

## Het beroepsproduct

Titel: 'Dit mag je niet weten! Veilige communicatie in het digitale tijdperk.'

### Inleiding

In deze opdracht van Beta excellent ga je alleen of in een groepje van leerlingen zelf ontdekken hoe je veilig kunt communiceren op het internet via versleutelde berichten. Je gaat leren hoe je een eenvoudige boodschap kunt versleutelen en weer kunt ontcijferen. Aan het eind van de opdracht lees je hoe je resultaten worden beoordeeld.

### Doel

Het doel van deze opdracht is dat je leert om een ontwerp te maken voor een systeem waarmee je berichten kunt versleutelen en weer kunt ontcijferen. Je gaat dit ontwerp voorbereiden, uitvoeren en testen. Na het testen schrijf je op wat je er van hebt geleerd en hoe je ontwerp door de test is gekomen. Je ontwikkelt je vaardigheid om een goede strategie te kiezen die tot een bruikbare oplossing leidt. Hiervoor heb je kennis nodig van de getaltheorie en hoe deze theorie in de afgelopen tijd zich heeft ontwikkeld.

De getaltheorie is begonnen bij de Griekse wiskundige Euclides. Andere wiskundigen zoals Euler, Fermat en Turing hebben de theorie uitgebreid en geschikt gemaakt om berichten te versleutelen. Je leert hoe de geschiedenis van de cryptografie die ooit bij de Romeinse keizer Julius Caesar is begonnen zich heeft ontwikkeld in de Tweede Wereldoorlog en in het digitale tijdperk waarin we nu leven.

### De weg naar je doel

De opdracht die je krijgt geeft veel vragen en uitdagingen waarbij je ruimte krijgt waarin zelf kunt kiezen. Je creativiteit zal worden geprikkeld, maar je zult ook keuzes moeten maken en goed moeten plannen om de opdracht op tijd klaar te krijgen. Je wordt geholpen hierbij met video boodschappen, hints, tussentijdse uitdagingen en de docent die je begeleidt.

### Waarom is deze opdracht belangrijk?

Het lijkt soms alsof we nog nooit zo veel met elkaar hebben gecommuniceerd als nu, in het digitale tijdperk. Elke leerling heeft een mobiele telefoon en 24 uur per dag Whatsapp, Facebook en Instagram tot zijn of haar beschikking. Maar met deze toename zijn er ook steeds meer zorgen over de privacy. Daarom versleutelt Whatsapp tegenwoordig alle berichten. En daarom heeft Google een uitgebreid privacy regelement. Maar is dat genoeg? En hoe werken die systemen van versleuteling? Werken ze wel echt? Dat wil je toch zelf ontdekken! Om meer te weten over moderne versleuteling (cryptografie) moeten we terug naar de kern, terug in de geschiedenis van de wiskunde.

### De onderdelen van deze opdracht

1. Getaltheorie, wat zijn getallen eigenlijk?
2. Verzamelingen en delers. Het algoritme van Euclides
3. Modulo rekenen
4. Cryptografie van Julius Ceasar, de eerste geheime oorlogscommunicatie
5. Diophantes, Fermat, Euler en zijn indicatoren
6. Vigenère en andere systemen
7. Je eigen cryptografisch ontwerp maken.
8. Je ontwerp testen, uitvoeren en presenteren

