New York, Sep. 18th, 1935

Dear Friedman:

Since I last wrote you I have put in some more time on the ADFGVX Cipher, and have come upon some points in the "general Solution" which seem to me to require more light before I can satisfy myself that this is indeed a general solution.

I certainly have no desire to discount the pretty solution of the messages given. If I mention or intimate the existence of luck in the solution, it is not that I wish to disparage luck in connection with cryptography. On the contrary, I know from experience how to value it; and I am convinced that a cryptographer can no more get along without it than a physician. - And now to my points.

Any solution of the ADFGVX System must depend on a determination of 1) the number of columns in the transposition rectangle, and 2) the number of letters in each column.

The assumption that the material at hand for this purpose will include 12 messages written in the same key is a perfectly fair one, based, no doubt, on actual war-time experience. Is it equally fair to assume that 2 of these 12 messages will contain the same number of letters? Even in the 12 messages given the variation in the number of letters per message is considerable - the shortest has 108 letters and the longest 254; still two of them contain 186 letters, and this fact plays a prominent part in the solution, increasing as it does the material on which the opening steps are based.

The principle of "Reversals" is, of course, basic in the solution, and is sure to be of service when circumstances allow. I think it would have been well to point out that these reversals will appear only (a) if the first of two columns has an odd number of letters and the second is of the same kind (i. e. + or -) as the first; or (b) if the first of two columns has an even number of letters and the second is of a different kind from the first. To state the same thing negatively: if the first of two columns has an even number of letters and the second is of the same kind as the first - or if the first has an odd number of letters and the second is of a different kind from the first, there will be no reversal as between these columns. Roughly, and without actually calculating the probability, this a fifty-fifty chance. The test messages begin with 3 odd columns each containing an odd number of letters, and that is a piece of good fortune which the solvers very properly used to good advantage - but it is a piece of good fortune none the less, and its recurrence cannot be counted on.

Suppose col 4 had followed col 1 (I am using the col numbers of the transposed text , i.e. as the message was sent); the first two sets of ten letters would then show

1st ten			2nd ten			
odd		even	odd		even	
1	A	6	2	A	1	With weights according to Figs
3	D	1	7	D	2	1 and 2 of the text, these figure:
0	F	2	0	F	2	1st ten, odd-even 148, even-odd 104
3	G	0	4	G	4	2nd ten, odd-even 196, even-odd 176
2	V	1	1	V	1	
1	X	0	0	X	0	There is no reversal

Now let col 5 follow col 4, not forgetting that two letters of col 4 remain to be used. The third set of ten will now show:

3rd ten		
odd		even
3	A	2
4	D	4
2	F	0
0	G	2
1	V	1
0	X	1

odd-even 148, even-odd 123.

Again there is no reversal.

The further along we go, the more the sets of ten are bastardized. Thus, 51-60 contains 5 letters from each of two columns, and any work put on such a set of letters could, of course, yield valid results only through the arrival of Santa Claus.

The opening analysis shows that the second set of ten letters is preponderantly of a different nature from the first. Why sets of just ten were chosen is not stated - of which more a bit later. The conclusion is drawn that there is a reversal "near the tenth letter." Then we read, "This same sort of reversal takes place in the third ten, but this time the break is definitely indicated. The simultaneous appearance of V and X in the sequent positions 22 and 23 indicates that 22 is the end of one column and 23 the beginning of another." It is true that a foot-note points out that the point is not absolute, and is merely "an indication based upon probabilities." This remark belongs not in a foot-note but in the text proper so that it may receive due consideration. As a matter of fact it receives no consideration whatever: from this moment on the column length of 11 letters is assumed to have been proved. The way was paved for this conclusion in the italicized statement on page 3: "A reversal of this alternation indicates the end of one column and the beginning of another." I cannot convince myself that the 11-letter column length has really been proved at all.

In itself the simultaneous appearance of V and X in positions 22 and 23 proves little or nothing - at most it may arouse a suspicion. In the two messages under consideration the phenomenon appears 6 times - at 14-15, 22-23, 44-45, 67-68, 120-121 and 179-180. Three of these occurrences mark column divisions and three do not - surely there is no strong indication in that.

