

# Het Raadsel Enigma

Toelichting bij de slides

## Cryptografie

Schets een scenario aan de klas waarin ze een briefje moeten doorgeven door de klas. Hoe zorgen ze ervoor dat niemand die het briefje onderweg vasthoudt de inhoud ervan kan lezen? Dit moet natuurlijk op zo'n manier gebeuren dat de uiteindelijke ontvanger van het briefje wél de inhoud kan ontcijferen.

Misschien oppert iemand een versie van de Caesarversleuteling zoals in de slides. Om te versleutelen wordt elke letter drie plekken opgeschoven in het alfabet. Dit kun je nog veralgemeniseren door de letters een  $x$  aantal plekken op te schuiven.

Laat de leerlingen nadenken over een manier om deze manier van versleutelen te kraken. Hopelijk zegt iemand dat dezelfde letters worden afgebeeld op dezelfde letters. Zo kun je aan veelvoorkomende letters zien wat de verschuiving is. Bijvoorbeeld: ongeveer een vijfde van alle letters in het Nederlands is de letter e<sup>1</sup>. Alle letter e's worden in een bericht op dezelfde letter afgebeeld. In het gecijferde bericht kan men dus kijken welke letter (of letters) het meeste voorkomt: dit zal dan wel origineel de letter e zijn geweest. Deze methode heet *Frequentieanalyse*.

## Rotormachine

Tijdens de Eerste Wereldoorlog was Nederland neutraal, en wilde dat graag blijven. Dit bleek lastig vol te houden in Nederlands-Indië, dat bestond uit vele kleine eilandjes die onmogelijk allemaal in de gaten konden worden gehouden door de tien schepen die de Marine daar tot haar beschikking had. Het gebeurde dan ook vaak dat Britse, Franse of Japanse schepen het neutrale Nederlandse gebied binnenvoeren. Er mocht alleen aangevallen worden met strikte orders uit Batavia. Veilige communicatie was dus essentieel. De manier die tot dan toe werd gebruikt (codeboeken) was niet meer houdbaar, dus er was behoefte aan een nieuw cryptografisch systeem.

---

<sup>1</sup> <https://onzetaal.nl/taalloket/letterfrequentie-in-het-nederlands>

Twee luitenanten, Theo van Hengel en Rudolf Spengler kregen op Marinebasis Willemsoord (Den Helder) de taak om een nieuw apparaat te ontwerpen dat deze behoefte kon vervullen. Zij bedachten het idee van een rotormachine. Deze rotormachine is nooit gebruikt door de Nederlandse Marine, omdat van Hengel en Spengler het niet eens kon worden met de Staat over wie de eigenaar was van het patent.<sup>2</sup>

Onafhankelijk van elkaar bedachten meerdere uitvinders de rotormachine, maar de Nederlanders waren de eerste. De Duitse Arthur Scherbius patenteerde zijn eigen versie van de rotormachine in 1918, en noemde het *Enigma*. Hij verkocht zijn machine in eerste instantie aan commerciële partijen zoals banken en verzekeraars, maar had later ook een contract met het leger, aan wie hij een aangepaste versie van Enigma verkocht.

## Werking Enigma

De werking van een rotormachine (en daarmee de Enigmamachine) is het makkelijkste uit te leggen met een alfabet van zes letters. Links op het plaatje is een toetsenbord te zien, rechts een lampenbord. Als men de b indrukt, gaat de letter A branden. Hierna draait de rotor een zesde slag (bij de Enigmamachine 1/26-ste slag). Als we nu de b indrukken, gaat een andere letter branden.

Nu voegen we een tweede rotor toe, en bekijken we het systeem in twee dimensies in plaats van drie (anders worden de tekeningen onoverzichtelijk). De rechterrotor draait altijd als er een knop wordt ingedrukt. De linkerrotor draait alleen als de rechterrotor een volledige draai heeft gemaakt. De rotoren werken nu net als de wijzers op een klok: de minuutwijzer draait alleen als de secondewijzer een hele revolutie heeft voltooid. Een andere vergelijking is de kilometer teller op een oude auto.

Nu wordt de reflector toegevoegd. Nadat een signaal door de rotoren is gegaan, wordt het er weer door teruggestuurd. Dit heeft een ontzettend belangrijk gevolg. In het plaatje drukken we de b in, en gaat de D branden. De reflector zorgt ervoor dat als we de d hadden ingedrukt, dat daardoor de B ging branden. Deze werking zorgt ervoor dat de Enigmamachine werkt. Om te communiceren kan men dus een instelling van de Enigmamachine afspreken als geheime sleutel. Bij het intypen van het bericht beweegt de machine exact hetzelfde als bij het intypen van het gecijferde bericht.

