

312 *Comes*  
*Personal*424 N. George Mason Drive  
Arlington, Virginia  
8 February 1949Professor George E. McCracken  
977 25th Street  
Des Moines 12, Iowa

Dear George:

Under separate cover I am sending you the copy of ISIS for your autograph.

I have gone through the article again and compared it with the original article which you wrote some years ago and had dittoed. The article as it appears in ISIS is a very great improvement on the original, although I must say that I found certain of the footnotes in the latter rather interesting. In particular, I appreciated the translations of the Latin which, of course, you could not include in the ISIS version.

Your article reminded me that I had at one time concluded to make use of the term "steganography" to apply to what we now call the field of "open code" and I will get the Terminology Committee to do something on it.

On page 218 right after the thingamajig which separates the top section from the bottom, there appears a line beginning "At the head of his work Kircher prints (2) the following paragraph . . . ." What on earth is the "(2)" there for? Is it a misprint?

I did not find your description of the code system too clear. It seems to me also that you might have called attention to the fact that from a technical point of view the "decode" section of Kircher's code is really the "encode" and vice versa, because obviously it is only in the Latin list where "encode" and "decode" entries are identical and, since the work was intended for polygraphic purposes, the arrangement for Latin was not too significant. Another thing you might have mentioned is that attempts have been made in very recent times to do what Kircher attempted.

- 2 -

These attempts are exemplified in the Marconi International Code, put out a few years ago by the Marconi Telegraph Co., and in the International Code of Signals, put out by the International Telecommunication Union.

I am a bit afraid that you have given too much credit to old man Vigenere on page 223. I don't think that Vigenere was "one of the greatest cryptographers who ever lived" nor was it he "who first introduced the basic idea of polyalphabetic substitution." The latter goes back even beyond Porta, who mentions it; Alberti certainly used and talked about polyalphabetic substitution.

I wonder whether you have ever seen Mandelsohn's article on Vigenere. If you haven't, I will be glad to send you a reprint with my compliments.

On page 224 in the example of cipher text, in the right hand column, the fourth item should be "23" and not "33". You unfortunately carried this error over from the original article. I saw that you had already picked up one typographical error on page 216, which is a rather unfortunate one. I checked every single encipherment example!

I, too, wish there were some explanation of that very peculiar and not particularly amusing story attributed to Porta, which you have mentioned on page 226. I wonder whether a more careful search through Kircher's text might not give some clue?

Finally, with reference to the magic square, it is a mighty good thing that the magic square is based upon the number "34" because had it been "33" or "35" there are lots of people who would say that it refers to Bacon. For if you sum the numerical values of the letters of the name you get either 33 or 35, depending upon whether the letter "j" is in the normal sequence or not. It is possible that a search through the Kircher book will give some significance to the number "34". I'm sure it had some.

I have, as you see, gone over the article pretty carefully and some of my comments are probably of a minor significance. I have already told you that I think you did an admirable piece of work and one which is worthwhile. I will be very glad to have your comments on my comments.

With cordial greeting, I am,

Sincerely yours,