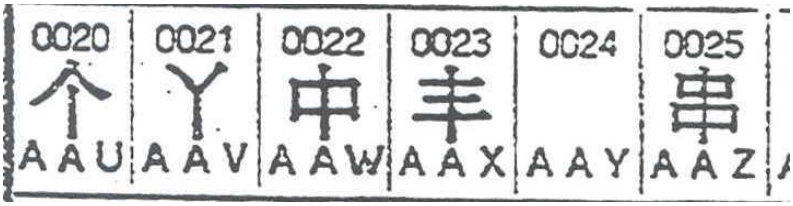
The Chinese Telegraph Code February 15

In the late 1800s telegraphic encryption was difficult for China for one obvious reason — its written language was not compatible with standard telegraphic systems. Telegraphy was strictly a Western invention, employing a Western alphabet. The Chinese written language was not alphabetically-based. Fortunately for the Chinese however, telegraphy did employ numerals.



The first Chinese telegraphic code dates to 1871. Attached is part of a page of the Viguier Code (named after the French customs officer in China who invented it in the early 1870s). According to this code, every Chinese character or word was given a four digit equivalent. The Chinese word or character meaning central or middle, 中, for example, is 0023. 0023 would then be sent by telegraph instead of by character or word.

Yet this system had problems. Numbers were both more expensive and difficult to transmit than letters, putting nations that did not use an alphabet at a disadvantage. These nations therefore scrambled for ways to remove this disadvantage, leading to numerous Romanization efforts and other creative schemes. Another problem was encryption. Simple possession of another's codebook was apparently all it took to read a message. These codebooks, moreover, were easy to obtain since many were created for the commercial world. Cryptologic security for the Chinese simply became a matter of "codebook management."

Interestingly, Viguier appears to be the first to address the problem of telegraphic encryption in Chinese. As explained in his 1873 work, The New Telegraph Codebook, his solution was to simply add what he called a "key number" to encrypt the Chinese four digits numbers that corresponded to characters. This way, a message could only be decrypted if both sides possessed the key

number. As a case in point, you would add “5555” to the Chinese character for rice, 米 (4149 in Viguier’s book). What would be transmitted by telegraph would be 9694 (4149 + 5555, with each digit calculated modulo 10). The only way to decrypt the message would be to have the key number. Viguier did not state how these key numbers were determined but they very well may have been randomly chosen.

What is described above, i.e., applying additives to codebook numbers, was hardly unique, many countries did this for traditional codebooks. The Japanese in World War II, for example, did this to their JN-25 codebook.* Analysts working the VENONA project in the 1940s discovered as well that the Soviets would add an additional group of four digits, randomly generated, to any four digit codeword.** Stripping off this additive—to find the actual codebook numbers—was a far more difficult task.

It is now known that the Japanese, in particular, enjoyed great success decrypting Chinese messages during this time period. As a case in point, they were regularly reading Chinese diplomatic messages pertaining to Korea. Since the Chinese at this time were novices at telegraphic cryptology, it is unclear how much “extra protection” they actually gave to their codebooks.

* It was decryption of JN-25 messages that greatly facilitated the U.S. victory at Midway in June 1942.

** VENONA was a U.S. project launched to exploit ciphers used by the Soviet espionage services during World War II.