Annex 17. David Sissons to Kenneth McKay, 28 November 2004

22 SAVIGE ST
CAMPBELL
A.C.T., 2612
<d.sissons@tpg.com.au>

28 November 2004

Mr K.L.McKay
[redacted]

Dear Ken,

Many thanks for your very prompt and effective response of November 18th and November 23rd to my request for assistance. It is very kind of you to help me in this way. I am very much in your debt.

Please excuse my delay in replying. Because of my ignorance of such techniques it has taken me several attempts to absorb your suggestions.

You may remember in 1945 my passing around John Buchan's short story *The Loathly Opposite*. It purports to be the tale told by the Director-General of G.C.&C.S. when it was his turn to address the dining club of V.I.Ps of which he was a member. It was Buchan at his most dramatic and the characters were writ large. Some of the dialogue promoted considerable merriment among you and your colleagues. Here are a few typical pieces.

> 'I had besides a metallurgical chemist, a golf champion, a leader-writer, a popular dramatist, several actuaries, and an East-end curate. None of them thought of anything but his job, and at the end of the war, when some ass proposed to make them OBEs, there was a very fair imitation of a riot...
>
> 'Once you have written out the letters of a message numerals there are many means by which you can lock it and double-lock it. The two main devices, as you know, are transposition and substitution, and there is no limit to the ways one or other or both can be used.... By way of an extra complication,

> too, the message, when decyphered, may turn out to be itself in a difficult code. *I can tell you our job wasn't exactly a rest cure*'.
>
> Burminster cried out like one in pain 'It can't be done. Don't tell me that any human brain could solve such an acrostic'.
>
> 'It was frequently done'...
>
> '*Give me the trenches*' said Burminster in a hollow voice. '*Give me the trenches any day*'...
>
> 'We called this particular cypher 'PY', and we hated it poisonously. *We felt like pygmies battering at the base of a high stone tower*'.

For the next few days, whenever confronted with a troublesome passage, Ron or Eric would come out with one or other of the exclamations italicised above.

I'm afraid that, devoid of both experience and aptitude, I feel very like one of the aforementioned pygmies. So, please continue to be patient with me in your explanations

UK versus KU

In the third paragraph of your letter of November 18th you write: 'From my UK/KU example you could guess that if *b-j* is right then *h-e* is to be preferred to *e-h*, or vice versa'. Could you spell out the logic of this in more detail for me, please. If KU in *j-b* and not UK in *b-j* is right, why is it then more likely that *e-h* and not *h-e* is right. In fact in each of these cases KU=*ru* is correct. But why does this follow? In the whole message KU/UK occurs 11 times—on seven of these occasions it is KU=*ru*, on the other four occasions it is UK=*comma/period*; but until the code-values are known, had the cryptanalyst any grounds for suspecting a preponderance of KU over UK?

You return to this problem in the 3rd-last paragraph of your letter of November 23rd—in the context of all seven blocks of our specimen message. In the whole message GO/OG appears 11 times, of which GO=*no* accounts for 7 and OG=*begin English* for only 4; but I can't see what grounds the cryptanalyst would have for considering OG the more likely.

Sinkov's Chaining

I'm much encouraged by your suggestion that Sinkov's chaining technique may be the answer to our problem. (Incidentally, why is it that in Sinkov's example he can chain all 8 columns in a single operation but in our's we arrive back at 1 after only 1-4-9-2-8?). You suggest that chaining may limit us to only two possibilities—10-2 6-9 7-4 3-1 5-8 or its exact reverse 8-5 1-3 4-7 9-6 2-10. This is exciting; for it seems to be exactly the situation that Trendall had reached—he was, before he knew any code values, providing keys correct in every particular except that they were reversed. I'd be most grateful for any subsequent thoughts you may have on this.

Budge

I think I may be able to reduce my search for bibulous Budge in the Dept of Veterans Affairs roll to manageable proportions if I can narrow down his age group. In the 'pep talk' that Ron gave me on my arrival, he described him as 'an older man who is unlikely to last long in jungle conditions'. Can you narrow that down a bit further— e.g ten years older than yourself? Twenty years older than yourself? In my day there were two or three Sigs, who used to alternate. The one who was there most days was Cpl Power (who participated in our *sezumba* conspiracy at Ian's expense). According to the Veterans roll Power was born on 28/11/07 and served with 4 Aust Special Wrls Coy in Greece and Crete in 1941. Hence he would have been 37 in 1944. Do you remember Budge as the older of the two. One of Power's reliefs that I remember (Finlay?) was much older—he told me that he was a telegraphist on *H.M.A.S. Sydney* when she engaged the *Emden*. (I suspect that Finlay had a gambling or a drinking problem; for at our first meeting he tried to borrow money off me).

The Emperor's Codes

I found this one of the best books on the subject. The author makes very enterprising use of extensive British documentation until very recently withheld from public access. It provides chapter and verse for the decision in late 1942 to disband Nave's organization. Apparently it was a decision taken at the highest level (in which Bletchley participated) and not, as Archer believed, unilateral action by Cdr Fabian and his American superiors.

Once again, many thanks for your expert and patient assistance. it seems to me that you have solved the thorny problem. My hearty congratulations.

Best wishes,

(D.C.S.Sissons)

4