Het is dus heel belangrijk om zoveel mogelijk mogelijke instelling van de machine te hebben. Dan zijn er namelijk heel veel mogelijke sleutels en is het dus moeilijker om de sleutel zomaar te raden. Om het aantal instellingen te

---

<sup>2</sup> Voor meer informatie: De Leeuw, Karl. "Dutch Invention of the Rotor Machine, 1915-1923" *Cryptologia* 27:1, 73-94, (2003).

vergroten werd het stekkerbord toegevoegd, waar twee letters worden verwisseld voordat het signaal door de rotoren gaat, en nadat het weer terugkomt. Dit stekkerbord heeft een gigantisch aantal mogelijkheden.

## Op slot

Elk bericht dat men wilde versturen moest 'op slot' gedaan worden met een sleutel. De sleutel veranderde elke dag om middernacht. Deze sleutels werden op sleutelbladen verspreid, per maand. Het totaal aantal mogelijke sleutels gaan de leerlingen ook uitrekenen in de opgaven. In de slides staat een voorbeeld van een sleutelblad van de landmacht uit mei 1938.

De *Walzenlage* is de volgorde van de rotoren. De *Ringstellung* is een interne instelling van de rotoren en geeft aan hoe de interne bedrading van de rotoren staat ten opzichte van het alfabet op de buitenste ring. De *Ringstellung* is vaak erg lastig te begrijpen zonder een echte Enigmarotor te zien. Daarom komt deze in de opgaven ook niet aan bod. De *Grundstellung* is de beginstand van de rotoren, de letters op het sleutelblad zijn de letters die op de Enigmamachine te zien zijn door de kleine raampjes. De kolom *Steckerverbindungen* geeft de instelling van het stekkerbord aan. Op 31 mei 1938 moest H verbonden worden met Z, R met V, etc. De kolommen *K.E.G.* en *Kenngruppen* zijn alleen ter controle en zijn voor deze les niet interessant/belangrijk.

## Enigma in Polen (1932)

In 1932 is er in Polen dreiging van twee kanten. In de Pools-Russische Oorlog (1919-1921) kreeg Polen belangrijke informatie door het kraken van vijandelijke cryptografie. Dit proces wilde ze opschalen, en daarom richtten ze in 1931 het Biuro Szyfrów op. Drie belangrijke wiskundigen die daar werkten waren Marian Rejewski, Jerzy Różycki en Henryk Zygalski. Van deze wiskundigen was Rejewski de belangrijkste.

## Methode Polen

Er staan hier de eerste zes letters van 65 Enigma berichten verstuurd op dezelfde dag. In deze tijd moesten Enigma operatoren zelf een drieletterige code verzinnen (voor zover dat mogelijk is) en deze twee keer versleuteld versturen. De eerste zes letters van een bericht zouden dus altijd verschillend moeten zijn. In realiteit werd zelden een compleet willekeurige drieletterige code verzonden. De ontcijferde berichtssleutels waren vaak drie keer dezelfde letter, een deel van

het alfabet of rijtjes van drie letters op het Enigma toetsenbord. Dit is leuk om door de leerlingen te laten raden.

## **Enigma in Polen (1933)**

Rejewski en zijn team kraakte Enigma dus al in 1933! Hetzelfde jaar dat Hitler aan de macht kwam in Duitsland. Hij gebruikte hiervoor onder andere de fouten de Duitsers maakte in de procedure van het verzenden van berichten (zoals op de vorige slides), maar ze hadden nog veel meer informatie nodig. Rejewski gebruikte heel veel permutatietheorie, en zijn originele paper die hij hierover schreef is interessant om te lezen, en begrijpbaar voor een eerstejaars wiskundestudent (maar zeker niet voor scholieren).

## **De volgende stap (1939/1940)**

De Duitsers maakten de code ingewikkelder door onder andere meer soort rotoren toe te voegen. Hierdoor werkte de methode van de Polen niet meer. De Polen stuurden op 30 juni 1939 een bericht naar de Fransen: "il y a du nouveau": er is iets gaande. De Fransen, de Britten en de Polen ontmoetten elkaar in Pyry, vlakbij Warschau. De Poolse wiskundigen gaven alles wat ze hebben over Enigma aan de Fransen en Britten. Blauwdrukken, berekeningen, ontcijferde berichten, etc. De Britten brachten al deze informatie naar Bletchley Park, waar ze kort daarvoor de GC&CS (Government Code and Cipher School, voorloper van huidige GCHQ) hadden opgericht. Hier werkte onder andere de bekende wiskundige Alan Turing, die uiteindelijk samen met zijn team een nieuwe methode bedacht om de Enigma berichten te kraken.

