De Baas Op Internet

Module 3:

Geheimtaal

Leerkrachtinstructie

Ontwikkeld door:

waag society

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

NETWERK DEMOCRATIE

Gerealiseerd met bijdragen van:

SIDN fonds

FONDS 21

debaasopinternet.nl

Onderzoek:

DE CODE IS ALTIJD TE KRAKEN

Soms wil je dat jouw bericht alleen gelezen kan worden door degene voor wie het bestemd is. Dan kun je er geheimtaal van maken. Op het internet heet dat encryptie: Je versleuteld een bericht zodat alleen de ontvanger het kan ontsleutelen. Geheimtaal (ook wel cryptografie genoemd) is altijd al belangrijk geweest, ook voordat er computers waren. Door geheimtaal konden de Egyptische farao's de nieuwste roddels aan elkaar doorgeven. Maar wat is cryptografie precies en hoe werkt het?

Thema We maken kennis met geheimtaal: Het versleutelen van boodschappen. We denken na over berichten die we in geheimtaal zouden willen versturen. Ook leren we de achterliggende principes van geheimtaal beter begrijpen.	**Doelgroep** PO groep 7 en 8 VO 1e en 2e klas **Lesduur** 1,5 uur (of 2x 45 minuten)
Lesdoel Begrijpen wat geheimtaal is en snappen waarom cryptografie (geheimtaal) van belang kan zijn bij het versturen van berichten.	**Benodigdheden** Werkbladenset (1 per leerling) Losse vellen papier Splitpennen (om Caesarschijven in elkaar te zetten) Oude boeken (waarin getekend mag worden) Knutselmateriaal: Scharen, pennen, stiften, lijm, nietmachine, plakband Eventueel cijferslotjes/kistjes of andere dingen voor een escape room (mogen leerlingen zelf meenemen)
Voorbereiding Lesmateriaal downloaden Lesmateriaal doornemen Werkbladen printen Materialen verzamelen Caesarschijven in elkaar zetten Leerlingen instrueren om materiaal van thuis mee te nemen om in te zetten in de escape room, denk aan: Hangslotjes, cijferslotjes, kistjes die af te sluiten zijn.	**Vakgebieden** Deze module draagt bij aan de PO kerndoelen: Nederlands: 2, 3, 4 Rekenen/wiskunde: 23 Oriëntatie op jezelf en de wereld, Natuur en techniek: 44,45 Deze module draagt bij aan de VO kerndoelen: Nederlands: 1, 6 Mens en natuur: 29, 31, 33 Mens en maatschappij: 36, 38, 39 De module kan gegeven worden binnen de vakken informatica, techniek, maatschappijleer en de mentorles.

Stap 1	**Berichten versleutelen en ontcijferen** We oefenen met vijf verschillende geheimtalen om berichten te versleutelen en ontcijferen. Kun je de cryptografie ontrafelen? Lukt het zelf berichten te versleutelen? Het belangrijkste in iedere geheimtaal is de sleutel die nodig is om de geheimtaal te snappen. Daarmee kan de ontvanger het bericht begrijpen maar iemand die de sleutel niet heeft kan dat niet.
Stap 2	**Bouw een escape room** Met de kennis die is opgedaan over het versleutelen van berichten in geheimtaal, gaan we in teams escape games maken. Een escape game is een reeks puzzels die opgelost moet worden om een geheime boodschap te vinden. Met je team krijg je een half uur om een boodschap te versleutelen. Hierbij gebruik je minimaal twee cryptografiemethodes. Aanvullend daarop kun je puzzels gebruiken zoals raadsels, rebussen, sudoku of kruiswoordpuzzels. Het antwoord van puzzel 1 leidt tot de sleutel van puzzel 2. En puzzel 2 leidt tot het bewaarde geheim, bijvoorbeeld de code van een slotje of het bericht dat beveiligd moest worden. Zo ontstaat een soort mini “escape room”.
Stap 3	**Speel de escape rooms** Wanneer alle escape rooms goed en wel beveiligd zijn, gaan de teams elkaars escape rooms ervaren. Hierbij proberen ze de cryptografie te ontrafelen en de verborgen boodschap te ontdekken. Als dat niet lukt, dan demonstreren de bouwers hoe de raadsels opgelost hadden moeten worden.