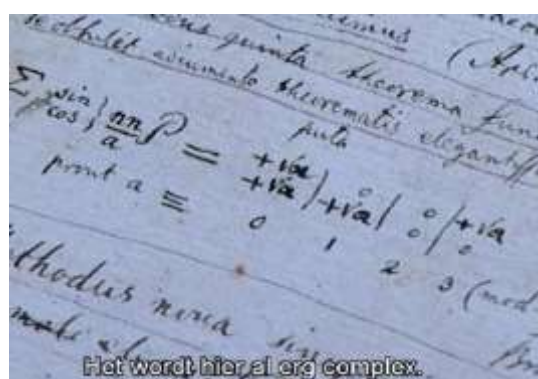
Bij elk onderdeel zijn een aantal standaardvragen die je moet beantwoorden en naar keuze een aantal praktische opdrachten van verschillende moeilijkheidsgraden. Uit die opdrachten kies je die opdracht die jou of jullie het meeste aanspreekt. Je mag alleen werken of in een groepje, zolang je dit maar goed overlegt met je docent. Als je in een groepje werkt, moet je achteraf goed beschrijven wie wat heeft gedaan en welke bijdrage ieder heeft geleverd aan het eindproduct.

**Stap 1** De eerste stap is om deze opdracht helemaal goed door te lezen en op zoek te gaan naar meer informatie over het onderwerp cryptografie. Op internet is hier veel over te vinden en elke week krijg je veel links die je hierbij op weg helpen. Schrijf in een kort deelverslag wat je onderzoek heeft opgeleverd (Hoofdstuk 2).

**Stap 2** Maak een planning voor jezelf waarbij je in een schema zet wat je allemaal gaat doen, wanneer je het gaat doen en hoeveel tijd je hiervoor denkt te gebruiken. Maak het een realistische planning. Je mag je houden aan de volgorde van de onderdelen zoals ze in deze opdracht staan, maar je mag ook je eigen volgorde bepalen. Als het resultaat maar is dat je een eigen ontwerp maakt met een goede wiskundige argumentatie erbij.

**Stap 3** Maak een lijstje met alles wat je belangrijk vindt voor je eigen ontwerp. Waar moet het aan voldoen? Hoe ga je het ontwerp testen? Hoe wil je het presenteren?

**Stap 4** Elke week werk je aan de vragen die gesteld worden in de onderdelen van de opdracht en maak je keuzes over de soort van versleuteling waar je je in wilt verdiepen. Er zijn vaste feedback momenten met je leraar. Hierin vraag je toestemming om door te gaan op de weg die je hebt gekozen. Je moet hierbij laten zien dat je de kennis en vaardigheden hebt die nodig zijn om het gekozen product ook echt af te maken.



**Stap 5** Als je geleerd hebt wat priemgetallen zijn en hoe je kunt werken met modulo rekenen en binaire getallen ga je een eerste voorstel formuleren voor je begeleider. In het voorstel staat welk soort van versleuteling je wilt ontwerpen en waarom je daarvoor kiest. Je ontwerp hoeft nog niet helemaal uitgewerkt te zijn, maar je weet er genoeg van om aan een ander duidelijk te maken welke wiskundige vaardigheden en toepassingen je gaat inzetten. (Hoofdstuk 3)

**Stap 6** Als je toestemming hebt gekregen om je ontwerp af te maken ga je je eigen versleutelings systeem bedenken. Je maakt een korte boodschap die je gaat versleutelen en je maakt een bijbehorende sleutel. Geef aan welke wiskundige formules en vaardigheden je hierbij nodig hebt. (Hoofdstuk 4) . Je gaat je ontwerp testen op andere leerlingen en je vraagt hen om feedback. Je controleert aan de hand van de beoordelingsnormen of je ontwerp voldoet aan de eisen van deze opdracht. (Hoofdstuk 5)



**Stap 7** Als je ontwerp klaar is, ga je een poster maken en eventueel een video of powerpoint presentatie waarin je eigenschappen van je product laat zien. Je voert een test uit van je versleuteling systeem door een kort bericht te versleutelen en aan andere leerlingen te vragen of ze je code kunnen kraken. Je schrijft hierover een korte evaluatie (Hoofdstuk 6)

