

MINIMODULES VOOR 3 HAVO



Bioethanol
Complex rekenen

Cryptografie

Digitaal!
Evolutie van het oog
Forensisch onderzoek
Fractals
Grafentheorie
Navigatie
Zonne-energie

Ontwikkeld voor



Door

Jeroen Borsboom
Hans van Dijk
Arjan de Graaff
Jeroen Heilig
Peter Keeven
Nicole de Kleijn
Wim Launspach
Henk Ubbels
De Praktijk
Wessel van de Hoef

Auteurs:

*Jeroen Borsboom, PSG Jan van Egmond, Purmerend
De Praktijk, Amsterdam*

Hans van Dijk, Pieter Nieuwland College, Amsterdam

Arjan de Graaf, Bonhoeffer College, Castricum

Jeroen Heilig, Petrus Canisius College, Alkmaar

Peter Keeven, Keizer Karel College, Amstelveen

Nicole de Kleijn, Fons Vitae Lyceum, Amsterdam

Wim Launsspach, Hermann Wesselink College, Amsterdam

Henk Ubbels, Oscar Romero, Hoorn

Zonne-energie

Grafentheorie

Fractals, Digitaal!

Navigatie

Complex rekenen

Forensisch onderzoek

Cryptografie

De evolutie van het oog

Bioethanol

Eindredacteurs:

Hans van Dijk

*Pieter Nieuwland College, Amsterdam
Amstel Instituut, Amsterdam*

Wessel van de Hoef

*Fons Vitae Lyceum, Amsterdam
Amstel Instituut, Amsterdam*






Beste leerling,

Dit jaar een profiel kiezen, met nieuwe vakken?

De komende lessen maak je kennis met een stukje wiskunde dat niet in de schoolboeken staat: Cryptografie. Als je een natuurprofiel (natuur en gezondheid of natuur en techniek) kiest, krijg je misschien de gelegenheid ook het vak 'Wiskunde D' te kiezen. Cryptografie is een onderdeel dat bij wiskunde D aan de orde kan komen. Belangrijk is in ieder geval dat de manier van denken in deze lessen overeenkomt met wat er bij wiskunde D van je verwacht wordt.

In deze "minimodule" maak je kennis met een aantal geheimschriften en je leert coderen, decoderen en kraken. Je werkt in tweetallen samen, je codeert berichten voor elkaar en decodeert ze ook. Samen ga je proberen geheimschriften te kraken.

Alle minimodules hebben dezelfde opbouw, wat het werken ermee vergemakkelijkt. Je zal in de modules veel icoontjes tegenkomen. Deze icoontjes hebben de volgende betekenis:

-  : Leestekst
-  : Achtergrondinformatie
-  : Opdracht
-  : Practicumhandeling
-  : Internetopdracht

We wensen je veel plezier bij het maken van deze minimodule. Hopelijk vind je de inhoud van deze minimodule leuk en interessant genoeg om in ieder geval een natuurprofiel te kiezen en misschien wel wiskunde D.

Er is ook een bijlage aanwezig met hulptabellen, vergeet deze niet te gebruiken!
Gebruik voor het uitwerken van de opdrachten ruitjespapier.

De auteurs

Inhoudsopgave


Hoofdstuk 1	Mono-alfabetische substitutie	Blz. 5
§ 1.1	Cijfercode	Blz. 5
§ 1.2	Caesar code	Blz. 5
§ 1.3	Atbash code	Blz. 6
§ 1.4	Versleutelen met een zin	Blz. 7
Hoofdstuk 2	Poly-alfabetische substitutie	Blz. 9
§ 2.1	De Vignere methode	Blz. 9
§ 2.2	Het Vernam systeem	Blz. 13
Hoofdstuk 3	Tot slot	Blz. 13
Bijlage	Hulptabellen	Blz. 14

Studieplanner

Les	Datum	Stof	k/z ^{*1)}	Omschrijving
1		Hst. 1	k/z	Lees de tekst en doe de opdrachten in tweetallen.
2		Hst. 2	z	Lees de tekst en doe de opdrachten in tweetallen
3		Hst. 3	z	Evaluatie

*1) k = klassikaal, z = zelfstandig

Hoofdstuk 1 Mono-alfabetische substitutie

-  Een mono-alfabetische substitutie is een versleuteling waarbij elke letter in het alfabet op dezelfde manier wordt vervangen door een letter of een cijfer. We bekijken hier 4 soorten mono-alfabetische substituties.


§ 1.1 Cijfercode

-  Van dit geheimschrift heeft iedereen wel eens gehoord. Je geeft aan elke letter in het alfabet het getal mee van de positie van de letter in het alfabet. Zie de tabel hieronder:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26


Het is eenvoudig berichten om te coderen en ook om te decoderen. Deze code lichten we niet verder toe. Veel mensen hebben van deze code gehoord en daardoor is hij ook eenvoudig te kraken.

