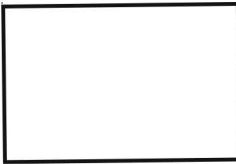


Non - Responsive

~~CONFIDENTIAL~~

A Boer War Cipher

BY IONA H. RADICE

~~Confidential~~

The first part of this note on a Boer War cipher appeared in the NSA Technical Journal, Vol. X, No. 3. Miss Radice now offers the solution to the problem.

The cipher is polyalphabetic using a minuend Vigenere square. The key my father used was his own name repeated as often as necessary, viz. RADICERADICERAD This gives as plain:

"After dinner Mr. Winston Churchill the correspondent of the Morning Post and two others tried to escape. But only Churchill got away"

A monograph frequency count shows that it cannot be a transposition or simple substitution: polyalphabetic is therefore the most likely considering the date (1899), and the fact that the cipher can be solved on such a short passage indicates that the alphabets must be closely related and the key probably cyclic. The repeated 3-letter word "ytz" confirms this, and implies that the key period divides 18. Cribbing "the" here gives "RAD" as key if the system is minuend—an astute reader will remember the encipherer's name and be home.

Alternatively from context it is quite likely that the cipher words "Gvkaywart" and "Ptjraxjps" have the same underlying plain. When they are differenced mod-26 "RCBJYZRCB" is obtained, confirming the hypothesis and giving the key width as 6.

Finally, everybody knows that Winston Churchill *did* escape from the Boers—some might even have remembered the date he did so!

I suggest that this was the first occasion on which the great man's name was enciphered—a fate which must have befallen it tens of thousands of times since.

~~CONFIDENTIAL~~