The Flaw in the JN-25 Series of Ciphers, II

Peter Donovan.

From 1939 to 1945 the Imperial Japanese Navy made heavy use of a series of additive cipher systems generically named JN-25 by the cryptanalytical unit of the United States Navy. Each of these consisted of a code-book assigning a five-digit 'group', always a multiple of three, to each word or phrase in a very long list and encrypting these by 'false' (non-carrying) addition of a five-digit group ('the additive') taken from a long table of essentially random such. The author's earlier paper explains how this use of multiples of three provided a route for relatively rapid recovery of the additive and thus the decryption of intercepts. Another quite different and rather surprising source of insecurity inherent in this use of multiples of three was noted only in 1943 and became the basis of a process code-named 'Mamba' needed in 1944. This note sets out a further consequence of the statistics underlying Mamba: the use of multiples of three in JN-25 codebooks betrays itself very quickly.

KEY WORDS: additive cipher systems, characteristics, JN-25, Mamba, multiples of three, Op-20-G, scannable.

This paper deals with codebooks assigning to each word or phrase in a (long) list a 5-digit 'group' which is a multiple of three or *scannable* in the jargon of WW2. Here the groups are allowed to have initial 0s: thus 12345 and 00078 are groups. Being a multiple of three (equivalently, being divisible by three) means that the corresponding number, 12345 or 78 in these examples, is a multiple by three or, equivalently, the sum of the five digits, 15 in both examples, is a multiple of three. The *characteristic* χ of such a group is defined to be the reduction modulo 10 of the sum of the five digits: thus $\chi(12345) = 5$.

One might well guess that of the 33334 scannable groups from 00000 to 99999 about 3333 have characteristic 0, about another 3333 have characteristic 1, etc. This is far from being the case. A simple electronic calculation checks that for $0 \le i \le 9$ the number $m(i)$ of scannable groups with characteristic i is as set out below:

$$m(0) = 3247 \quad m(1) = 5875 \quad m(2) = 1780 \quad m(3) = 1780 \quad m(4) = 5875$$
$$m(5) = 3247 \quad m(6) = 925 \quad m(7) = 4840 \quad m(8) = 4840 \quad m(9) = 925.$$

These *Mamba numbers*, were known to the American naval cryptanalysis unit Op-20-G in 1943 but the calculation must have been quite tedious. Working out that it was worth calculating at all was a major achievement in cryptanalysis.

There is a 'false' or 'non-carrying' addition process defined for 5-digit groups: one just adds the pairs of corresponding digits and reduces these modulo 10. Thus $12345 + 00078 = 12313$. This example shows that the sum of two scannable groups may well not be scannable. There is a corresponding false subtraction: for example $12345 - 00078 = 12377$. The useful identities $\chi(a+b) = \chi(a) + \chi(b)$ and $\chi(a-b) = \chi(a) - \chi(b)$ are valid for 5-digit groups a and b provided the addition and subtraction involved are 'false' in this sense.

When a depth of two with both GATs identical (a *hit*) is detected no information is obtained about whether the groups in the codebook are all scannable. Such occurrences have to be disregarded for present purposes.

There are $33,334 \times 33,333$ pairs a, b of scannable 5-digit groups with $a \neq b$. For each γ with $0 \leq \gamma \leq 9$ one may may use the values of the above Mamba function m to calculate the number of these pairs of scannable groups with $\chi(a) - \chi(b) = \gamma$. If $q(\gamma)$ denotes the proportion of the $33,334 \times 33,333$ pairs a, b with $\chi(a) - \chi(b) = \gamma$, one works out that: $q(0) = 13.5\%$, $q(1) = 9.1\%$, $q(2) = 7.5\%$, $q(3) = 12.5\%$, $q(4) = 10.9\%$, $q(5) = 7.0\%$, $q(6) = 10.9\%$, $q(7) = 12.5\%$, $q(8) = 7.5\%$, $q(9) = 9.1\%$.

