NOTES ON ADFGVX SOLUTION

It was not assumed that two of the messages were of the same length; that was quite an accident of which we were enabled to take advantage. Such an accurance is not necessary. However it might be pointed out that its occurrence was more frequent than would occur by chance due to the German practice of breaking up long messages into shorter sections, sent separately.

If two messages of the same size were not available, some assumption could be made about the width, in keeping with the knowledge that it is odd or even. Then two messages differing by a number of letters equal to a multiple of the length of the key could be treated in exactly the same way as the two messages of identical lengths. Such pairs of messages would surely be available as one would ordinarily have had more than twelve messages in any day's traffic. (Cf. Publication entitled, German Military Ciphers from Feb. to Nov. 1918, by J.R. Childs, P. 13 par. 2. "The number of messages which were intercepted in the cipher (ADFGVX) varied from 25 a day upon the inception of the system to as great a number as 148 during the last days of May").

This assumption of width would answer all the objections about using sets of ten letters and would permit the determination of where the reversal takes place without any particular difficulty. In fact the correct assumption would lead to a ready determination of the breaks between the various columns.

The simultaneous appearance of V and X in positions 22 and 23 is of oustanding importance because of the difference in frequency of these two letters in the two tables. It is by no means the same phenomenon as the repetitions at 14-15, 44-45, etc.

* * * * *

It is certainly true that the solution as given takes advantage of the particular messages at hand. This is a peculiarity of Cryptanalysis itself. It is not possible to give a general solution for a cipher system in the same way that one can give a general solution for a problem in Mathematics. In Cryptanalysis general principles may be laid down, but then illustration requires a particular example which of necessity is in some respects unlike any other particular example.