MOST SECRET

Selection Tests Nov. 5 1942

When a menu is run on the bombe we can regard the bombe as looking for a "partial key" which satisfies certain conditions. The partial key consists of a wheel-order, a relative of "ZZZ" ringstellung, and the stecker of certain letters of the alphabet. The conditions which it is required to satisfy are,

(i) that the stecker shall be consistent among themselves, and

(ii) that the partial key shall decode certain pairings of the crib (those used on the menu) correctly.

However, what we are really looking for is a key which satisfies conditions (i) and (ii) above, and also the further condition of having exactly 10 pairs of stecker. It is this discrepancy between what the bombe is looking for and what we are looking for which makes certain of these "partial keys" inherently more likely to be correct than others.

Suppose we have given a "partial key" or bombe story satisfying conditions (i) and (ii) above. What is the chance of its being the right answer?

This chance depends on:-

a) the chance of the crib itself being right

b) the chance of the turnover assumption implicit in the menu being right

c) the number of possible wheel orders

d) the actual stecker contained in the partial key.

a), b), c) will vary with each particular job run, but d) can be worked out for the various standard types of menu.

Suppose now that we have a crib which is correct, ad a menu on it which is also correct. Suppose that 60 wheel orders have to be run, and that they are all equally likely to be right. Suppose that we have a bombe story which contains p self-stecker and r pairs of stecker. Let M = M(p,r) be the number of 10-stecker keys which contain the given p self-stecker and r stecker.

Then,

Let N be the total number of 10-stecker keys, then,

For the given bombe story,

The a priori chance of the self-stecker and stecker being right =

The a priori chance of the wheel order and ringstellung being right =

The a priori chance of the stop being right =

The a priori chance of the stop being wrong =

But the story at least goes round the menu, so, if the menu has L links on it,

The chance of a wrong story going round the menu =

The chance of the right story going round the menu = 1

(The chance of getting the result from the right story =

And the chance of getting the result from a wrong story =

= approx.

Thus the chance of the story being right is proportional to:
Or the odds on the story being right are proportional to
So if we write chance= , odds = we have,

Now suppose we have a number of stories on the given menu, and that
= the number of stories with chance The menu is correct, and

so the correct story is among the number (supposing the bombe has not missed it!). The exact chance of any particular story being right is then,

This chance cannot be evaluated until we know the details of all the stories on the menu, but it can be approximated to if we substitute for
the expected number of stories having chance C(p,r) - - not the actual number obtained. This is precisely how the selection is done.
Actually 0(p,r) is measured; and clearly if we test only those stories with 0(p,r) greater than a we are in effect testing those whose chance of being right is greater than b, the relation between a and b being determined by the value of K for that particular job.
Details
Definition A "deciban" =1/10 log10: and so the number x would be measured by 10 log10 x decibans. The adding of decibans is the multiplying of factors.
Flowers' analyser. This measures the number in units of

"2-decibans". The points (p,r) of the "selection board" are wired to the numbers corresponding to and to these numbers is added the 2-deciban measure of

25L (by means of a plug). [log 1025= 1.4 = 14d.b. =7 units of the scale]. The result is shown on the display panel.
Hence if the number +14 is shown on the panel, this corresponds to +28 decibans and so

For any given job one has to work out what risk one is taking by only testing stops above a certain scale reading.
The above selection of stories is the best possible, but of course there are other methods not quite so sensitive. One of these is by the measurement of "z" - the number of off-chain

steckers, assuming that for the correct story it will be less than a certain value. This method is very much simpler to carry out on a machine.
Graphs have been drawn to show the relation between the percentage of stories to be tested, and the risks involved in rejecting the others, for these two methods of selection. It should be noticed that p, r and z take only integral values and so both C(p,r) and z take a number of discrete values, and so selection has to be done by "chopping off" at one of these discrete values. Whether this can be done effectively depends on how near the discrete values are to each other and on the sensitivity of the selection.
From the graphs we can see that the "z-method" is not sensibly worse from the risk point of view (the curves keep fairly close together), but that it provides a much fewer number of discrete values in the range required. Thus, for example, on a 12-chain we must, by the z-method, either take a risk of only 7% or take a risk of as much as 20%. There is no intermediate value. The first method does provide intermediate discrete values.
Of particular interest are the menus which have 12 enigmas or less (which would run three times on a 36-enigma machine). These menus are:

103
:
10 stops,
1 stecker
112
:
93 stops,
5 stecker
121
:
730 stops,
18 stecker
130
:
4,900 stops,
52 stecker

The 103 would run on Mammoth without any selection at all, and would give 1 stecker per wheel order. The 112 would give 5 stecker, but this could be reduced to 11/4 by taking a risk of 7% (postulating z = or less than 7). The 121 menu gives 18 stecker which, by the z-method could be reduced to 4, with a risk of 7% (z= or less than 7), or to 11/2 with a risk of 20% (z = or less than 6. In all these cases the crucial values are z=6, and z=7 so we should require particular sensitivity in this range.
It is clear, therefore, that the most important case - the 112 - can be run 3 at a time with only 7% risk if we have the z-method of selection. Query: is it worth fitting selection for this case alone? The 121 case is not so important since 4 stecker is rather a lot and 20% risk (to get only 11/2 stecker) is a substantial risk. The most frequent use of the 121 would probably be on short stretches of crib. The 130 would not be run at all.

O.K.L.
5/11/42