Possibly the text means to say that when, for other reasons, there is a suspicion of break, then and then only the phenomenon may indicate the point of the break. Even that is, I think, too strong an assertion; and in this connection I point back to what I said above as to the test based on two sets of ten letters each.

Why just ten letters? It seems to me that a cryptanalyst examining the two messages, especially one who is ready to be impressed by the VX recurrence might more readily have chosen 14 than 10 because the same phenomenon occurs there. He would then apply his odd-andeven tests to the first and second sets of 14 with the following result:

1st 14			2nd 14		
odd		even	odd		even
1	A	6	1	A	0
4	D	1	2	D	5
1	F	3	4	E	3
4	G	3	3	G	2
2	V	1	1	V	1
1	X	0	3	X	3

These show by weighted frequencies,
1st 14, odd-even 196, even-odd 157
2nd 14, odd-even 191, even-odd 197

We should have a rectangle with 9 columns of 14 letters and 4 of 15. We may consider the second column one of 14 letters with a reversal (not very strong) or one of 15 (odd-even 208, even-odd 197) without a reversal. In the latter case the second column (no reversal after a column with an even number of letters)

would be of the same kind (say +) as the first.- The would-be solver would be up a tree. But so I believe would the actual solvers of the messages except for a piece of luck: they noted the VX repetition at 22-23 and drew conclusions which seem to me not warranted, and these conclusions proved correct. Our hypothetical solver drew conclusions little if any less warranted and came out wrong: one man's meat and another man's poison!

I find myself unable to agree with the argument on page 5 demonstrating that all the first five columns are long: "Employing the same reasoning as before, it is quite evident that there is a break between 55 and 56." The break between 22 and 23 was assumed mainly because of the VX phenomenon there; nothing of that kind occurs here. The only other previous reasoning that can apply is that brought to bear on the first twenty letters (page 4, top). The conclusion drawn there is that "this reversal would indicate that column 1 of the transposition rectangle* ends somewhere near the tenth letter." How can the evidence here be said to point to more than a break in the neighborhood of 55 - to a break at exactly 55? The point is important, because from this conclusion that there is a break at 55 is drawn the further very weighty conclusion that the first five columns are all long. Suppose we examine the matter a little further.

Let us assume the correctness of the conclusion that there is a break at 22, and that columns 1 and 2 contain each 11 letters and are + columns. Let us now arbitrarily suppose that column 3 contains 10 letters and is the short column of the message. Column 4 and all subsequent columns will then be long. I see nothing at this point - nothing indeed short of the actual correct arrangement of the columns - to contradict this assumption; following the text, columns 5 and 6 (letters45 - 55 and 56-66) compare as follows:

col 5			col 6		
odd		even	odd		even
4	A	3	0	A	3
4	D	0	5	D	3
0	F	3	0	F	3
2	G	4	2	G	1
1	V	0	5	V	0
1	X	0	0	X	0

Weighted Freq acc'g to Figs 1 and 2:
col 5, odd-even 154, even-odd 121
col 6, odd-even 206, even-odd 139

On the assumption that 3 is a short column, col 5 would contain letters 44-54 and col 6 letters 55-65, showing

col 5			col 6		
odd		even	odd		even
3	A	4	3	A	0
2	D	4	3	D	4
3	F	0	3	F	0
4	G	1	2	G	1
0	V	1	0	V	5
0	X	0	1	X	0

Weighted Freq as before:
col 5, odd-even 137, even-odd 160
col 6, odd-even 138, even-odd 189

Both 5 and 6 are now minus where they were plus before; but what is there at this stage to show that this is wrong?

*The term "transposition rectangle" seems to be used in two contradictory senses. Here, and in the third line below figure 4 (page 5) it means the rectangle after transposition has taken place; 6 lines above the bottom of page 6, on the other hand, it means the rectangle containing the message before transposition - or I so understand it.

The conclusion that the first 5 columns are long is vital to the reasoning of page 6, which places column 2 in the original transposition rectangle. And even then the column is placed through the presence in the twelve messages of a message with one additional short column - a new piece of good fortune to add to those already mentioned.

I shall be much interested to hear what the message solvers say on these points - and glad to be corrected where I am wrong.

Cordially yours

Charles J. Mendelsohn