Belangrijke ideeën:

- Mensen hebben altijd geheime berichten verstuurd en zijn daar behoorlijk inventief in geweest.
- Geheimschrift bestaat uit drie onderdelen:
  - het originele bericht
  - het versleutelde bericht
  - en de sleutel: de wijze waarop het bericht te ontcijferen is
- Het versleutelen van berichten heet encryptie of cryptografie.
- Ieder versleuteld bericht is te ontcijferen, hoe gecompliceerd de sleutel ook is.

Geheimen zijn van alle tijden. Geheimtalen ook.

Het geheim willen houden van informatie is geen mens vreemd. De Romeinen kenden al inventieve manieren om boodschappen over het slagveld of door het Romeinse rijk te versturen.

Hoe vervoer je de sleutel?

De cryptografie methodes waarmee we oefenen zijn slechts een kleine greep uit de mogelijke manieren waarop je een geschreven bericht kunt versleutelen. In alle gevallen is het belangrijk dat alleen de schrijver en de ontvanger weten welke methode er precies gebruikt wordt en wat de sleutel is.

Als iemand het bericht onderschept of de sleutel onderschept, dan is er nog geen probleem. Maar wanneer iemand beide weet te bemachtigen, dan kan deze het bericht gemakkelijk lezen. Dit is een probleem met alle analoge en digitale encryptiemethodes: Hoe vervoer je de sleutel?

In de module ‘Encryptie’ gaan we verder in op digitale manieren om berichten te versleutelen. Met de komst van de computer is er ook een antwoord gevonden op het vraagstuk van het vervoer van de sleutel.

Belangrijke begrippen:

- **Geheimtaal**
  Ook wel cryptografie genoemd. Een taal die voor zender en ontvanger te begrijpen is maar voor anderen niet.

- **Versleutelen**
  Informatie zo bewerken dat deze alleen begrijpelijk is als je de sleutel hebt.

- **Sleutel**
  In de context van deze module is de sleutel de hint, de informatie, het inzicht of ander element dat maakt dat de lezer de cryptografie kan doorgronden en toegang krijgt tot de boodschap.

- **Encryptie**
  Het coderen (versleutelen) van gegevens, een bestand of een boodschap op basis van een bepaalde logica. Deze versleutelde gegevens kunnen ook weer ontcijferd of gedecodeerd worden zodat men de originele informatie weer terugkrijgt. Dit proces wordt decryptie genoemd. (Moderne digitale versleuteling krijgt meer aandacht in de module ‘Encryptie’.)

- **Escape room**
  Dit is een spel waarbij je als groep in een kamer wordt opgesloten, het doel is om te ontsnappen door het samen oplossen van puzzels en raadsels. Het spel is zo uitdagend, dat maar een klein deel van alle groepen zonder hulp ontsnapt. In deze les gaan we gelukkig niemand opsluiten, maar we gaan wél aan de slag om cryptografie en geheimtaal in te zetten om puzzels en raadsels voor elkaar te maken.

Verdieping:

- **Geheimschrift (Klokhuis aflevering)**
  Als je iets meer tijd hebt voor de les, kijk dan samen naar de Klokhuis aflevering over geheimschrift.
  https://www.hetklokhuis.nl/tv-uitzending/1248/Geheimschrift

