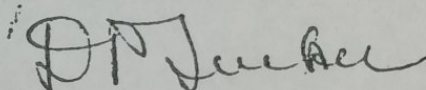
His manner was cocky and condescending. Dow and Wenger displayed a reserved cautiousness born of many encounters with eager and confident inventors. Being one at heart myself, I started asking questions. It quickly transpired he had an auto-key system which depended on the correct decipherment of the previous letter and the correct reception of the cipher letter. The blocks were also transposed in a manner which I did not go into once I realized he had an auto-key. I asked what happened to the deciphering process when he encountered a garble. He said that stopped further decipherment until the garble was cleared, but that in his experience with telegraph and cable, such garbles were rare. I told him the bulk of Navy traffic went by radio where our average garble rate at that time was 6%. He mumbled something about thinking the Navy had perfected radio, and visibly wilted. Having faced the moment of truth a few times myself with pet ideas, I realized how badly he felt and suggested that since both State and Army used cable and teletype extensively, his system might interest them. It is only now after reading his SILENT YEARS from the local library that I realize my effort at kindness only made things worse.

I think both you and Farago underestimate Safford's cryptologic ability as a whole. While I know Safford would be the first to hail Friedman as his master with cryptanalysis and the source of much help, I consider Safford his superior as a cryptographer and Rochefort says Safford is a topflight cryptanalyst even though R is not especially cordial towards S. on a personal basis. Safford started ten years later than Friedman with a box of codebooks inherited from the British Navy in 1924 and by 1927, when I met him, had acquired an amazing grasp of the entire cryptologic field and had started an organization on a shoestring which achieved the highest cryptographic security in the world by WWII. In 1927 he told me of weaknesses he had discovered in British and Japanese systems which were still present in WWII. As for the State Department, even my enlisted radio-men in China who handled State traffic used to spot security breaches in the traffic we handled for them. He was an utterly sincere, able and inspiring

leader who was more responsible than anyone else for the Navy's high degree of communication security and intelligence from 1924 until he retired five years after the normal retirement date for Captains. He deliberately sacrificed promotion in the interests of maintaining the Navy's security, because cryptology was the deadend in the eyes of the line promotion board. Furthermore, he lays things on the line and does not play politics - I doubt if he knows how. He deserved every cent of the \$100,000 just as much as Friedman in the Congressional award. He showed his strength of character in the Pearl Harbor investigations when he stood his ground while everyone else was wilting under the intense pressure. . Very few except those directly involved realize how intense and ruthless that pressure was, particularly in the Army, and especially on Safford in the Navy. All in all, Safford is one of the great, if unspectacular, heroes of modern cryptology. Without him, there probably would have been no victory at Midway, for he was Rochefort's, Dyer's, et al, mentor and founder of the team, as well as its coach.

This letter has stretched out much farther than I intended when I started. I can not close however without expressing again my admiration for your outstanding work which will endure as a landmark in its field for many generations. I am glad you have avoided many of the controversies, or at least taking sides, that are endemic in this field, thereby achieving your goal of entertaining and informing.* I have learned a great deal.

Very sincerely,



Rear Admiral, USN, Retired.

* You have summarized the official and establishment case against the conspiracy theory of the revisionists very well on page 976, and have satisfied yourself that it is the proper side to be on in this controversy. To date I have had to bring in a Scotch verdict for myself. There are still too many suspicious circumstances not satisfactorily explained. Too many people at the working level had 20-20 foresight as well as hindsight. Safford, for one, took action to order the destruction of code and cipher publications which might be compromised by Japanese hostilities, at the time "Winds Execute" message came in. Intelligence desks in both the Army and Navy got out memos to their seniors pointing out the significance of the 1300 delivery time of the 14th part of the dispatch to Nomura. With the exception of the Navy Court of Inquiry composed of competent men not particularly fond of Kimmel but who cleared him, none of the other investigations were composed of an unbiased or competent majority. The Roberts inquiry was a farce and a travesty by any fair standards. Much of the PHA testimony was contradictory and palpably false. Probably the most significant indication is the long list of qualified witnesses which were carefully not called in both investigations. The odds are that history will probably support your viewpoint, at least until the unlikely event of some irrefutable contrary evidence comes to light later on. On the other hand, the conspiracy to whitewash and cover up afterward is quite evident and most suspicious in itself because of its extraordinary ruthlessness, mendacity and extent. Hence my own reluctance to pass judgment yet. Furthermore, these are only a few and less publicized arguments. At any rate, the revisionists have a much stronger case than the Baconians who survived for so long!