**Stap 8** Je maakt een verslag (ca. 10 A4) waarin ten minste de volgende onderdelen staan:

- Titelpagina waarop de datum, jullie namen, de naam van je docent en de titel van je ontwerp
- 1. Inleiding waarin je vertelt waarom je versleutelen belangrijk vindt (ca. 1 A4)
- 2. Het onderzoek dat je gaat doen om tot het ontwerp van een geheime code te komen (ca. 2 A4)
- 3. Beschrijving van je ontwerp (ca. 2 A4)
- 4. Beschrijving van de wiskundige kennis en vaardigheden die je hebt gebruikt (ca. 1 A4)
- 5. Het resultaat van de uitvoering en testen van je ontwerp (Ca. 1-2 A4)
- 6. Hoe is het proces en de samenwerking verlopen? Hoe evalueer je zelf je ontwerp? Welke feedback heb je gekregen van je docent en je medeleerlingen? (Ca. 1 A4)
- 7. Eindconclusie, wat heb je van deze opdracht geleerd? (Ca. 1 A4)

### Hoe word je begeleid?

De begeleiding is deels op afstand via ICT hulpmiddelen zoals Padlets en video's. In de weekopdrachten wordt hiernaar verwezen.

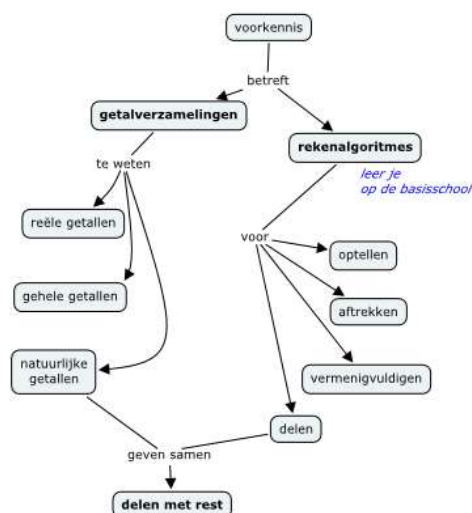
### Opdrachten per week

Om je te helpen met je onderzoek is er elke week een aantal opdrachten rond een bepaald thema. Je mag deze opdrachten allemaal maken of je mag er ook een deel van overslaan. Het doel is om een goed werkend versleuteling systeem te maken, en het maken van de vragen kan je hierbij helpen. Je mag de vragen ook maken in een andere volgorde dan dat ze hier worden aangeboden. Kortom, zolang je je einddoel maar haalt, mag je veel verschillende wegen kiezen om er te komen. Kies je eigen weg die bij jou past. De opgaven staan in een aparte opgavebundel die je download op [www.10voorwiskunde.nl](http://www.10voorwiskunde.nl)

### Week 1

*Deze week ga je beginnen met het ontdekken van nieuwe getallen. Wat zijn getallen eigenlijk en wat kun je er mee? Wat is er zo bijzonder aan priemgetallen? We gaan kennis maken met verschillende soorten van getallen. We ontdekken welke getallen bij elkaar horen en hoe grote getallen zijn opgebouwd uit kleine getallen. We duiken in de geschiedenis van getallen met enkele mooie video's. En we maken kennis met belangrijke woorden uit de cryptografie.*

In onderstaande tabel vind je hulpbronnen voor deze week.



Video		Getallen	Opgave 1.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 1.2
Artikelen			Opgave 1.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 1.4 en 1.5
Eindverslag		Hoofdstuk 1. Inleiding	Opgave 1.6

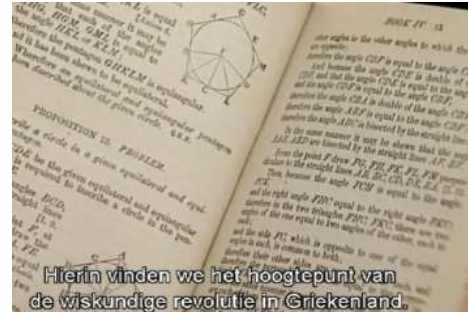
## Leerkern week 1

De leeruitkomsten van week 1 zijn dat je rekenmethodes kunt gebruiken waarmee je priemgetallen kunt ontdekken en dat je in staat bent om de grootste gemene deler en het kleinste gemene veelvoud van 2 getallen kunt berekenen

## Week 2

### Spelen met het algoritme van Euclides

Wat is eigenlijk een algoritme en wat kun je er mee? Waarom is het algoritme van Euclides ook na meer dan 2000 jaar nog steeds handig en wordt het veel gebruikt?



