

Het Raadsel Enigma

Docentenhandleiding

Inleiding

Maar dit ga ik toch nooit in het echte leven gebruiken? is een veelgehoorde vraag in de wiskundeles op de middelbare school. De stof is vaak abstract en het is voor de leerling misschien niet meteen duidelijk waarom ze het voorgeschoteld krijgen. In deze les komen leerlingen in aanraking het maatschappelijk belang van wiskunde in de context van de Tweede Wereldoorlog.

Cryptografie gaat over het gebruiken van geheimtaal: het versturen van berichten die niemand kan lezen, behalve degenen met de juiste sleutel. Het is een door en door wiskundig onderwerp. Het analyseren en bedenken van cryptosystemen wordt al jaren gedaan door wiskundigen. Dit gecombineerd met de context van spionage en oorlog maakt het een spannend, interessant en belangrijk onderwerp.

In deze lesmodule gaat het om het begrip en de analyse van de Enigmamachine. Ze komen erachter hoe deze werkt door zelf berichten te ontcijferen met een zelfgemaakte papieren versie van de Enigmamachine, en ze analyseren de Enigmamachine door het aantal mogelijke instellingen te bepalen.

De lesmodule komt vanuit de wiskunde, maar is in feite een interdisciplinaire les, dat de vakken Wiskunde, Geschiedenis en Duits omvat.

Leerdoelen en doelgroep

Leerdoelen

Deel I Weten hoe de Enigmamachine werkt

Deel II Bericht kunnen ontcijferen met een papieren Enigma

Deel III Kunnen uitrekenen hoeveel mogelijke configuraties er zijn voor het instellen van de machine

Doelgroep

Het knutselen en ontcijferen van het bericht (Deel I en II) kan worden gedaan door leerlingen van elk niveau en leerjaar. Het gaat hier vooral om het goed kunnen lezen en volgen van instructies.

In Deel III komt pas echt wiskunde aan bod. Hiervoor is enige voorkennis van combinatoriek voor nodig. Ook kunnen leerlingen het extra combinatoriek document bij de opgaven houden. Opgave 2 en 3 kunnen worden gemaakt door zowel Wiskunde A als Wiskunde D leerlingen die al in aanraking zijn geweest met cryptografie. Opgave 4 is al uitdagender. Hier moeten leerlingen inzien dat je dubbel getelde combinaties weg kunt delen. Men kan dus kiezen om Wiskunde A leerlingen alleen opgave 2 en 3 te laten doen, het antwoord op opgave 4 geven. Hiermee hebben ze genoeg informatie om opgave 5 te doen. Wiskunde D leerlingen kunnen de uitdagende opgave 4 wel doen. Let op dat hier ook meerdere mogelijkheden zijn om tot het antwoord te komen. Een extra opgave kan dus zijn om meerdere methodes te bedenken en te bewijzen dat deze equivalent zijn.

Praktische informatie

Lesoverzicht

De les bestaat uit twee delen: de presentatie en de opgaven. In de presentatie krijgen de leerlingen informatie over de Enigmamachine. De presentatie behandelt de werking van de Enigmamachine, hoe deze is gekraakt door de Polen en Britten en de impact van het kraken ervan op het verloop van de Tweede Wereldoorlog.

In Deel I proberen de leerlingen van de Enigmamachine beter te begrijpen. Ze knutselen hun eigen Enigmamachine van een Pringle bus en een werkblad, om uiteindelijk (met tussenstappen) een bericht te ontcijferen dat echt in de Tweede Wereldoorlog is verzonden (en versleuteld met een Enigmamachine).

In Deel II staat de wiskunde van de Enigmamachine centraal. De veiligheid van de machine werd gerealiseerd door het grote aantal mogelijke instellingen van de machine. Om een bericht te kraken had je de juiste instelling nodig, maar gokken was dus nutteloos. In dit deel gaan de leerlingen zelf uitrekenen hoeveel mogelijke instellingen de Enigmamachine heeft om daarmee een idee te krijgen van de veiligheid van de machine. Combinatoriek staat hier dus centraal.

