Rosepark House (160)
Upper Newtownards Road
BELFAST BT4 3NR

M Frode Weierud
4 Le Pre Vert
1041 Route De Mategnin
F 01280 Prevessin-Moen
FRANCE

2 October 1996

Dear Frode

Thank you for your letter of 2 October and its enclosures.

I should have written before now to thank you for the Opendoor disc and the Enigma simulator, but at least I have done so on the phone. My apologies, but as you know, I have not been up to scratch over the past few months.

I enclose a copy of-

> Enclosure (A) (analysis of CCM keys) and (B) (period of CCM);
> a memo of 24 July 1944 on testing the CCM (and its flaws);
> signals from GCCS of 10 and 11 March 1945 (typed by me, as the copies I have are poor - the few omissions (indicated by dots) are not relevant (indicating copies to other people and so on);
> a page from an article I am writing on "Typex and the Admiralty", which summarises some of the facts about the CCM, mainly based on the above.

I'm not now sure whether or not to change the title of the article to "Typex, the Admiralty and the Combined Cipher Machine", in view of what I think are quite significant findings about the CCM. I may not have sent you the whole article, but would be happy to do so. While not all of it is new, I have found out that the Admiralty ordered Typex in 1939. Hinsley is again wrong.

I also have some very detailed pages of an analysis of the CCM's stepping, using a "fix" which consisted of a link between the 1st and 4th rotors. But since I am not able to do any copying myself at the moment, this will have to wait for a week or so. On different subjects, I then hope to send some of the BP memos (most are not very interesting) and a little on the ISOS, ISK and GIMP (short for "German impulse" ciphers. The latter papers really consist mainly of lists of the ciphers involved and their dates. I will also send three pages on Typex Mk 22 (probably a post-war development, since the reflector was pluggable and it was issued to Royal Navy destroyers).

I have found a little more out about Typex. The period with (the wartime) four notches was 4394 (per the US SSA analysis marked "for US eyes only" (but containing no real detail!). Interestingly, that was CCM's minimum period - with good rotors. The CCM seems to have used sets of 10 reversible inserts ("R" in the lists of rotors indicating the reversed version). Nine notches were first proposed for Typex in January 1945, along with other changes to Typex, strongly suggesting they came into service post-war. Typex Mk 22 had nine notched rotors for the inserts at A C E I N Q T V Y. All Mk 22 rotors had nine notches.

If Typex with four notches had a 4394 (= 17576/4 or 26x13x13) period, it strongly suggests to me that the Typex stepping action was slightly different ~~to~~ from that of Enigma (was commercial Enigma the same as military? Typex designers probably saw only the

((26-4)/2)×26

former, at least for many years). I cannot get your new formula for Enigma to provide a 4394 period for Typex (4 notch). Deavours and Kruh say that four notches gave a ((26-4)/2)*26 cycle for two rotors. But that can scarcely be right without qualification and much more explanation (or at least is very misleading), since that does not lead to 4394. Since D & K worked only from photos, I do not see how we can be sure that Typex was the same as Enigma. It was supposed to be different (quite how is not clear). My guess is that Typex did not have the same movement anomaly feature as Enigma.

Please do not do any further work on Typex's period on my behalf, the 4394 period is adequate for my present purposes.

Please do not pass on the CCM papers, or say anything about what I have found, as I am hoping to publish.

Thank you for your good wishes about my so-called "yuppie flu". "Flu" is actually a bit of a misnomer. The better name is "chronic fatigue syndrome", but mine (like many) was triggered by a virus - last winter. No one knows anything about much about it and there is no easy cure. There was something about it in some of the English papers on Thursday, 3 October. I am not too bad a case, but small upsets set me back a few weeks. I doubt if I will be back at work. However, I have just been cheered to hear that I will be allowed to use the Library facilities when I do fully retire.

As to the Internet for e-mail, I have no immediate plans to join, as I do not have enough e-mail contacts at present. But continental, especially Swiss, postal charges horrify me. Please be careful as to how much you send me - double-sided copies would be fine, even if they were upside down on the reverse page, as happens to me sometimes!

Incidentally, some Venona material is apparently on the Internet.

It was interesting to read about the PRO CD-ROMs. I imagine they will go in for this kind of release more often in the future. It would be terrific to have some of the decrypts available that way, but I doubt if the market is big enough. On the whole, the PRO is not advanced on the IT front. The indexes are obviously prepared on word processors at present. The printed index to HW 1 (part of the C archive - the decrypts shown to Churchill) are very detailed, but a bit of a pain to use, because they are so long - ideal for being studied at home. I suggested that they make them available on floppy disc in Ascii form. But the PRO does not have them on disc in the first place! I can only assume that the PRO received them direct from the relevant department - probably MI 6 (SIS).

I also enclose a couple of blank discs to make up a bit for those with programs on them which you have kindly sent me at various times.

Best wishes

Yours sincerely

Ralph

R ERSKINE