## **Rejewski en Turing**

De methodes van Rejewski en Turing verschillen fundamenteel van elkaar. Rejewski maakte gebruik van een ciphertext-only attack, die dus alleen gebruik maakte van de onderschepte berichten.

Bij Turing's gokt men eerst een deel van de tekst. Dat lijkt onmogelijk (het is immers het hele punt om de echte tekst te achterhalen), maar is mogelijk door een aantal eigenaardigheden van Duitse procedures. Door middel van triangulatie kan makkelijk achterhalen waar een bericht vandaan is verstuurd. Het weerbericht werd elke ochtend om 6 uur verstuurd. Als de verzendlocatie dan bekend is, is de kans groot dat het verzonden bericht het weerbericht van die locatie bevat (WETTERVORHERSAGEXBISKAYA).

De Duitsers moesten ook melden als er niks te melden was. De format (of vorm) van deze berichten was vaak hetzelfde, en dus waren

KEINEXBESONDERENXVORKOMMISSE

en

KEINEXBESONDERENXEREIGNISSE

ook goede gokken.

Zo'n gok voor een tekst noemen we een *crib*.

## Cribs

Als je eenmaal een crib hebt gevonden kun je deze onder het gecijferde bericht leggen. We willen erachter komen hoe 'diep' de crib in ons gecijferde bericht ligt. Hierbij maken we gebruik van het feit dat een letter nooit naar zichzelf kan worden gecijferd. We zien dat als het tekst inderdaad op deze plek in het bericht voorkomt, de S naar zichzelf gecijferd zou zijn. Dat kan niet, dus schuiven we de hele tekst een letter op. Zo gaan we door tot we een mogelijke plek voor het bericht hebben gevonden. Dit hoeft natuurlijk niet de enige mogelijkheid te zijn, maar het is belangrijk te bedenken dat crypto-analyse geen exacte wetenschap is.

## Menus

Van de crib kunnen we een *menu* maken. We denken dat dit deel van de tekst over generaal Rommel gaat. We schrijven alle letters op, en trekken een lijn tussen twee letters als ze onder elkaar staan.

Aangezien een stand van de Enigmamachine gegeven wordt door een transpositie weten we dat  $\pi_3(M) = G$  en  $\pi_3(G) = M$ .

We kiezen een willekeurige instelling van de Enigmamachine. Verder kiezen we een letter uit een cykel in het menu (op de slides G), en we kiezen een andere willekeurige letter (op de slides A). We testen de hypothese dat deze letters met elkaar verbonden zijn in de dagsleutel.

Nu hebben we het volgende diagram:

$$G \xrightarrow{\text{stekkerbord}} A \xrightarrow{\text{rotoren}} ? \xrightarrow{\text{stekkerbord}} M$$

We gebruiken nu de Enigmamachine zonder het stekkerbord, en drukken de A in. We krijgen dan de letter te zien die met M verbonden is op het stekkerbord (bijvoorbeeld de O). Zo kunnen we het hele menu rondwerken: we kunnen achterhalen waarmee de E is verbonden op het stekkerbord, vervolgens de F. Nu

kunnen we opnieuw kijken waarmee G is verbonden op het stekkerbord. Het blijkt dat we heel vaak op een andere letter uitkomen dan de A. Oftewel, onze hypothese is fout óf we hebben een verkeerde willekeurige instelling van de Enigmamachine gekozen.

De Turing-Welchman Bombe is een machine die deze beredeneringen automatisch en heel snel kan doen.

Als de Bombe een mogelijke oplossing had gevonden, stopte de machine. De operator schreef de mogelijke oplossing op, en liet de machine weer verder draaien. Ondertussen checkte de operator of de gevonden oplossing inderdaad de juiste was.

## Foute Bombestops

Het aantal keren dat de Bombe foutief stopte, kon worden beperkt. Turing schreef dat het aantal foutieve Bombestops worden gegeven door de formule op de slides. De HM-factor is een constante die afhangt van het aantal letters in het menu. We weten niet hoe Turing aan deze waardes komt. Hij schreef in zijn notitieboekje op dat de berekeningen 'tedious and uninteresting' zijn.

In de praktijk wilde men rond de 5 foute Bombestops. Er werd net zo lang gezocht naar een goede crib totdat men een menu had dat aan deze eisen voldeed.

Verder werden er talloze andere technieken gebruikt om Enigmaberichten te kraken, waaronder Banburismus en Rodding. Deze technieken maakten ook gebruik van zwakheden in de machine, en werden met de hand gedaan.