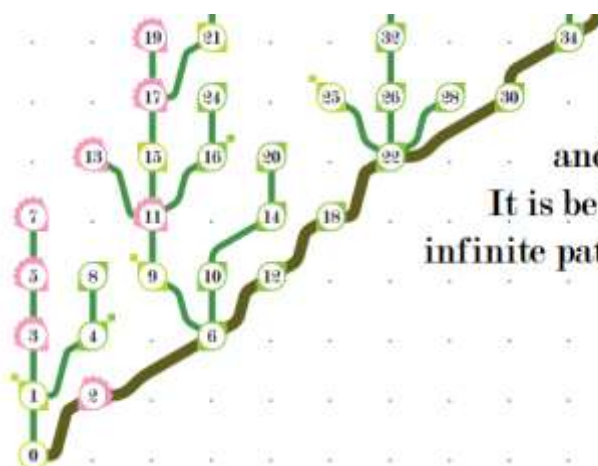
Hierin vinden we het hoogtepunt van de wiskundige revolutie in Griekenland.

Video		Euclides1 (BBC)	Opgave 2.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 2.2
Artikelen			Opgave 2.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 2.4 en 2.5
Eindverslag		Hoofdstuk 2	Opgave 2.6

## Leerkern week 2

De leeruitkomsten van week 2 zijn dat je rekenmethodes kunt gebruiken waarmee je priemgetallen kunt ontdekken en dat je in staat bent om de grootste gemene deler en het kleinste gemene veelvoud van 2 getallen kunt berekenen

Een algoritme is een methode om een probleem op te lossen. Algoritmes kunnen heel eenvoudig zijn maar ook erg ingewikkeld. Meestal bepaal je eerst je doel en zoek je daarna een methode om je doel te bereiken, je algoritme.



Subtract the number of divisors from a number in the tree, and you get the number under it. It is believed there is only one infinite path, shown in brown.

### Week 3

Wat zijn delers en hoe maak je verzamelingen? Welke toepassingen zijn er voor delers? Wat heeft modulorekenen te maken met cryptografie? Maak een eigen poster met Grote Gemene Delers.

Video		Modulo rekenen, rest bij deling	Opgave 3.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 3.2
Artikelen			Opgave 3.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 3.4 en 3.5
Eindverslag		Hoofdstuk 1. Inleiding	Opgave 3.6

#### Leerkern week 3

De leeruitkomsten van week 3 zijn dat je de verschillende delers van getallen kunt vinden. Je kunt aangeven wat het betekent als er een rest is na deling.



### Week 4

Cryptografie van Julius Ceasar, de eerste geheime oorlogscommunicatie. Hoe werkte het geheimschrift van Julius Ceasar en wat heeft dit met wiskunde te maken. Kunnen we met het gebruik van wiskunde de code kraken en een nog lastigere code produceren?

Video		cryptografie	Opgave 4.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 4.2
Artikelen			Opgave 4.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 4.4 en 4.5
Eindverslag		Hoofdstuk 4. Wiskundige kennis die nodig is	Opgave 4.6

#### Leerkern week 4

De leeruitkomsten van week 4 zijn dat je een wiskundige formule kunt vinden om eenvoudige versleutelde boodschappen te ontcijferen

## Week 5

Diophantus, Fermat, Euler en zijn indicatoren. De geschiedenis gaat verder en er komen nieuwe trucks om codes te maken en te kraken. Wie zijn de hoofdrolspelers? Wat hebben ze bijgedragen?

