

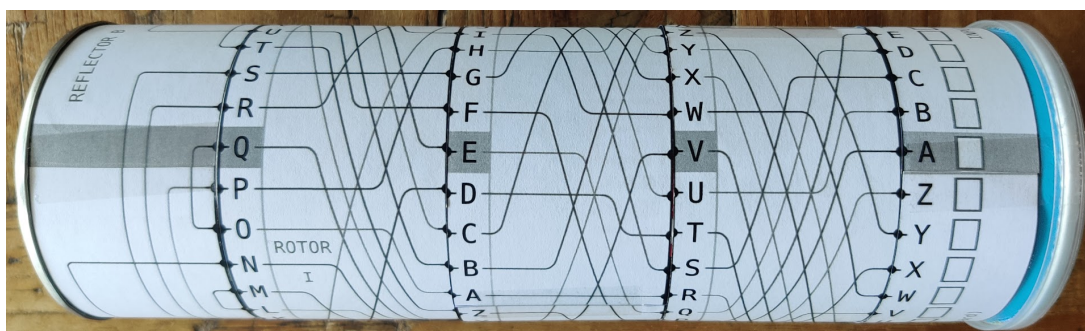
Het Raadsel Enigma

Opgaven

Deel I - Bouw je eigen Enigma

In dit deel ga je je eigen papieren Enigma bus bouwen die je in Deel II gaat gebruiken om een echt Enigma bericht te ontcijferen!

1. Knip de benodigde reflector en drie rotoren uit. Voor deze en alle volgende opgaven zijn dit de rotoren I, II en II en reflector B. Knip ook de input/output strip uit.
2. Plak deze strips zoals op het plaatje. Let hierbij op dat de grijze letters van de reflector en input/output strip op één lijn liggen. Van links naar rechts zie je de reflector, de drie rotoren en dan de input/output strip.
3. Zorg ervoor dat de reflector en de input/output strip zijn vastgeplakt aan de bus en dat de drie rotoren vrij kunnen draaien.



Om de papieren Enigma te gebruiken hoeft je nu alleen nog de Grundstellung in te stellen. Op het plaatje staat de Enigma ingesteld op Grundstellung QEV. Voor de Grundstellung ABC draai je de rotoren zo, dat er ABC komt te staan op de plek waar nu QEV staat (dus naast de grijze vlakjes op de reflector en input/output strip). Voor elke letter in je bericht doe je nu het volgende:

1. Draai de rechterrotor (in ons geval rotor III) één slag naar je toe (zodat de letter naast het grijze vakje één plek vooruit gaat in het alfabet). Zorg ervoor dat alle andere rotoren niet bewegen. **Let op:** dit doe je ook al voor de eerste letter!
2. Zoek nu de letter in je bericht op de input/output strip, en volg het lijntje door de drie rotoren, door de reflector, terug door de drie rotoren, en lees de output letter af op de input/output strip. Schrijf deze letter op.

Om te testen of je de papieren Enigma goed hebt gebouwd, staat hieronder het woord *enigma* met Grundstellung ABC en verder dezelfde instellingen als in de instructies:

XYZAUJ

De *turnover* speelt ook een grote rol bij de Enigmamachine. Dit is het punt waarop een rotor de linksliggende rotor meeneemt tijdens het draaien. Op de papieren enigma wordt dit aangegeven met de grijze letters op de rotoren. Volg de onderstaande regels goed:

1. Als de letter op de middelste rotor grijs is, draai je **alle drie** de rotoren.
2. Anders, als de letter op de rechter rotor grijs is, draai je de **middelste en rechter** rotor.
3. Anders draai je alleen de **rechter** rotor.

Onderstaand bericht heeft Grundstellung ABR, en er komt tijdens de versleuteling een turnover voor:

MABOBI

Deel II - Zelf ontcijferen

De Duitsers verspreidden de dagsleutel op sleutelbladen zoals deze

Geheim - Luftwaffe Allgemeine - Maschinenschlüssel für Monat Februar 1941														
Tag	Walzenlage		Ringstellung	Steckerverbindungen										Kenngruppen
28.	I	V II	U Y E	HT	MR	CY	VW	JZ	FN	QX	BP	yab	mly	ocl slg
27.	IV	V III	C N L	WX	GJ	AC	MZ	DI	FL	OY	NT	iog	vwd	ght cqv
26.	I	V II	H T M	HQ	WX	CE	PR	AU	BY	MZ	FK	otx	rgh	eps lgd
⋮	⋮		⋮					⋮						⋮

