The Turing Bombe

What it was and how it worked

5. Checking the Stops

Some checks were performed by a device called a machine gun which searched the diagonal board for two letters steckered to the same third letter. For example, if, say, G is steckered to Y, and R is steckered to Y then due to the reciprocal nature of the Enigma's plugging, Y must be steckered to both R and G, but this is impossible so any stop exhibiting this property can be rejected. The machine gun got its name from its array of uniselectors which sounded like a burst of machine gun fire as they successively searched the cables of the diagonal board for duplicate steckers. The bombe had to be halted to use the machine gun and as it would not eliminate all false stops it was not always used.

Note that in Figure 4.1, the presence of two dead wires in the *F* cable does not imply that F is doubly steckered. This is because F is not in the menu and therefore the *F* cable has no scramblers attached to it so the only way its wires can be energised is through the diagonal board. Since the *f* wire in the *F* cable is not connected to any other cable via the diagonal board it is not connected to any other cable at all and therefore can never be energised.

The check was usually performed by a Wren on a checking machine, which was similar to an Enigma with the stepping mechanism disabled. The rotor order and positions were set up in accordance with the order and positions discovered by the bombe. The stecker pairings discovered by the bombe were also plugged up on the checking machine, these would not generally be all the necessary stecker pairings however so any additional steckers had to be determined. There also remained the tedious task of manually determining the Ringstellung.

When the checking machine was set up in accordance with the stop the ciphertext was keyed in, and if it yielded German text, or a close approximation to it, that indicated the stop was correct and the cry *'Job's up, strip machine!'* was called out and the bombe which found the stop, and all the other bombes working to break the same key were halted and then unplugged in preparation for the next job.

If this procedure failed to yield German text the stop was not correct and the next stop was examined.

