

Enigma-handleiding en de Alphabet Slide Rule

Chris Hakkaart

Enigma

De meesten van ons zullen wel eens een Enigma in een museum gezien hebben. Er staat er een in het Nationaal Militair Museum te Soesterberg, om veel andere redenen ook een interessant museum. Trek wel de nodige uren uit voor een bezoek want mijn bezoek van maar liefst vier uur was veel te kort. Er is zeer veel te zien en te leren, en diegenen die nog in militaire dienst gezeten hebben zullen wel het een en ander aan voertuigen herkennen.



In een van de vitrines staat een Enigma-M, een codeermachine, officieel genaamd *Schlüsselmaschine*, die de Duitse krijgsmacht voor en tijdens de Tweede Wereldoorlog gebruikte. De Enigma is een elektromechanische codeermachine van het type rotormachine. De Duitse krijgsmacht had verschillende varianten van de Enigma in gebruik, waaronder de Enigma-M, die vooral bekend staat als de Marine Enigma, maar ook werd gebruikt door het leger en de luchtmacht.

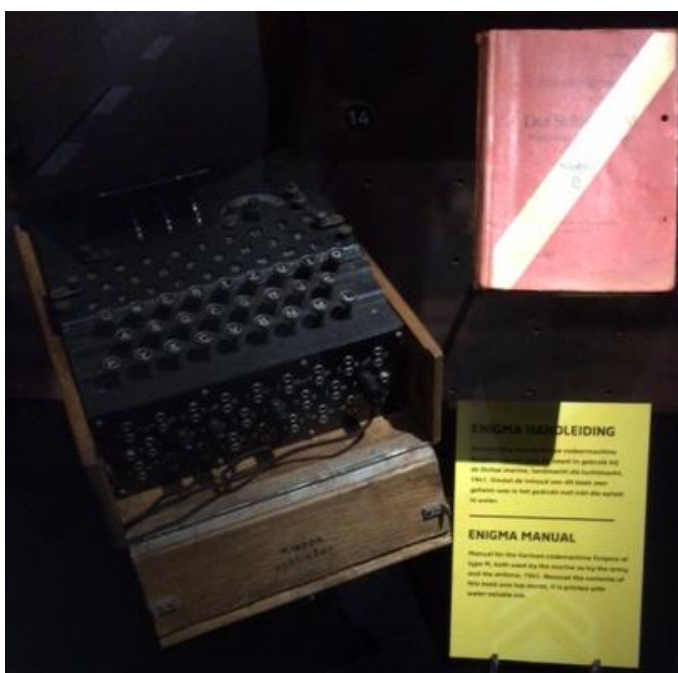


Fig. 1. De Enigma-M in het Nationaal Militair Museum te Soesterberg

Bletchley Park

In Bletchley Park, in Engeland, is tijdens de oorlog zeer ingenieus werk verricht om de Enigma te kraken, wat tenslotte ook lukte. Daarover is in 2014 de film *The Imitation Game* gemaakt, waarin Alan Turing en zijn team op een intrigerende wijze worden belicht. Een bijzondere film, waarin visie, techniek, binnenlandse en buitenlandse politiek verweven zijn.

Handleiding

De handleidingen voor het gebruik van de Enigma werden natuurlijk niet op grote schaal verspreid. Sterker nog, er waren stringente maatregelen genomen om te voorkomen dat ze in handen van de vijand zouden vallen. Het verbranden was een beproefde methode.

Voorts dienden de handleidingen zo opgeborgen te worden, dat ze nat konden worden: de tekst kon in water oplossen, omdat deze met oplosbare inkt was geschreven. De meeste kans dat de levensduur beperkt zou zijn? Zie onderstaande tekst in fig. 3.



Fig. 2. Beschrijving van de Enigma-M-machine.

Een uiterst zeldzaam exemplaar van de handleiding, dat de oorlog overleefd heeft, is in het bezit van het Nationaal Militair Museum. Van deze handleiding zijn waarschijnlijk maar heel weinig exemplaren bewaard gebleven. Er zijn maar twee andere exemplaren bekend, een bij het Bundesarchiv in Berlijn en een in het Imperial War Museum in Londen.

Het exemplaar van het Nationaal Militair Museum is goed bewaard gebleven. Achterin staat met Duitse Pünktlichkeit genoteerd dat de laatste mutatie in het boek is aangebracht op 20 juni 1944. Uit een

stempel in het boek blijkt dat het exemplaar afkomstig is van de Marinebefehlshaber in den Niederlanden, een functie die tussen 1940 en 1945 is vervuld door vijf verschillende personen.

Later kwam het boek in het bezit van Nicolaas Govert de Bruijn (1918-2012), een Nederlandse wiskundige en hoogleraar in de wiskunde aan de Technische Universiteit Eindhoven. Hij staat vooral bekend om zijn vele bijdragen op het gebied van de (wiskundige) analyse, getaltheorie, combinatoriek, combinatieler en logica. Dat verklaart De Bruijn's belangstelling voor de Enigma. Zijn kleinzoon, Rommert De Bruijn, heeft de handleiding van de Enigma-M, uit het bezit van zijn opa, aan het Nationaal Militair Museum geschonken.