§ 1.2 Caesar code

-  Deze code werd in de Romeinse tijd door Caesar gebruikt om berichten te versturen. Om een bericht te coderen werden alle letters van het alfabet 3 plaatsen naar rechts opgeschoven. Om dan vervolgens een bericht te decoderen werden de letters weer 3 plaatsen teruggeschoven. Zie de tabel hieronder:

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Later is deze code ingewikkelder gemaakt door alle letters tegelijk een willekeurig aantal plaatsen (in plaats van 3) te laten verschuiven. Het aantal plaatsen dat verschoven wordt is dan bekend bij de zender en de ontvanger. De spaties konden worden weggelaten, de ontvanger moest die dan zelf toevoegen.

-  1) Codeer een zelf bedachte zin met behulp van Caesar code. Verschuif de letters 5 plaatsen naar rechts. Gebruik de hulptabel van de bijlage.
Mijn gewone zin:

Mijn gecodeerde zin:

- ✎ 2) Verzend de gecodeerde zin uit opdracht 1 aan je buurman/-vrouw en ontvang zijn/haar zin. De gecodeerde zin van mijn buurman/-vrouw is:

De gedecodeerde zin van mijn buurman/-vrouw is:

- 📄 Deze manier van coderen is niet erg veilig, want met een beetje proberen is er snel achter de verschuiving te komen.
- ✎ 3) Hoeveel verschuivingen moet je maximaal proberen om een Caesar code te kraken? Leg je antwoord uit.

- ✎ 4) Ontcijfer samen met je buurman/-vrouw de volgende tekst, die gecodeerd is met een willekeurige Caesar code. Gebruik hierbij de hulptabel van de bijlage.

De zin luidt: *uswksjoskvwzwwjkwjnsfzwljgewafkwjabc*

De ontcijferde zin luidt:

§ 1.3 Atbash code

- 📄 Deze code is bekend van het boek de 'Da Vinci Code' van Dan Brown. De Atbash code spiegelt de letters van het alfabet. Zie de tabel hieronder:

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Ook deze code is niet moeilijk te kraken, omdat de letters van het alfabet nog in volgorde staan. Je kunt hetzelfde te werk gaan als bij de Caesar code.

§ 1.4 Versleutelen met een zin

- ☰ Je kunt ook de letters van het alfabet vervangen met behulp van een zin. Dan wordt het alweer moeilijker om de code te kraken. Je bedenkt dan als sleutel een zin, bijvoorbeeld: 'Deze zin ga ik versleutelen.' Dan zet je de verschillende letters van deze zin achter elkaar: 'Dezingakvrslut'. Je vervangt deze letters met het begin van het alfabet en dan komt de spatie en de overige letters komen er dan in alfabetische volgorde achter. Zie de volgende versleutelingstabel:

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	Z	I	N	G	A	K	V	R	S	L	U
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	B	C	F	H	J	M	O	P	Q	W	X	Y

- ✎ 5) Codeer een zelf bedachte zin met behulp van een met je buurman/vrouw afgesproken sleutelzin. Gebruik de hulptabel van de bijlage.
Onze sleutelzin luidt:

Mijn gewone zin luidt:

Mijn gecodeerde zin luidt:

- ✎ 6) Verzend de gecodeerde zin uit opdracht 5 aan je buurman/-vrouw en ontvang zijn/haar zin.
Decodeer zijn/haar zin.
De gecodeerde zin van mijn buurman/-vrouw is:

De gedecodeerde zin van mijn buurman/-vrouw is:

- ✎ 7) Verzend één van jullie zinnen aan een ander groepje en ontvang een zin van een ander groepje. Probeer de zin te kraken zonder dat je de sleutelzin weet.
De ontvangen gecodeerde zin is:

De gedecodeerde zin is:

- De code die gecodeerd is met een zin, is moeilijk te kraken als je de sleutelzin niet weet. Ook als je weet dat een bericht is gecodeerd met behulp van een mono-alfabetische substitutie, maar je weet niet welke, is het moeilijk te kraken. Wat je dan zou kunnen doen is een frequentie-analyse. Als de gecodeerde tekst maar lang genoeg is, dan kan je tellen hoe vaak elke letter voorkomt. De letter die het meeste voorkomt zal dan waarschijnlijk de e zijn. Degene die daarna heeft meeste voorkomt de n, enzovoorts.

De volgende letters kies je dan aan de hand van de volgende frequentietabel waarin de percentages staan waarin letters voorkomen in de Nederlandse taal:

A	B	C	D	E	F	G	H	I	J	K	L	M
7,9	1,4	1,0	5,8	19,4	0,6	3,0	3,7	6,1	2,1	2,5	3,7	2,4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10,0	5,8	1,4	0,0	6,0	3,4	6,0	1,6	1,9	1,9	0,0	0,0	2,4

Deze manier van kraken kost veel tijd en het is ook een beetje proberen of er inderdaad goede zinnen uitkomen. Als de tekst een brief is, dan kan je bijvoorbeeld proberen eerst de plaatsnaam, die bovenaan de brief staat te kraken, en daarna de rest van de brief. Gelukkig kunnen computers snel de frequenties tellen en daarom wordt frequentie-analyse vaak toegepast.