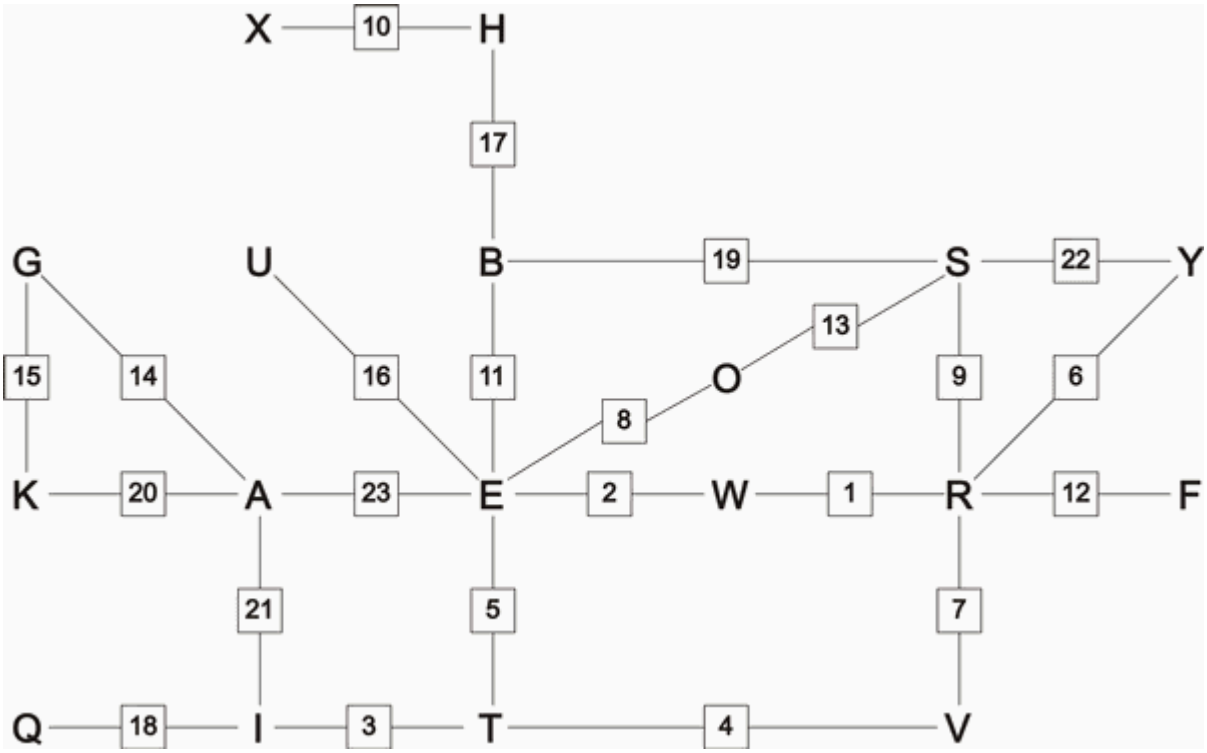

Figure 1.6 Crib-Ciphertext Pairings

Returning now to Figure 1.6 we see that it encompasses a span from scrambler position 1 to position 23 of 23 letters. There is therefore a 23/26 or 88% chance of the Enigma's middle rotor turning over during encipherment. If this occurred some of the bombe's scramblers would be in the wrong position relative to the other scramblers and the bombe will therefore not produce valid stops. So to eliminate the possibility of a middle rotor turnover ruining the bombe run we can form two separate menus, one using the span 1-13, the other using the span 14-23. We know that at most one of these two menus can have suffered a middle rotor turnover during its encipherment, so at least one of them will yield valid stops.