Thus 59.9% of the $33,334 \times 33,333$ ordered pairs of different scannable groups have the characteristic of their difference 0, 3, 4, 6 or 7 and 40.1% of these pairs have the characteristic of their difference 1, 2, 5, 8 or 9.

Now suppose that some secretive agency is generating randomly 5-digit groups a, b and x and transmitting by radio the pairs of false sums $a+x$ and $b+x$. One would expect that calculation of $\chi(a+x) - \chi(b+x) = \chi(a) - \chi(b)$ would yield 0, 3, 4, 6 or 7 about 50% of the time. If instead that agency is generating randomly scannable 5-digit groups a and b and arbitrary groups x and then transmitting the pairs $a + x$ and $b + x$, one would now expect that such a calculation would yield 0, 3, 4, 6 or 7 about 60% of the time.

Let us return to the decryption of JN-25 ciphers. The codebook was supplemented by a long 'table of additives', that is a table of randomly generated 5-digit groups. The transmitting clerk would choose a starting place in this table, and encode and/or encrypt information about which starting point had been chosen. This would be transmitted as part of the message and would be called the indicator(s). The message would be written out using every fourth line on a form with both horizontal and vertical lines. The codebook would then be used to write the appropriate code groups directly below the corresponding words. Below these would be written consecutive groups taken from the table of additives. Each entry in the fourth line would consist of the false sum of the code group and the additive group directly above. The groups in this fourth line would be transmitted by radio and so were called GATs (groups as transmitted). The intended recipient was supposed to interpret the indicators and then reverse this process.

The codebooks would be changed after some months with the additive table usually being changed more often. In 1942 Op-20-G found it necessary to introduce a standard reference system for these additive ciphers. For example JN-25B8 was the JN-25 system with code book B and additive table 8 and was in use in the leadup to the Battle of Midway.

When a change was made to a new code book and a new table of additives there would be no total guarantee that the new code groups would all be scannable. There was always the risk that the Japanese communications security people might have worked out that this practice was insecure. But suppose that Op-20-G had broken the indicator system and could thus put intercepted messages 'in depth', that is written out horizontally on paper divided into rectangles so that GATs obtained from the same additive were in columns. This was generally the case in 1942 and much of 1943. After about 200 *depths of two*, that is pairs of GATs y, z calculated from the same additive, had been detected,

$\chi(y) - \chi(z)$ could be calculated for each pair. If the values 0, 3, 4, 6 or 7 had occurred as this difference for about 60% of cases one could infer that the new JN-25 codebook was using only scannable groups and so the special decrypting techniques could be used. If these values had occurred for about 50% of the pairs one would know that decryption was likely to be much harder. And if these values had occurred for about 40% of the pairs a radically new cipher system would have been detected.

More realistically, the first 100 depths of two might include 65 that yielded 0, 3, 4, 6 or 7. This would confirm that only scannable groups were in use. If the first 100 depths included only 55 it would be necessary to obtain and examine more data.

It is not particularly obvious how this method should be modified to handle, for example, 25 depths of eight in the new system rather than 200 depths of two. Yet such could arise if eight operators encrypted their first messages in the new system using the top left entry of the middle page in the table of additives as starting point.

The following *ABC* method is in all probability a minor piece of WW2 cryptanalysis that was overlooked at the time. The method for depth two is more likely to have been implemented: this author does not know. However he can certify that hunting for decryption methods is a very long process.

The mathematical theory underlying it is somewhat technical and does not need to be explained here. Instead simple computer calculations of the relevant means and standard deviations justify it retrospectively. The cryptanalyst working with WW2 technology would not have been able to run vast numbers of experimental calculations and instead would have had to work out the mathematical theory of this situation directly.