Video		Fermat en Euler	Opgave 5.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 5.2
Artikelen			Opgave 5.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 5.4 en 5.5
Eindverslag		Hoofdstuk 1. Inleiding	Opgave 5.6

### Leerkern week 5

De leeruitkomsten van week 5 zijn dat je rekenmethodes kunt gebruiken waarmee je priemgetallen kunt ontdekken en dat je in staat bent om de grootste gemene deler en het kleinste gemene veelvoud van 2 getallen kunt berekenen



## Week 6

Vigenère en andere systemen. In de moderne tijd gaan we computers gebruiken om de codes ingewikkelder te maken. Hoe kun je zelf een computer gebruiken om codes te maken en te kraken?

Video		Turing Enigma	Opgave 6.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 1.2
Artikelen			Opgave 1.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 1.4 en 1.5
Eindverslag		Hoofdstuk 1. Inleiding	Opgave 1.6

### Leerkern week 6

De leeruitkomsten van week 6 zijn dat je rekenmethodes kunt gebruiken waarmee je priemgetallen kunt ontdekken en dat je in staat bent om de grootste gemene deler en het kleinste gemene veelvoud van 2 getallen kunt berekenen

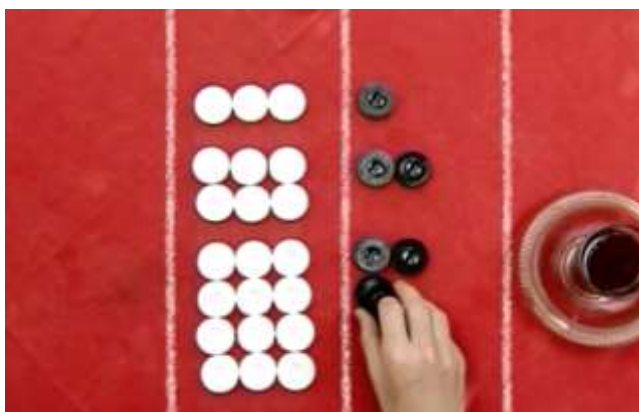
## Week 7 en 8

Hoe ga je nu je eigen cryptografisch ontwerp maken? Hoe gebruik je de wiskunde? Hoe gebruik je de geschiedenis? Hoe worden gegevens op je pinpas versleuteld?

Video		Euclides1 (BBC)	Opgave 7.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 7.2
Artikelen			Opgave 7.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 8.1 en 8.2
Eindverslag		Hoofdstuk 1. Inleiding	Opgave 8.3

### Leerkern week 7 en 8

De leeruitkomsten van week 1 zijn dat je rekenmethodes kunt gebruiken waarmee je priemgetallen kunt ontdekken en dat je in staat bent om de grootste gemene deler en het kleinste gemene veelvoud van 2 getallen kunt berekenen



## Week 9

Nu ga je je ontwerp testen, uitvoeren en presenteren. Wat zijn je ontwerp-eisen? Waar moet je systeem aan voldoen.

Video		Euclides1 (BBC)	Opgave 9.1
ICT		MCR-modulaire en cryptografische rekenmachine (TUE)	Opgave 9.2
Artikelen			Opgave 9.3
Boek(digitaal)		<a href="http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf">http://www.uitlegklas.nl/voorbeelden/basiswiskunde.pdf</a> Basis wiskunde	Opgave 9.4 en 9.5
Eindverslag		Heel het verslag afmaken en presenteren	Opgave 9.6

### Leerkern week 9

De leeruitkomsten van week 9 zijn dat je rekenmethodes kunt gebruiken waarmee je priemgetallen kunt ontdekken en dat je in staat bent om de grootste gemene deler en het kleinste gemene veelvoud van 2 getallen kunt berekenen

## **Bijlagen**

**Hoe wordt je werkstuk beoordeeld?**