About the Cover

Low-level cryptography

The image on the cover was loosely suggested by Peter Donovan's article in this issue, which refers to the cryptanalysis of Japanese naval communications by Americans, British, and Australians during World War II. The cover displays the *wabun* telegraphic code for the Japanese syllabary known as *katakana*, in which a large number of communications were transmitted. Other protocols were also used. Standard Morse code was used to transmit numerals, either as groups of length four or five digits taken from a code book, or as the transmission of characters through Chinese telegraphic code. In addition, sometimes the Roman alphabet was used to transcribe *katakana*. Altogether, an impressively complicated collection of conventions.

Difficulties in cryptanalysis of Japanese communications began with the difficulties of the language itself, and the Japanese military deceived themselves into thinking this would make their communications especially secure. Layers of complexity were piled on top of this. Next up was the difficulty in the low-level interpretation of the messages intercepted, since many messages, especially in the early days of interception, were transmitted in *wabun* and others used Roman transcription. It was just after the First World War that the Americans started training operators to interpret Japanese telegraphic transmissions, but at first on a rather haphazard basis. A readable account of the history of this work can be found in *The Silent War* at

`http://corregidor.org/crypto/chs.whitlock/whitlock.htm`

The author, Duane Whitlock, was one of the U. S. Navy code group evacuated from the Phillippines during the invasion of 1942.

Later on, as Donovan says, the most secure systems sent messages as groups of five decimal digits. According to Alan Stripp in *Code Breakers in the Far East*, this was transmitted in standard Morse code according to the translation

0	1	2	3	4	5	6	7	8	9
O	N	Z	S	M	A	T	R	W	V

The systems used by the Japanese to encrypt high-level messages were extremely sophisticated, and if used correctly should have been impossible to break. Much of the Allies' success was through traffic analysis, which did not depend on reading messages, but just on keeping track of where messages originated and to whom they were sent.

The most secure system, JN-25, was encoded in a process of two steps. In the first, a code book was used to translate pieces of the message into groups of five digits. This sequence was written down in a (virtual) line. Then a sequence of additives were written underneath these, and on a third line were written the "false sums" of the first two lines in which decimal carry was ignored. A typical (if totally imaginary) sequence might be as follows:

message	submarine	departure	Honolulu
code groups	98721	13671	76542
additives	35678	17896	46781
transmitted	23399	20467	12223

In early versions of JN-25, each of the code book groups of five digits had the property that the sum of their digits was divisible by three. The purpose of this was presumably to make errors in transmission evident—again in American terminology, as a kind of "garble check".

This requirement limited the number of code groups to 33,334, and for mathematical reasons it made cryptanalysis much easier than it should have been. (Later versions did not have this feature, and this did succeed in foiling Allied techniques.) The additives were taken from an additive book, published and distributed separately from the code book. Each page of this book contained a grid of 5-digit groups, produced by some process supposed to be random. After writing down the message in code groups, the operator would open a page of the additive book, choose a position in the grid, and start writing down successive entries from the additive book underneath. He then recorded his starting place in the additive book in a preliminary part of the final message called the "indicator", using a separate enciphering scheme.

The Allies' tasks were formidable: to build up the code and the additive books over long stretches of time, and then to read the indicators of individual messages. At first sight the first two problems seem almost impossible to solve, but as with Allies' reading of German transmissions, these tasks were made easier by the fact that early implementations were simpler than later ones, and by frequent bad decisions by both operators and code-makers. In particular, changes in the code book were not simultaneous with changes in additives, so that "divide and conquer" was operable.

A valuable analysis of some of the cryptanalysis of Japanese communications can be found in Chapter VI of *Machine Cryptography and Modern Cryptanalysis* by Cipher Deavours and Louis Kruh. It specializes in the machines used for diplomatic messages, but includes also useful observations about the nature of the Japanese language and the problems it posed for telegraphic communication.

The technical literature on JN-25 is sparse. The most detailed coverage is in some *Cryptologia* articles by Peter Donovan, particularly the one he includes in his reference list. There are also some forthcoming articles by Chris Christensen on the history of machinery developed by Americans for the cryptanalysis of Japanese codes.

One could wish for more, especially since famous mathematicians such as Andrew Gleason and Marshall Hall took part in the war effort. It is not clear, unfortunately, if any relevant documentation remains extant.

—Bill Casselman
Graphics Editor
(`notices-covers@ams.org`)