APPLICATION OF RINGSTELLUNG RANGE TO BOMBE

Consider a menu made up on a length L of a crib; for simplicity assume that the menu covers the first 1 t.o. position of the possible 26, and suppose that the zz (bombe reading) of the first position on the crib in the correct (breakage) position is b; then if x is actual distance of t.o. from beginning of the crib, t is the position of the t.o. (5, 10, 17, 22, 26) and r the English Ringstellung of the 3rd (fast wheel)

$$(t\text{-}x)\text{-}b = r.$$

$$\therefore \quad x = t\text{-}b\text{-}r$$

$$\text{But } 1 \le x \le 26$$

$$\therefore \quad b \le t\text{-}l\text{-}r \qquad b \ge t\text{-}26\text{-}r$$

and so we have a range (26-l) of possible positions of the fast enigma end wheel bombe reading.

In the case of a R.Range $r_1 \le r \le r_2$ the appropriate formulae may easily be seen to be

$$B \le t - \ell - r_1 \qquad b \ge t - 26 - r_2$$

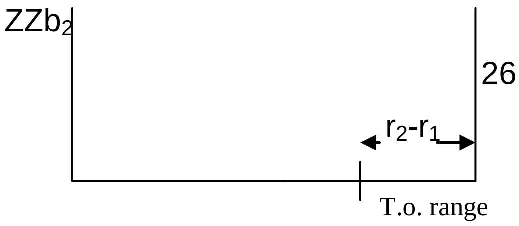
and the corresponding range is $(26 - \ell) + d$ where $d = r_2 - r_1$. Using the above, a fraction $\frac{(l-d)}{26}$ of the actual bombe stops may be discarded. If the present slow and fast wheels were interchanged (as will be the case on Bombes 6 and & [I think]) a fraction $\frac{(l-d)}{26}$ of actual <u>bombe time</u> could actually be saved.

The natural development of this formula, x = t – b – r is the use of the whole length of a crib. In outline, the knowledge of R.S. Range enables us to indicate the possible t.o. positions for any bombe reading of 3rd wheel of 1st enigma and as the wheel revolves (clockwise) the 't.o. range' moves along the crib from right to left. So a menu is made up on the whole 26 t.o. positions. The slow and fast wheels are interchanged, and the bombes automatically made to stop after $(26)^2$ revolutions. This allows the appropriate middle wheel turnovers to be made, as will be explained later, and any enigmas which happen to be under the 'Shadow of the t.o.' are automatically cut out by the simple expedient of turning the 'buttons' on the corresponding wheels.

To return to the formulae: with the same notation as before, put
$b_2 = t - 26 - r_1$

From $b = t - x - r$ we see that for <u>fixed b</u>, x is a decreasing function of r, and that for <u>fixed r,</u> b increases as x decreases. Then as r increases from r_1 to r_2, b will decrease from b_2 to $b_2 - (r_2 - r_1)$.

If then we set the enigmas in positions 123……..26 at zzb_2; $zzb_2 + \ell$,…..$zzb_2 - \ell$; for R.S. Range: $r_1 \le r \le r_2$, the T.O. range is from position 26 to $26-(r_2-r_1)$
As the end wheel revolves the t.o. range moves from right to left along the crib.

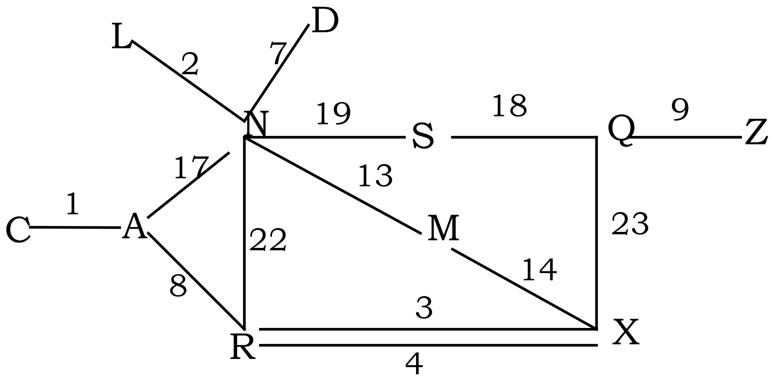


From all this we see the following procedure.