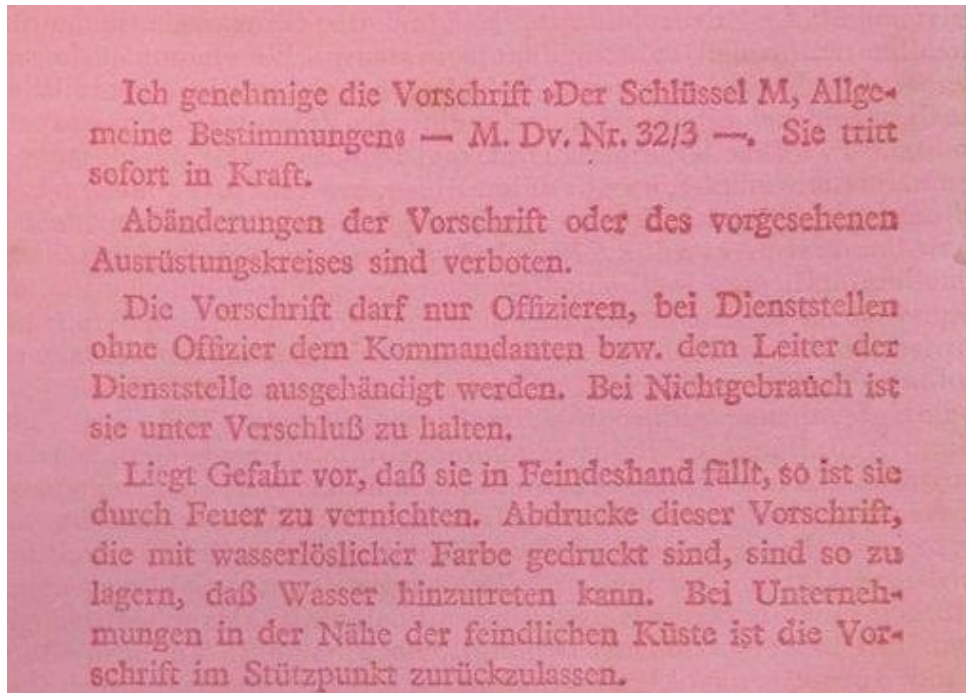


Fig. 3. Voorschrift uit de handleiding.

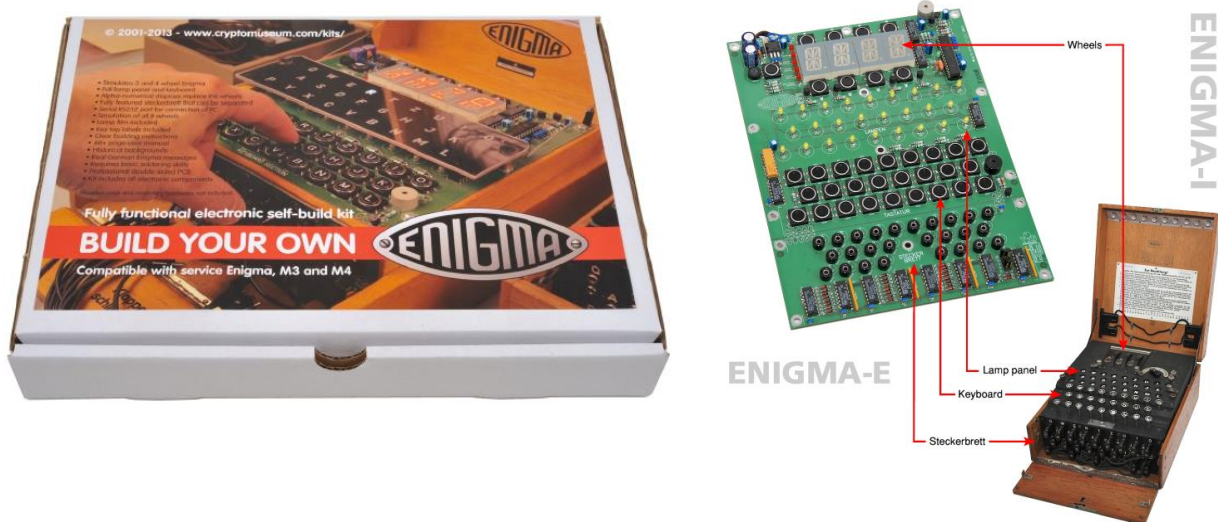


Fig. 4. Enigmabouwdoo's

Bouwdozen

De Enigma boeit nog steeds vele mensen. Net zoals er voor de rekenliniaal digitale versies zijn ontwikkeld, heeft er een soortgelijke ontwikkeling bij de Enigma plaatsgevonden. Er zijn nu bouwdozen te koop (zie e-mailadres hieronder) met een printplaat, waarmee je je eigen elektronische Enigma kunt bouwen.

De volgende stap is een Enigma software programma als simulator van de elektromechanische versie van de Enigma dat je op je eigen PC kunt draaien. Wellicht om je eigen files mee te versleutelen?

Alphabet slide rule

Wanneer je door de informatie over versleuteling en de Enigma op het internet bladert, kom je tegen dat er na de oorlog, door diverse landen, encryptie-apparaten ontwikkeld zijn. En geloof het of niet, daar zit ook een *alphabet slide rule* tussen, een woord dat ik nog niet kende. Deze blijkt door de Nederlandse Defensie begin jaren zeventig ontwikkeld te zijn, gebaseerd op een methode, die al door de Romeinse keizer Julius Caesar gebruikt werd. Vandaar de naam, de Caesar Cipher. Die methode komt in feite neer op het verschuiven van de posities van de letters.



Fig. 5. De Caesar Cipher box

De Caesar Box in figuur 5 is voor trainingsdoeleinden van het Nederlandse leger gemaakt. Heeft iemand er wel eens een in het echt gezien? De strips met letters schuif je in een transparant frame naar bepaalde posities, waardoor je je tekst *onbegrijpelijk* kunt maken.

Bronnen:

1. <https://www.nmm.nl/over-het-nmm/kenniscentrum/thema-y/handleiding-enigma-codeermachine/>
2. <http://www.intelligenia.org/m1290.htm>
3. <https://www.yumpu.com/nl/document/view/20452896/handleiding-enigma-machine-jotacross-2009>
4. <http://www.cryptomuseum.com/kits/enigma>