**Aan de slag 26**

**Enigma simulator**

Hieronder zie je een voorbeeld van hoe de Deutsche Luftwaffe boodschappen verstuurde die met de Enigma gecodeerd waren. De operators van de Enigma gebruikten nooit de dagsleutel om een boodschap te versleutelen, maar ze gebruikten deze dagsleutel alleen om een boodschapsleutel van drie letters, het *trigram,* te maken; deze sleutel werd door de operator gekozen. Dit trigram werd gebruikt om de rest van de boodschap te versleutelen. Deze procedure moest ervoor zorgen dat overmatig gebruik van de geheime dagsleutel vermeden werd, zodat iedere boodschap van dezelfde dag met een andere bij toeval gekozen sleutel versleuteld werd.

Tijdens de oorlog werden verschillende varianten op dit systeem toegepast om de codeboeken te gebruiken. In het algemeen bevatten de codeboeken alle instellingen van de Enigma voor een hele maand. Het sleutelblad van de operator bevatte de volgende informatie:

Op dag 31 wordt de volgende boodschap verzonden:

Om deze boodschap te ontcijferen, moet je de volgende stappen nemen:

1. Kies de juiste Walzen (rotors) en pas de Ringstellung aan.
2. Plaats de Walzen in de machine.
3. Stel de pluggen of 'Stecker' in op dag 31.
4. Zet de startpositie op EHZ; dat is het eerste trigram van de boodschap.
5. Decodeer in deze positie het tweede trigram TBS om de boodschapsleutel te verkrijgen. Dat moet een XWB opleveren.
6. Stel de gedecodeerde boodschapsleutel (XWB) als startpositie in op de Enigma.
7. Decodeer het bericht.