1. Make up menu on the whole of the 26 t.o. positions of the crib.
2. Put this on the bombe, remembering to number the enigmas I --- XXVI, corresponding to the positions of the equivalent constatations on the crib.
3. Set enigmas I --- XXVI at zzb_2 ----zzb_2- ℓ. (Remember that the fast and slow wheels will be interchanged.)
4. Suppose that the R.S. Range on the end wheel is 4, then cut out enigmas XXVI to XXIII (by turning buttons on one wheel of each enigma).
5. When the first two wheels have completed one cycle the bombe is automatically stopped.
6. Enigma XXVI is 're-engaged' and its middle wheel turned over one. Enigma XXII is now cut out.
7. After one more cycle of the first two wheels, enigma XXV (of course in <u>fact</u> enigma p $1 \le p \le 26$ <u>may not</u> exist) is re-engaged; its middle wheel turned over one; and enigma XXI is cut out.

The procedure should now be clear. It is evident that any correct crib can be broken on one menu. Whether or not any time will be saved by this method as against the ordinary method, will depend on a number of factors which will be considered in turn.

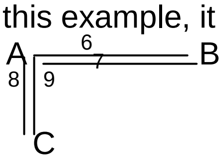
(a) Example of a menu on 17th Orange, using the whole length (23) of the crib, and assuming a R.S. Range of 4 on the last wheel.



With no cut out this is a 15 and 4 closures.

To examine whether it will be possible to run such a menu on the bombe (minus machine-gun presumably), we must cut out in turn any links lying in range 1 – 4, 2 – 5, 3 – 6, 4 – 7,-------23 – 26, 24 – 1, 25 – 2, 25 – 3; and <u>average</u> the number of stops obtained; remembering that a particular 'weak' chain will only occur $(26)^2$ instead of $(26)^3$ times. In the above case the number of stops per W.O. should be about .11.

From this example, it is obvious that the kind of thing we want to avoid if possible is



As these two closures, and (probably) two of the three letters would be cut out at one fell swoop when the T.O. Range is from 6 – 9. In fact the menu technique is diametrically opposite to the present methods: the ideal menu on the whole range of 26 would be built up of independent 'power houses' which could not be cut out simultaneously.

(b) The question of time saved by application of this method.

If the first and third wheels are reversed, the third wheel (which will now become the slow wheel) can be set at the lower limit of range given by I, and when it has covered the permissible range (in the case of a disconnected menu the 'b range' will obviously consist of two or more disconnected ranges) the bombe may be stopped.

In this way there would be a saving $\frac{(b-d)}{26}na$: where 'n' is the number of runs, and 'a' the time for each run.

Suppose that we put down a (good) crib on all sixty wheel-orders (this would appear to be the safest policy on Red. for example) the time taken to run two menus would be:

$$\frac{(26-l+d}{26}\; n_1 a \qquad \frac{26-(26-l)}{26} + dn_2 a$$

where n_1 and n_2 are the number of runs for menus of length ℓ and 26- ℓ respectively (in practise n_1 and n_2 are both 20 if possible. On occasion n_1 may be 30).

Anyway, put n_1 and n_2 = 20: and the total time definitely to fail a crib is

$\frac{(26\;\; 2d)}{26}\; 30a$:a saving $20a - 20a\frac{d}{13} = 20a\frac{13-d}{13}$

On a good Ringstellung day (d=4, say), we would save $20a\frac{9}{13}$ hours.

Compare this with the time taken completely to fail a crib on one menu using the new method with the modified bombe. This will be in almost all cases 30a, since it is rarely possible to build up a strong enough menu on less than fifteen enigmas (on a double-decker red crib it might well be possible).

So we see that $20a + \frac{d}{13}20a \text{ p } 30a$

provided that $\frac{20d}{13} \text{ p } 10$

i.e. $d \text{ p } \frac{13}{2} = 6\tfrac{1}{2}$

Actually a R.S. Range >7 is a pretty poor business, so in most cases it is quicker to run the job on two menus.