## Bletchley Park

Het is het waard om stil te staan bij Bletchley Park zelf. Het was een enorme operatie van zo'n 10.000 mensen die onderling heel hecht waren. Alle medewerkers moesten zweren nooit iemand te vertellen over hun werk, dus er werd onderling veel met elkaar gesproken en leidde tot een progressieve en vrije werkomgeving: een kleine maatschappij. Dit gecombineerd met excentrieke persoonlijkheden maakte Bletchley Park tot wat het was.

Bletchley Park werd omschreven als *The biggest bloody lunatic asylum in Britain*. Churchill had door hoe belangrijk Bletchley Park was voor de Oorlog, en noemde het *The geese who laid golden eggs and never cackled*. Dit omdat ze ontzettend waardevolle informatie leverden, terwijl ze weinig terug vroegen. Een beroemde memo van Churchill laat ook zien hoe belangrijk hij de werkzaamheden van Bletchley Park vond: *ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done*.

Eén van de meest markante figuren op Bletchley Park was Dilly Knox. Een ongelooflijke intelligente (en ietwat vreemde) taalkundige, die in de Eerste Wereldoorlog ook cryptograaf was: hij heeft geholpen met het kraken van het beroemde Zimmerman Telegram, waarna de Verenigde Staten zich mengden in de Eerste Wereldoorlog. De afdeling van Knox kreeg alle extreem moeilijke berichten die niet gekraakt konden worden. Zijn afdeling bestond alleen uit vrouwen, omdat hij vond dat mannen te snel afgeleid raakten. Zijn 'unit' kreeg de naam *Dilly's Fillies*.

Een van de vrouwen die bij hem werkte was Mavis Batey. Ze kwam als 19-jarige binnen op Bletchley Park en het eerste wat Knox tegen haar zei was *Oh, hello, we're breaking machines, have you got a pencil?*. Ze was verantwoordelijk voor het kraken van de versie van Enigma van de Italiaanse Marine, een van de meest ingewikkelde versies van Enigma.

Ze ontcijferde een bericht, en les *Today's the day minus three*. Niet wetende wat dat precies betekende, wachtte het team van Knox drie dagen. Na drie dagen kwam er een lang bericht binnen, dat ze nu konden kraken dankzij Batey. Het was een aanvalsplan van de Italiaanse Marine op de Britse vloot in de Middellandse Zee. Dankzij het kraken van dit bericht konden de Britten de aanval voorkomen.

Batey was ook verantwoordelijk voor het kraken van de versie van Enigma die werd gebruikt door de *Abwehr* (Duitse geheime dienst). Omdat de Britten nu wisten hoe ze de dagsleutel konden bepalen, konden ze dus ook nepberichten vercijferen en verspreiden als nepnieuws. Dit werd het *double cross* (XX) systeem genoemd.

Een van de belangrijkste manieren waarop deze tactiek werd gebruikt had te maken met de D-Day landingen en werd *Operation Fortitude* genoemd. De Britten lieten de Duitsers geloven dat de D-Day landingen plaats zouden vinden in Calais. Veel Duitse troepen werden daar dus heengestuurd, denkend dat er een grote aanval van de geallieerden zou komen. In realiteit kwamen de geallieerden aan land in Normandië, enkele honderden kilometers naar het zuiden.<sup>3</sup>

## Impact van Ultra

Alle informatie die verkregen is uit het kraken van Enigma wordt verzameld onder de naam *Ultra*. Op het hoogtepunt werden er 84.000 berichten per maand ontcijferd. Dat is een klus waar ongeveer 10.000 mensen aan mee hebben geholpen. Ongeveer driekwart van het personeel op Bletchley Park was vrouw.

<sup>3</sup> <https://www.cryptomuseum.com/people/batey/mavis.htm>

Het is lastig om te bepalen wat de invloed van Ultra is geweest op het verloop op de oorlog. Sommige schattingen zeggen dat het de oorlog met twee jaar heeft ingekort. Wat vast staat is dat het ongelooflijk waardevolle informatie heeft opgeleverd voor de geallieerden.

Churchill wist dat hij de strijd op het land en in de lucht zou gaan winnen. Over de strijd in het water had hij grote zorgen. De Duitse onderzeeërs gebruikten namelijk geavanceerde aanvalstechnieken, waar de Britse vloot niet tegenop kon. Churchill heeft gezegd dat Ultra de doorslaggevende factor was in *the Battle of the Atlantic*.

### **Meer weten?**

Zie Docentenhandleiding voor een kleine toelichting bij alle bronnen.