

# Annex 18. David Sissons to Kenneth McKay, 19 December 2004

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

19 December 2004

Mr K.L.McKay

Dear Ken,

Many thanks for your very helpful letter of December 2nd in response to my queries of November 28th.

I'm not sure that I fully understand your explanation of how far the cryptanalyst could establish the correct sequence within each bigram pair from the occurrences of OG/GO bigrams throughout the whole *Takasago Maru* message.

It seems to me that all he could say is that they are probably a mixture of a frequently occurring code-group and another less common group. Suppose he arbitrarily opted for one throughout, settling on GO. This would provide him, in the page of alternatives attached to your letter of November 21st, the following pairings: in Block 1 j-b, in Block 3 c-a, in Block 4 g-d and either f-i or i-f (alerting him to the fact that in this message both code-groups GO and OG are present), and in Block 5 h-e. In the case of j-b, c-a, and g-d he would have been correct; in the case of h-e would have been wrong. Thus, because GO represents *no* (the possessive suffix and the adjectival suffix), one of the most commonly occurring syllables in the Japanese language, and because OG, 'English spell' is a rarely occurring group, he would have achieved a limited success, securing the correct sequence in three out of five of the bigram pairs. But is this limited success of any use to him? Can he make use of it as a first step towards the correct pairing of the other two bigram columns?

In the hope that another long message might help, I encoded in GEAM using the same key (FGFGF) the famous '*Winds*' *Code Set-Up* message of 18 Nov 1941 (Attached). My hopes, however, were disappointed. I'm afraid that I can get nothing out of it.

One interesting thing, however, emerged. Unlike the *Takasago Maru* message, this '*Winds*' message does not contain the code-group OG (=Spell English). Furthermore, it appears to me likely that only a small proportion of messages would contain 'Spell English'. Therefore, if the cryptanalyst had believed that the GEAM code contained only the one code-group GO/OG, he would on the basis of the *Winds* message have paired all five of the bigram columns correctly; for as luck would have it GO is present in each of the five. Trendall, however, was aware that the Japanese diplomatic code vocabulary was so large that every bigram and its reverse had to exist as code-values. Similarly he had no means of knowing that of the two possibilities, GO and OG, one was relatively little used. It is therefore to me inconceivable that Trendall would have resorted to such a dangerous procedure to solve the pairing problem.

In the blocks I have underlined some long repeats. These, however, did not show up on the message-pad. I don't know whether they can be of any help towards a solution.

And so it looks as if I must, at last, admit defeat and throw in the towel. You went to a great deal of trouble to help me. I do apologise for wasting your time.

Many thanks for your great help.

With very best wishes to you and yours for a Merry Christmas and a Happy 2005,

Yours sincerely

(D.C.S.Sissons)

Encl: 1