Benodigdheden

Voor n leerlingen is het volgende nodig:

- n opgavevellen
- n werkbladen 'Paper Enigma'. (Let op dat deze op de goede schaal worden geprint. Probeer eerst zelf een papieren Enigma te bouwen met je eigen werkbladen)
- n Pringlesbussen (Er kan gekozen worden om in tweetallen te werken, in dat geval heb je $n/2$ Pringle bussen nodig)
- Scharen en plakband

Lesduur

De presentatie neemt ongeveer 35-45 minuten in beslag. Afhankelijk van de snelheid van de leerlingen kunnen de opdrachten 60-120 minuten duren.

Lesindeling

Presentatie (35-45 min)

Tijdens de presentatie hoeven de leerlingen in principe niets te doen. De leerlingen worden wel aangemoedigd om na te denken over cryptografische problemen en deze te delen.

Opgaven (60-120 min)

Hier gaan de leerlingen zelf aan de slag. De opgaven bestaan uit twee delen. In Deel I gaan de leerlingen zelf aan de slag met als uiteindelijk doel het ontcijferen van een echt Enigma bericht. In Deel II staat de combinatoriek centraal en gaan de leerlingen onderzoeken hoe veilig de Enigmamachine nu eigenlijk was. De volgorde van de delen kan worden aangepast. Zo kan de docent ervoor kiezen om eerst Deel II uit te delen en Deel I pas uit te geven als de leerling Deel II heeft gedaan.

Deel I In dit deel gaat de leerling zelf een Enigmamachine bouwen, om daarna een code te ontcijferen met de Enigmamachine. Er zit best wat nuance in de draaiing van de roteren. Als de papieren Enigmamachine eenmaal geknutseld

is, worden dezes nuances één voor één toegevoegd aan de opgaven. Bij alle berichten is de juiste instelling voor de Enigmamachine gegeven. De opgave in het volgende deel is dus alleen maar het ontcijferen van het berichten, er hoeft niks gekraakt te worden. Om het overzichtelijk te houden is het stekkerbord leeg, alhoewel deze wel kan worden toegevoegd. De rotorvolgorde van elke tekst is ook hetzelfde, dus als de papieren Enigma eenmaal is gebouwd, kan deze voor alle drie de opgaven worden gebruikt, zonder hem uit elkaar te hoeven halen.

De eerste tekst is bedoeld om te checken of de leerling het idee snapt van de rotormachine. Hier is het belangrijk dat een letter wordt al afgelezen *voordat* de rotor draait. Dit bericht is kort, dus de enige rotor die draait, is de linker rotor. Dit heeft het effect dat het eerste bericht makkelijk te ontcijferen is, en geeft de leerling (hopelijk) de motivatie om de andere (ietswat moeilijkere) berichten te ontcijferen.

Bij de tweede tekst is er een *turnover*. De links liggende rotor neemt de middelste rotor mee. Dit is aangegeven met een grijze letter (zie ook de bouw instructies).

Deel II De derde en laatste tekst is het lastigst. Dit komt omdat het een langere tekst is, en waar dus vaker een turnover voorkomt.

Het is heel makkelijk om bij dit deel je eigen opgave te bedenken. Gebruik een simulator (of de papieren Enigma) om je eigen bericht te versleutelen en laat de leerlingen deze ontcijferen. Je kunt zelfs nog een wedstrijdelement toevoegen door een prijsje te geven aan de snelste codebreker. Een simulator die erg geschikt is, is <https://cryptii.com/pipes/enigma-machine>. Gebruik een Enigma M3, *Umkehrwalze* (UKW) B en rotorvolgorde I, II, III. Laat de Ringstellung op A voor alle rotoren. Het *steckerbrett* (stekkerbord) blijft leeg. Dit zijn dezelfde instellingen als in de opgaven. De *Grundstellung* (Position in de simulator) kun je zelf verzinnen. Let op dat langere berichten moeilijker zijn, aanzien er vaker een turnover voorkomt, en je makkelijk je positie in het bericht verliest (en je dus weer opnieuw moet beginnen).

