APPENDIX 2

7348

14 July 1954

GEE

Narrative Account of a Broken One-Time Pad System

by H. Campaigne

It is generally conceded that a one-time pad cipher system is immune to cryptanalysis. But a careful study shows that there are some tricky concepts involved, and that a cryptographer must be very careful indeed not to mislead himself. The Germans in the [redacted] during World War II did mislead themselves with a one-time system and we were able to exploit this weakness.

It may be of interest to quickly recount what happened, and estimate what it would have taken to make a more immediate and thorough exploitation.

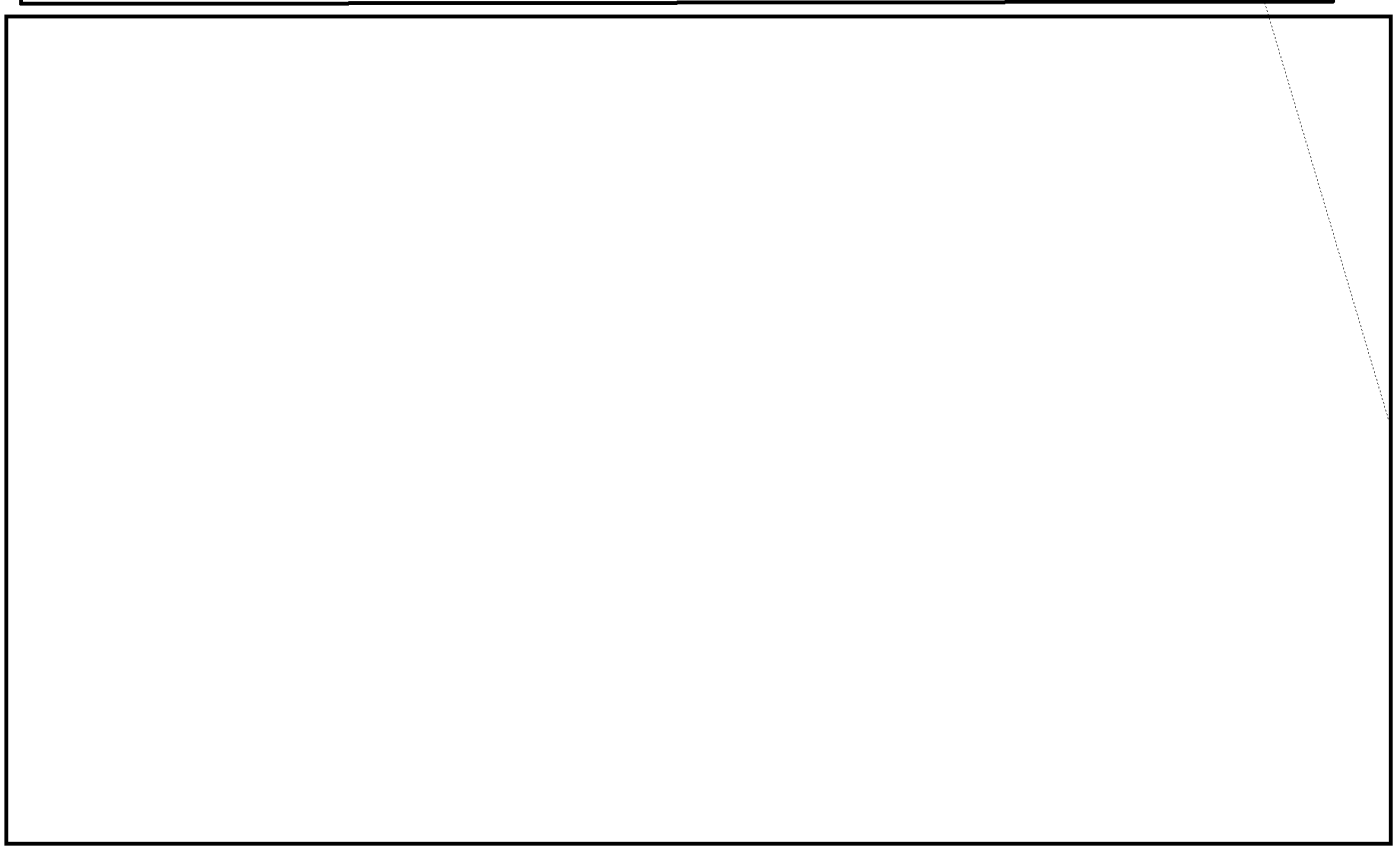
A study of German communications showed that for high level [redacted] messages a system which resembled one-time pad was being used. This system was designated GEE for short. It had apparently been in use since prior to 1934, and in 1943 was still being used heavily, perhaps a hundred thousand messages a year. Among the other German systems was another [redacted] system called GEC. These two were used among the same correspondents and employed the same code book.

In 1940 a passenger Dr. Emil Wolff, aboard a Japanese ship passing through the Panama Canal was found to have 3600 pages of additive. These were photographed and studied. The study established that the pages were intended for GEE, and that the additive was essentially random.

[redacted]

As more was learned about GEE hope revived that something could be accomplished. It was now known that an occassional exception to strict one-time use had been allowed. So a renewed attack was begun. An account of this has been excellently related by T. A. Waggoner in the ASA document "The Solution and Exploitation of the German One-Time Pad System, GEE" (TEC #TS290).

A restudy of the 3600 photostatted pages of additive taken from Dr. Emil Wolff showed that there were some non-random properties which had previously been overlooked.



The success described here did not occur until February, 1945, when the war was approaching its end. By May about 5000 pages had been read on the [redacted] circuit alone. The information in this traffic continued to be valuable even after hostilities ceased. In all 118,000 pages from this one link were read.

The question of interest now is, what equipment, procedure, establishment, or organization would have insured that this analysis succeeded, and would have expedited it?

It is clear that expeditious and reliable diagnosis is critical. [redacted]

In 1944 they were done much more easily. In 1954 they can be done more easily yet. But there is still room for improvement.

Evidently the diagnosis (which was correct) of one-time usage deterred any strong action at the time. The cryptanalyst must always be alert to exploit any mistake made by the communicator and must never be discouraged by the apparent unsolvability of a problem. This platitude must be considered basic.

Once the initial break had been made the exploitation was carried forward well enough, and today it could be done even more expeditiously, with more flexible and faster machinery. The critical stage is diagnosis. To get the traffic, get it sorted into homogeneous bundles, and make the counts in all the ways the analyst can think of, and get all this done fast is the preliminary goal to reading everything currently.