

Module 3:



Geheimtaal

Docenthandleiding

Ontwikkeld door:



waag
technology & society

**BITS OF
FREEDOM**
Voor jouw internetvrijheid

**NET
WERK
DEMO
CRATIE**

Gerealiseerd met bijdragen van:

SIDNfonds FONDS21

debaasopinternet.nl

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License



Module 3, Versie 1.1










Lesoverzicht

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 ontslutelen. 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?

	<p>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.</p>	 	<p>Doelgroep PO groep 7 en 8</p> <p>Lesduur 45 minuten</p>
	<p>Lesdoel Begrijpen wat geheimtaal is en snappen waarom cryptografie (geheimtaal) van belang kan zijn bij het versturen van berichten.</p>		<p>Benodigheden</p> <ul style="list-style-type: none"> . Werkbladenset (1 per leerling) . Losse vellen papier . Splitpennen (om Caesarschijven in elkaar te zetten) . Oude boeken (waarin getekend mag worden) om mee te versleutelen. . Video Missie 3 (Portal DG GvW)
	<p>Voorbereiding Lesmateriaal downloaden (Portal DG GvW) Lesmateriaal doornemen Werkbladen printen Materialen verzamelen Caesarschijven in elkaar zetten</p>		<p>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</p>



Lesopbouw

Stap 1	<p>Berichten versleutelen en ontcijferen</p> <p>We oefenen met twee verschillende geheimtalen om berichten te versleutelen en ontcijferen.</p> <p>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.</p>
---------------	--

Samenvatting

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 module 5 '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.





Samenvatting (vervolg)

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 5 'Encryptie'.)

Verdieping:

- **Geheimschrift (Klokhuis aflevering)**
Als je iets meer tijd hebt voor de les, kijk dan samen naar de Klokhuis aflevering over geheimschrift. ([link op Portal DG GvW](#))



Draaiboek

Gebruik de video 'Missie 1' als presentatie / leidraad op je digibord in deze les

TIJD:	OEFENING:	WERKVORM:	MATERIAAL:
7 min	<p>Introductie</p> <p>Wie weet wat cryptografie is? Cryptografie wordt nu gebruikt voor versleuteling op internet, maar het beveiligen van berichten is altijd een belangrijk vraagstuk geweest.</p> <p>Deze les gaan we verschillende versleutelmethodes uitproberen en zelf een boodschap zo goed mogelijk beschermen.</p> <p>Start met een paar prikkelende vragen:</p> <ul style="list-style-type: none"> - Hoe bewaar je een geheim? - Wanneer maak jij gebruik van geheimtaal? - Hoe ontcijfer je geheimtaal? - Is een streepjescode ook een geheimtaal? <p>Schrijf de antwoorden en ideeën van de leerlingen op het bord.</p> <p>Afronding: Deze les gaan we zelf aan de slag met geheimtaal en het verbergen van boodschappen.</p>	klassikaal	Digibord
30 min	<p>Stap 1. Berichten versleutelen en ontcijferen</p> <p>In de werkbladen en Video Missie 3 vind je twee cryptografie methodes.</p> <ul style="list-style-type: none"> ☒ 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 3 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 meelesen? 	Klassikaal / tweetallen	<ul style="list-style-type: none"> . Video Missie 3 . Set werkbladen 1 per leerling . Caesar schijven . splitpennen
7 min	<p>Afronding:</p> <p>Leg een link met les over Privacy (Portal DG GvW).</p> <ul style="list-style-type: none"> . Zijn er berichten die ze liever versleuteld zouden willen versturen? . Wanneer wil je er zeker van zijn dat niemand meeleeft? . Welke eigen boodschappen zou je willen versleutelen in het dagelijks leven? 	klassikaal	