TIJD:	OEFENING:	WERKVORM:	MATERIAAL:
5 min.	**Introductie** Wie weet wat cryptografie is? Cryptografie wordt nu gebruikt voor versleuteling op internet, maar het beveiligen van berichten is altijd een belangrijk vraagstuk geweest. Deze les gaan we verschillende versleutelmethodes uitproberen en zelf een boodschap zo goed mogelijk beschermen. ➔ **Start met een paar prikkelende vragen:** - Hoe bewaar je een geheim? - Wanneer maak jij gebruik van geheimtaal? - Hoe ontcijfer je geheimtaal? - Is een streepjescode ook een geheimtaal? ➔ **Schrijf de antwoorden en ideeën van de leerlingen op het bord.** Afronding: Deze les gaan we zelf aan de slag met geheimtaal en het verbergen van boodschappen. Wanneer we dat kunnen, dan gaan we in teams een escape room bouwen.	***Klassikaal***	***Schoolbord***
30 min.	**Stap 1. Berichten versleutelen en ontcijferen** In de werkbladen vind je vijf cryptografie methodes. ➔ **Pak een leeg vel papier en probeer de methodes uit. Kun je een code kraken? Kun je een code maken?** ➔ **Schrijf op het werkblad een geheime boodschap voor degene die naast je zit. Kunnen jullie elkaars boodschappen ontcijferen? Lukt het om alle vijf methodes uit te proberen?** ➔ **Loop rond en vraag hoe het gaat.** ➔ **Daag leerlingen uit om breder over cryptografie en geheimtaal na te denken. Wie verstuurt er berichtjes via de telefoon? Hoe komt het dat anderen dan niet kunnen meelezen?** Verdieping: De kans bestaat dat leerlingen over end-to-end encryptie bij Whatsapp beginnen. Dat is inderdaad een veilige manier om te communiceren: Niemand kan meelezen. Maar: 'meta-data' wordt wel opgeslagen: Met wie je appt, wanneer en hoe vaak. Lees er hier meer over: https://bof.nl/2017/03/02/hoe-end-to-end-encryptie-jouw-communicatie-veilig-houdt/ Afronding: Leg een link met de module over Privacy. Zijn er berichten die ze liever versleuteld zouden willen versturen? Wanneer wil je er zeker van zijn dat niemand meeleest?	***Tweetallen***	***Werkbladen Oefenblad 'Berichten versleutelen' Pennen Losse vellen papier Oude boeken Caesarschijven***

TIJD:	OEFENING:	WERKVORM:	MATERIAAL:
30 min.	**Stap 2. Bouw een escape room** "Jullie hebben een half uur om in teams een boodschap aan je klasgenoten te bedenken en te beveiligen. Gebruik minimaal twee puzzels. Het antwoord op de eerste puzzel is de aanwijzing waarmee de tweede puzzel opgelost kan worden." "Je kunt de encryptiemethodes gebruiken, maar ook: kruiswoordpuzzel, rebus, sudoku, romeinse cijfercode, raadsel, latijnse/griekse tekst ontcijferen, morse code. Ken je nog andere puzzels?" ➔ **Deel de leerlingen in teams in.** ➔ **Controleer of leerlingen wel manieren bedenken waarmee de escape room voor anderen op te lossen is. Het mag niet té moeilijk worden. Ze moeten hun klasgenoten een beetje helpen met duidelijke aanwijzingen.** Afronding: Zorg dat de teams hun puzzels op tijd afronden, zodat er voldoende tijd overblijft voor stap 3 - het uitproberen van de escape rooms.	***Teams (3 - 5 personen)***	***Losse vellen papier*** ***Eventueel materiaal van thuis.***
20 min.	**Stap 3. Speel de escape rooms** Ieder team gaat nu een escape room van een ander team proberen op te lossen. ➔ **Zorg dat er per escape room een escape game master is van het team dat de puzzels gemaakt heeft. Die leerling introduceert de escape room aan de spelende groep. Die persoon vertelt ook wat er wel en niet mag in de escape room.** ➔ **Zet een timer en vertel tussendoor hoeveel tijd de teams nog hebben om het op te lossen. ("Nog 10 minuten, nog 5… de laatste minuut!")** Afronding: Als een escape room niet binnen de tijd wordt opgelost, laat de escape game master dan toelichten hoe de cryptografie ontsleuteld had kunnen worden.	***Teams (3 - 5 personen)***	

5 min.

Afronding

Klassikaal

➔ Kom terug op de boodschappen die de teams versleuteld hebben. Stel hierbij vragen:

Welke eigen boodschappen zou je willen versleutelen in het dagelijks leven? Zou je dat middels de escape room van team X doen? Hoe bepaal je wie de geheimtaal mag begrijpen?

➔ Vertel dat er later in de module 'Encryptie' met de klas verder gekeken wordt op welke manier een computer of telefoon cryptografie inzet om berichten die over het internet verstuurd worden, te versleutelen.

Antwoorden

In deze module zijn geen goede antwoorden te geven. Wanneer de leerlingen de aanwijzingen gevolgd hebben en de escape rooms 'gekraakt' zijn is de les geslaagd.