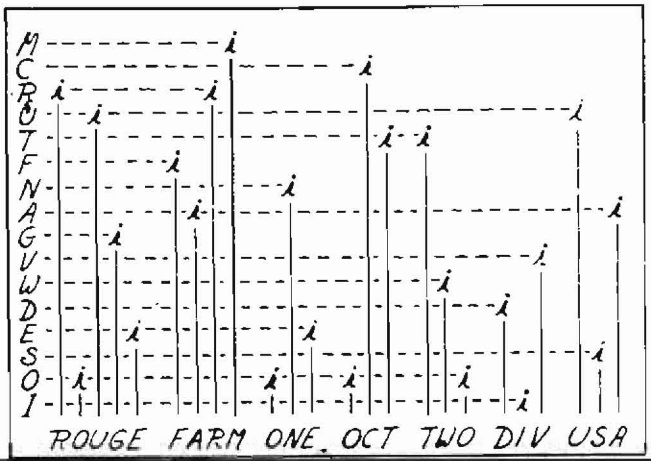
# AN IMPRACTICAL CIPHER

DAVID SHULMAN
New York, New York

One short story that will never win an O.Henry prize as the best short story of the year appeared in **Word Ways** as "Ivan's Letter" in the February and May 1982 issues. lt first appeared in **The Enigma** of June 1930, at which time a paltry prize of ten dollars was offered to anyone who could solve the cipher in the story. The prize was never claimed, and in my opinion it was not worth one's time or trouble to solve such a cipher. ln fact, the story should have never been reprinted. But, since **Word Ways** has resurrected it, some words of explanation are in order.

Erik Bodin, the author of the story (known as 'Viking' to the membership of The National Puzzlers' League), was one of its most skillful anagrammatists. Such skill as his is reflected in concocting the cipher missive upon which his story is based. (I use 'missive' to replace 'letter' in this article to avoid confusion with the alphabetic letters used in the cipher.) But, he betrayed an abysmal lack of knowledge of cryptanalysis with his explanation of how Sergeant Drummond solved it. No wonder nobody solved it at the time!

Before explaining the cryptanalysis used by Drummond, it is necessary to clarify the missive in the story as presented by **Word Ways**. In the original version in **The Enigma**, the missive was not typewritten but handwritten. As I understand it, the editor of **Word Ways** elected to use the typewriter in order to clarify the vertical alignment between each indicator letter 'i' in the missive and the corresponding letter in the secret message (written below the missive in the May **Word Ways**). However, for me, at least, the alignment was hard to check, and the editor should have used vertical lines to connect each 'i' to its message letter:



In effect, Erik Bodin constructed a concealment cipher, one in which the message is masked by a large number of extraneous letters. As hinted at above, he skilfully concocted the missive so that the indicator letter 'i' was placed at specified points on each line as many times as necessary to spell out the hidden message (found by transporting the letter at the beginning of each line horizontally to the 'i' and then vertically beneath the 'i'). The rest of the text had to be completed so that the missive would read sensibly. Also, he had to avoid using the indicator letter except where it was required on each line. As an expert in anagram construction, Erik Bodin had that kind of skill. But, as a practical system of enciphering, it is entirely out of the question to ask any correspondent to employ such a system, not even a spy as in the story.

In his story, the author would have us believe that his character, Sergeant Drummond, was able to solve the cipher by logical reasoning. From the cryptanalytic point of view, I would be very skeptical and conclude that his method was fortuitous hindsight. A system of concealment cipher such as this one has no methodology except trial and error. If you make as many guesses as you can and one of them works, you are lucky. Here we have so many variables that one may exhaust a lot of effort without success. This would explain the lack of solutions when the story was published. Why it was obvious to the Sergeant that Oiselle was a keyword and that its five different letters, EILOS, might include the key letter 'i' and his ability to see that this letter occurred at least once in each line and that this letter never fell into the same column - all this is beyond my limited powers of perception. On the other hand, I can perceive that none of these factors need be the correct one.

Using the same basic system of concealment cipher, I could construct the same type of message wherein any other word besides Oiselle could be a keyword. Moreover, whatever key letter I use could be used without the need to use it at least once on every line. Finally, instead of indicating the first letter of each line, it could be the last letter or any particularly numbered letter as agreed upon by the correspondents. With such a large number of variables, one must concede that a would-be solver such as Sergeant Drummond would have to resort to trial and error, assuming that he knew to begin with that this particular cipher system was being used. As far as the cryptanalyst is concerned, the shortness of the material limits his methods. On the other hand, the system is not a practical one for correspondents, and so the cryptanalyst may choose to ignore it altogether, especially for a paltry ten dollar prize!