Deel III In dit deel zal voorkennis over combinatoriek heel erg van pas komen. Er zullen dan ook verschillen zijn tussen de leerlingen. De docent kan ervoor kiezen om eerst nog een kleine snelcursus combinatoriek te geven, of de opgaven klassikaal te doen. Dit hangt volledig af van de voorkennis van de leerlingen. De docent bepaalt dus zelf de indeling van dit deel.

Literatuurlijst

In de loop der jaren is er veel geschreven over Enigma. Hieronder staan een aantal bronnen die door de docent geraadpleegd kunnen worden. De docent kan natuurlijk ook de leerling naar deze bronnen doorverwijzen.

- The Code Book, Simon Singh (bekend van *Numberphile*). Leesbare geschiedenis van cryptografie van Caesar versleuteling tot quantumcryptografie. Erg leesbaar voor niet-wiskundigen, en daarmee ideaal voor de geïnteresseerde leerling.
- Alan Turing: The Enigma, Andrew Hodges. Biografie over Alan Turing
- The Hut Six Story, Gordon Welchman. Welchman was een van de wiskundigen op Bletchley Park en werkte nauw samen met Alan Turing. Dit technische boek beschrijft methodes om Enigma berichten te kraken.
- Cryptology, Classical and Modern, Klima & Sigmon. Wiskundeboek over cryptografie, geschreven door (ex-)medewerkers van de NSA.
- Cryptomuseum: cryptomuseum.com. Een fantastische website waar veel grondige informatie over alle mogelijke crypto- en spionnenapparatuur te vinden is.
- The Queen of Codes, Jackie Uí Chionna. Biografie van Emily Anderson verschenen in 2023. Het boek onthult dat Anderson een van de beste codekrakers van het Verenigd Koninkrijk was, zonder dat ook maar iemand daarvan wist.
- The Rose Code, Kate Quinn. Een roman over drie vrouwen die op Bletchley Park werkten, gebaseerd op onder andere Mavis Batey. Het boek weet de sfeer van Bletchley Park goed te vangen.
- The Imitation Game (2014) is een film over Alan Turing, gebaseerd op het boek van Andrew Hodges. Dit is een film die je heel goed in de klas kunt kijken. Let wel op dat het geen documentaire is, maar een film. Er zitten veel onwaarheden in, maar desalniettemin is het een goede introductie in de wereld van Enigma en Alan Turing/Bletchley Park.
- <https://www.networkpages.nl/enigma-a-complexity-titan/>. Artikel voor middelbare scholieren waar dit ScienceLab uit voortgekomen is. Er is onder andere informatie te vinden over de combinatorische aspecten van de Enigmamachine, dus verwijst de leerlingen pas na de les door..

Over deze lesmodule

Deze lesmodule is voortgekomen uit mijn presentatie en workshop over Enigma bij *Leve de Wiskunde!* op de Universiteit van Amsterdam op 21 april 2023. Na de module meerdere keren te hebben getest (vak Klassieke Cryptografie in de Informatica Bachelor, Nationale Wiskunde Dagen in Noordwijkerhout), hebben vier leerlingen van de Bachelor Wiskunde aan de UvA feedback verzameld en aanpassingen gedaan voor het vak 'Onderwijs en Communicatie' in het tweede jaar. Hieruit is onder andere het supplement combinatoriek uit ontstaan.

Het hele project is al begonnen in 2021, toen ik bij Raf Bocklandt mijn bachelorscriptie heb geschreven voor de Bachelor Wiskunde. Hier is mijn enthousiasme en passie voor alles Enigma en cryptografie begonnen. De geïnteresseerde lezer kan mijn scriptie vinden in de scriptiebank van de UvA: https://scripties.uba.uva.nl/search?id=record_29012.

Voor vragen of opmerkingen over de inhoud van de les kan contact worden opgenomen met Stijn Maatje (stijnmaatje@gmail.com). Voor andere vragen of opmerkingen kun je contact opnemen met Nicos Starreveld (n.j.starreveld@uva.nl).

Al het materiaal mag worden hergebruikt voor *onderwijs gerelateerde activiteiten* onder een Creative Commons licentie. Vermeld hierbij Stijn Maatje, Diene van Batenburg, Tristan de Boer, Marijne Buhrman, Sjoerd Stoop en de Universiteit van Amsterdam.

Stijn Maatje, 2024