Tab. 1: Sleutelblad voor de periode 1940-1945

Op dit sleutelblad stond per dag de instellingen die gebruikt moesten worden om een bericht te vercijferen. De verzender en ontvanger hadden beide zo'n blad, en wisten dus hoe ze de machine in moesten stellen. Sommige karakters konden niet worden vercijferd met de Enigmamachine, zoals ü, ß, 1, 2, 3, ... Hier werden andere letters voor gebruikt:

Karakter in Duits	Vercijferd als
ch	Q
ß	SS
ä	AE
spatie/einde zin	X
1 (cijfers)	EINS

Tab. 2: Vertaaltabel voor Enigmaberichten

Opgave 1. Onderstaand bericht is versleuteld met een Enigmamachine met de volgende instellingen:

- Rotorvolgorde (Walzenlagen): I II III
- Startpositie rotoren (Grundstellung): MCK
- Stekkerbord (Steckerbrett): leeg
- Reflector (Umkehrwalze): B

Gebruik je papieren versie van de Enigmamachine en ontcijfer het bericht met de instructies uit Deel I. Let op dat het vercijferde bericht is ingedeeld in groepjes van vijf letters, om geen informatie weg te geven over de lengtes van de woorden. Dit bericht is ooit echt verzonden in de Tweede Wereldoorlog en versleuteld met een Enigmamachine!

HLWWT YXPAO UZIUUV VYYC UVSWI NMYGZ MQAYU ATPJW AETK

Deel III - Combinatoriek

In deze opgaven ga je met behulp van combinatoriek uitrekenen hoeveel verschillende instellingen de Enigmamachine had, om een idee te krijgen hoe moeilijk het was om de code te kraken.

Opgave 2 (Walzenlage). *Het centrale systeem van de Enigmamachine bestaat uit drie (verschillende) rotoren. Tot 1940 waren er in totaal drie mogelijke rotoren waar je uit kon kiezen. Na 1940 werden dit er vijf, en sommige versies van de Enigmamachine gebruikten er zelfs 8.*

- (a) *Op hoeveel verschillende manieren kun je rotoren kiezen voor de drie verschillende posities in de Enigmamachine uit een bak van drie rotoren?*
- (b) *Op hoeveel verschillende manieren kun je rotoren kiezen voor de drie verschillende posities in de Enigmamachine uit een bak van vijf rotoren?*
- (c) *Op hoeveel verschillende manieren kun je rotoren kiezen voor de drie verschillende posities in de Enigmamachine uit een bak van n rotoren?*

Opgave 3 (Grundstellung). *De Grundstellung geeft de beginstand van de rotoren aan. Dit wordt aangegeven met de letter die bovenop de rotor te zien is. In de Enigmamachine waren kleine vakjes uitgesneden, zodat je deze letter goed kon zien. Hoeveel van deze Grundstellungen zijn er mogelijk?*

Opgave 4 (Steckerbrett). (a) *Op hoeveel verschillende manieren kun je het stekkerbord bestekkeren met één kabel?*

- (b) *Laat zien dat je op 44850 manieren het stekkerbord kunt bestekkeren met twee kabels.*
- (c) *Laat zien dat je op 3453450 manieren het stekkerbord kunt bestekkeren met drie kabels.*
- (d) *In onderstaande tabel is te vinden op hoeveel manieren je het stekkerbord kunt bestekkeren met $1 \leq k \leq 13$ kabels. Vul de tabel verder in. Hoeveel kabels moet je gebruiken om zo veilig mogelijk berichten te kunnen versturen?*

k	Aantal manieren	k	Aantal manieren
0	1	7	$1.3 \cdot 10^{12}$
1	?	8	$1.1 \cdot 10^{13}$
2	44580	9	?
3	3453450	10	?
4	$1.6 \cdot 10^6$	11	?
5	$5.0 \cdot 10^9$	12	?
6	$1.0 \cdot 10^{11}$	13	$7.9 \cdot 10^{12}$

Opgave 5 (Complexiteit). Voor een instelling van de Enigmamachine is het volgende nodig:

1. Drie rotoren uit een bak van vijf (Walzenlage)
 2. Beginpositie van de rotoren (Grundstellung)
 3. Ringinstelling van de rotoren (Ringstellung)
 4. Stekkerbord met tien kabels (Steckerbrett)
- (a) Als we de Ringinstelling niet meerekenen, hoeveel mogelijke instellingen van de Enigmamachine zijn er dan mogelijk?
- (b) Een Britse codekraker kan elke vijf seconden checken of een bepaalde instelling van de Enigmamachine juist is. Hoe lang doet een team van 7000 codekrakers erover om alle mogelijke instellingen te checken (neem aan dat de codekrakers niet slapen).



Fig. 1: Een Enigmamachine. Met dank aan © Andy Hollingworth Archive en Simon Singh