Suppose given a depth of eight 5-digit groups with characteristics χ_1, χ_2, χ_3, χ_4, χ_5, χ_6, χ_7, χ_8 respectively. One can evaluate successively:

$A = \cos 3\pi\chi_1/5 + \cos 3\pi\chi_2/5 + \ldots + \cos 3\pi\chi_7/5 + \cos 3\pi\chi_8/5;$

$B = \sin 3\pi\chi_1/5 + \sin 3\pi\chi_2/5 + \ldots + \sin 3\pi\chi_7/5 + \sin 3\pi\chi_8/5;$

$C = \sqrt{A^2 + B^2}.$

From the viewpoint of WW2 technology, this needs a table of square and square root functions and the numerical values of $\sin 0^\circ = 0$, $\cos 0^\circ = 1$, $\cos 36^\circ$, $\sin 36^\circ$, $\cos 72^\circ$, etc.

From a mathematical viewpoint it is more appropriate to work with the complex numbers $A + iB$ which are sums of tenth roots of unity in the complex plane. Such sums are obtained in the theory of *random walks* and are of significance in the theory of polymers.

As we are considering not a single depth of eight but a batch of 25 depths the average, $\bar{C}$, of the 25 values of this C should be taken.

From the modern perspective it is easiest to program a computer to work out the mean of $\bar{C}$ when 10,000 batches of 25 depths of eight 5-digit groups are randomly chosen and their characteristics calculated. This is effectively the same as choosing the 1-digit numbers χ_1, χ_2, ..., χ_8 randomly. One discovers that the mean (or expected) value of $\bar{C}$ is about 2.53. The standard deviation is about 0.26.

Next the calculations are repeated for 10,000 batches of 25 depths of eight scannable 5-digit groups g_1, g_2, ..., g_8 and one randomly selected group x, not necessarily scannable.

Here one sets $\chi_1 = \chi(g_1 + x) = \chi(g_1) + \chi(x)$, etc. Elementary formulae may be used to show that C does not depend upon x. As before, $\bar{C}$ denotes the average of C taken over the 25 depths in a batch. It turns out that $\bar{C}$ has a mean value of about 3.84 with a standard deviation of about 0.30.

The averaging of C over a sample of 25 batches should ensure that the distribution of $\bar{C}$ is near enough to normal.

We return now to the task of examining 25 depths of eight intercepted GATs. For each depth A, B and C are calculated as above and the mean $\bar{C}$ of the 25 values of C determined.

A fairly reliable rule is that $\bar{C} < 3.15$ when the book groups being used are randomly selected and $\bar{C} > 3.15$ when the book groups are all scannable but otherwise randomly chosen. A realistic strategy is to note that usually but not always either $\bar{C} > 3.4$ or $\bar{C} < 2.9$. In the former circumstance one may (almost) deduce that the book groups are all scannable and in the latter the book groups are randomly allocated.

If it turns out that $2.9 \leq \bar{C} \leq 3.4$ it would be wise to obtain further data before making any conclusion. If instead of considering 25 batches of depths of eight one works with 50 such batches, the standard deviations of .218 and .296 are divided by $\sqrt{50/25}$ and so the calculations usually give correct information about the use or otherwise of scannable groups only in the new code-book.

The method used for handling depths of eight can be modified easily enough to handle other depths from about six upwards. Thus a batch of 15 depths of ten is usually enough to determine whether a new codebook uses only multiples of three. A mixture of various different depths is more complicated.

Regardless of whether this method was known at the time, the point is quite clear: the use of only scannable groups in a codebook betrays itself very quickly indeed.

THE AUTHOR

Peter Donovan is a retired member of and now visiting fellow at the Mathematics Department of the University of New South Wales, Sydney, Australia. His work with John Mack on a book to be entitled *The Cipher War in the Pacific, 1918–1945* is now almost finished.

SUBMITTED FOR PUBLICATION IN 'CRYPTOLOGIA', 27 JUlY 2009.

Peter Donovan, Mathematics Department, University of NSW, Sydney 2052 Australia.
`p.donovan@unsw.edu.au` Fax: +612 93857111. Home phone: +612 94168310.

The Maple program used to check assertions made in this paper is attached. Note that the seed for the random number generator was taken to be 2468: you may wish to change this. Note that it is set up for $P = 40$ batches of $Q = 25$ depths of 8: these numbers may be changed painlessly if required.