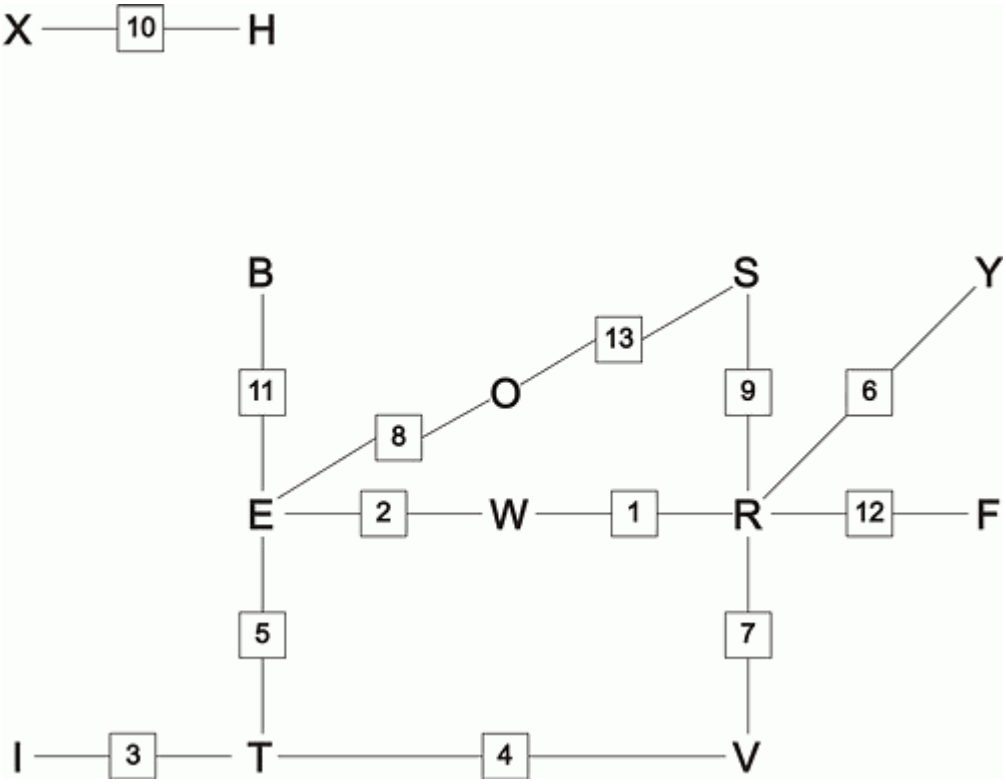

Figure 5.1 WETTERVORHERSAGEBISKAYA Split Menu 1

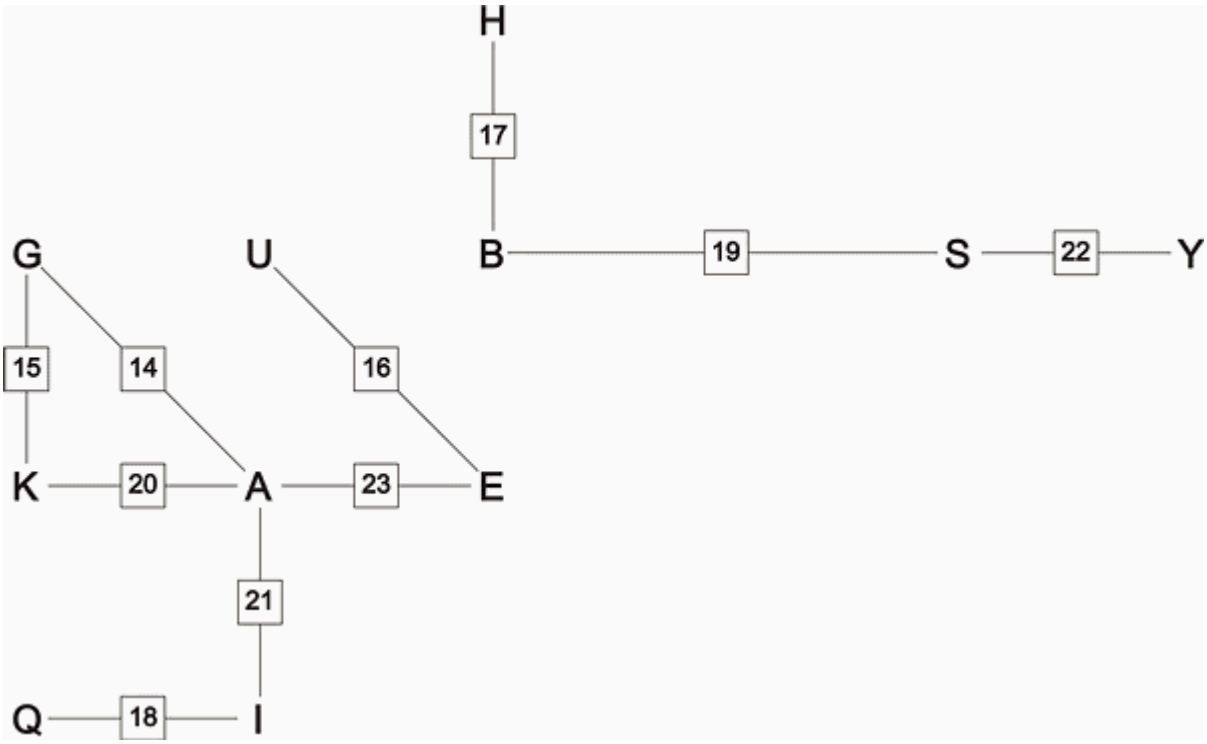

Figure 5.2 WETTERVORHERSAGEBISKAYA Split Menu 2

These new menus are represented in Figures 5.1 and 5.2. Figure 5.1 shows a stronger menu than Figure 5.2, containing as it does two loops in the main web of 11 letters and one additional web of 2 letters. Figure 5.2 shows a menu containing one loop in the main web of seven letters and one additional web of four letters. Neither of these menus is strong enough to produce a small number of stops which demonstrates the considerable difficulty of finding good menus even with an excellent crib like WETTERVORHERSAGEBISKAYA.

There are many aspects of the cryptanalytical operation that we have not considered in this brief essay:

We have not considered the great difficulty in predicting the frequencies on which messages would be transmitted, nor have we considered the difficulty in accurately intercepting and recording messages which may have been transmitted at a great distance from the interception stations often yielding a weak signal in poor atmospheric conditions.

We have not considered the difficulty in composing cribs, or the frustration of having composed a crib and having matched it to the ciphertext only to discover it is of little use because it yields a feeble menu.

We have not discussed the valuable bombe time wasted running menus derived from false cribs, or a correct crib in the wrong position.

We have not considered the potential unreliability of the electromechanical components in the bombes, nor of the fact that the bombes were seldom available in numbers adequate to cope with the number of keys which burgeoned as the war progressed.

We have not considered the urgent necessity of breaking the messages while the intelligence they contained was of operational value.

We have not considered the difficulty of disseminating the intelligence to the field commanders without it being intercepted by the enemy, nor the difficulty of employing the intelligence operationally without arousing the enemy's suspicions that the Enigma was being broken.

We have not considered improvements to the Enigma that were being introduced as the war entered its final phase. The introduction of a pluggable *Umkehrwalze*, known as *Umkehrwalze D,* threatened the entire Enigma-breaking operation, but was never put into large scale use. The *Uhr*, a mechanical attachment to the Enigma, provided the Enigma with another layer of complexity. Doubly-enciphering a message rendered all cribs useless.

The Germans failed to avail themselves of a very simple technique which would have made the Enigma much more secure. They could have placed the occasional random letter in the plaintext before encipherment. This simple expedient would have made it very difficult to match cribs to the ciphertext and so would have greatly increased the difficulty of obtaining good menus. During the height of the Normandy campaign, Bletchley Park was deciphering a staggering 18,000 messages each day.

When Germany surrendered, Churchill ordered the destruction of every one of the 200 bombes which had broken the Enigma on this industrial scale. Not a single fragment remains.

In intellectual challenge and commitment of resources, the production of ULTRA is equalled only by the MANHATTAN project and putting a man on the Moon. Its effect on history ranks with either.

Return to The Enigma and the Bombe main page

Home