REF ID:A70020

SPSIS-3

26 June 1944.

Mr. David Kahn, Windsor Gate, Great Neck, New York.

Dear David:

I am sorry that I cannot accede to any of your requests in your letter of June 13, as much as I would like to. In connection with your question as to whether your soldier friend can get the Signal Corps bulletins and give them to you, I do not think he had better try that as the laws are very strict.

We cannot send you any material of the kind that you asked about in connection with bootleggers during prohibition nor have we any material that you could work upon during the summer. It is thoughtful of you to volunteer to help.

I can appreciate your desire to have a photograph but I am afraid we cannot make one available to you. We are quite different from movie stars in this respect, but you can understand that this is necessary for the sake of the work.

Sincerely yours,

William F. Friedman, Director of Communications Research.

Approved for Release by NSA on 07-16-2014 pursuant to E.O. 13526

	F

EF ID:A70020

HEADQUARTERS ARMY SECURITY AGENCY WASHINGTON 25, D. C.

18 January 1946

Mr. David Kahn Windsor Gate Great Neck, New York

Dear Mr. Kahn:

Ŀ 1

I am sorry that I have been unable to answer your letter before this. I am also sorry that I cannot do better for you in answering the questions you asked than is indicated in the enclosure. It is not that I do not wish to give you all the information you desire, but that I cannot do so under regulations which are still applicable.

Very truly yours,

WILLIAM F. FRIEDMAN Director of Communications Research

l Incl: List of questions



SOLVING SIMPLE SUBSTITUTION CIPHERS CRYPTO-INDEX

DAVID KAHN Windsor Gate Great Neck New Yoxkt Editor, S-TUCK Publisher, NEON

فستر: به

PUBLICATION OFFICE and HEADQUARTERS . ROCHESTER, NEW YORK

EDITOR, SHERLAC

Cipher Editor, TRYIT Foreign Editor, EMPTY

Col. William F. Friedman Office of the Chief Signal Officer Headouarters, Army Service Forces Washington 25, D.C.

Dear Colonel Friedman:

Perhaps you remember me. I am David Kahn, and wrote to you on June 13 asking for information, which in a letter (SPSIS-3) you siad that you could not give me. I fully appreciate why you could not give me the material, them, at least. Maybe, this time, you can help me.

Is there any information that you can give me now concerning the Japanese codes, and the machine which deciphered them? Is there any information that you can give me concerning the use of the Hagelin machine during the war, by the Americans and Germans? I could go on like this forever, asking for information on this particluar thing or that, but I'll generalize it, and ask:

IS THERE ANY INFORMATION ABOUT CRYPTOGRAPHIC AND CRYPTANALYSIC METHODS USED BY THE UNITED STATES OR THE AXIS POWERS THAT YOU CAN GIVE ME, PRINTED OP. OTHFFWISE?

By printed information, I mean press releases, etc., and by otherwise, material which you can give me in a letter.

By the way, may I ask why cryptANALYTIC methods are so secretive? I'm sure the fixis powers have a way of decrypting our messages, so what difference would it make if they found out the same thing,--for undoubtedly they found the same weak points in the Hagelin machine that we did.

REF ID<u>#A</u>7<u>00</u>20

Perhaps in my eagerness to learn I'm overlooking things which I shouldn't, but if I am, won't you tell me what they are so I won't bother you again about them.

Could you also send me as much material about the breaking of the Jap code and the Hagelin machine as possible?

Here are a number of publications which I read about in Dr. Galland's book, and which, if you can, I would like you to send me. I have marked with a star (*) those which he has marked as not being available for the public, but his book was printed during the war, and it is now peace. So I hope that you can send re copies of them. Please notethat the one by Turkel is available for distribution. By the way, can Signal Corps Bulletins be bought now?

TURKEL, Enciphering with Apparatus and Machines, (trans. from German

by War Dep't, 6-20-34.

*FRIEDMAN, Elementary Military Cryptography, (1935 edition) Special Text 16: *FTIEDMAN, Advanced Military Cryptography (1935 Edition, Special Text 166) * TFIEDMAN, Military Cryptanalysis (1944)

Won't you fill out the enclosed sheet and return it to me, along with a letter of your own which goves other information? Thanks in advance.

A

Very truly yours,

VERY MERRY CHRISTMAS TO YOU 2