Hoofdstuk 2 Poly-alfabetische substitutie

- ☰ Een poly-alfabetische substitutie is een manier van versleutelen waarbij binnen een tekst meerdere substituties voorkomen. De letter a wordt dus niet altijd naar bijvoorbeeld een n versleuteld, maar steeds naar een andere letter. We bekijken 2 soorten poly-alfabetische substitutie.

§ 2.1 De Vignere Methode

- ☰ De Vignere Methode is een variant op de Caesar code. Je versleutelt de tekst met behulp van een woord. Deze variant op de Caesar code ken je misschien van het jeugdboek Briefgeheim van Jan Terlouw. Deze variant is bedacht door Blaise de Vignere in de 16^{de} eeuw en beschreven door Giovan Battista Bellaso in 1553.

Deze variant gaat als volgt te werk. Het sleutelwoord is bijvoorbeeld het woord 'getal'. Dit sleutelwoord wordt omgezet in de bijbehorende cijfers met behulp van de volgende cijfercode: a=0, b=1, c=2, ... , z=25. Voor het woord 'getal' wordt dit dan 6 4 19 0 11. Om te coderen wordt de eerste letter uit het bericht 6 plaatsen naar rechts verschoven, de tweede letter 4, de derde 19, de vierde 0, de vijfde 11, de zesde weer 6, de zevende 4 enzovoorts. Degene die het bericht ontvangt, kent het sleutelwoord 'getal' en hoeft dus alleen maar telkens het juiste aantal plaatsen naar links te schuiven. Een hulpmiddel bij het coderen en het decoderen volgens de Vignere methode is de Vignere tabel.

Deze tabel vind je op de volgende bladzijde.

De Vignere Tabel

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Om te coderen zoek je in de bovenste rij de letter die je wilt coderen. Zoek vervolgens in de linker kolom de letter uit het sleutelwoord die je gebruikt om te coderen. Op het snijpunt van de rij en de kolom staat de gecodeerde letter.

Om te decoderen zoek je in de linkerkolom de letter uit het sleutelwoord die je gebruikt om te decoderen. Vervolgens zoek je in die rij de gecodeerde letter op. De letter bovenaan de kolom is nu de oorspronkelijke letter.

- ✎ 1) Codeer een *lang* woord met behulp van een met je buurman/-vrouw afgesproken *korte* sleutel. Onze sleutel is:

Mijn woord is:

Het gecodeerde woord is:

- ✎ 2) Verzend het gecodeerde woord uit opdracht 1 aan je buurman/-vrouw en ontvang zijn/haar woord. Decodeer zijn/haar woord met behulp van de door jullie afgesproken sleutel. Het gecodeerde woord is:

Het gedecodeerde woord is:

- 📄 Je ziet dat het coderen en decoderen veel tijd kost. Op het internet zijn verschillende programma's te vinden die het coderen en decoderen voor jou doen. Bijvoorbeeld:
 - 🔗 www.sindark.com/NonBlog/CR/CR.html
 - 🔗 www.cryptool.com
- 📄 Deze Vignere-methode werd ongeveer 300 jaar lang niet gekraakt. In 1863 bedacht Friedrich Kasiski een manier om de lengte van het sleutelwoord te achterhalen. Charles Babbage bedacht onafhankelijk van hem dezelfde methode.

§ 2.2 Het Vernam Systeem

- 📄 Het Vernam systeem is in 1917 bedacht door Gilbert Vernam. Hij bedacht dat voor elk volgend symbool in de boodschap een andere letterverschuiving wordt gehanteerd. De sleutel is hier dus net zo lang als de boodschap zelf. In de praktijk spreek je dan vaak een sleutel af die een rij voorstelt die je altijd kunt aanvullen, omdat je sleutel anders steeds afhankelijk is van de lengte van de boodschap.

Je kunt bijvoorbeeld als sleutel gebruiken de getallen 1, 3, 5, 7, De eerste letter van de boodschap schuift 1 plaats op, de tweede 3 plaatsen, de derde 5 plaatsen enzovoorts. Wat gebeurt er dan als je bent aangekomen bij 27 plaatsen opschuiven? Ja inderdaad, dat is dan weer hetzelfde als 1 plaats opschuiven. Maar dit is niet zo handig, want nu is de sleutel precies 13 getallen lang.

Dat 27 plaatsen opschuiven hetzelfde is als 1 plaats opschuiven zeggen we in wiskundige taal zo: 27 is gelijk aan 1 modulo 26.

Notatie: $27 = 1 \pmod{26}$

- ✎ 3) Bereken voor de volgende getallen de kleinste verschuiving modulo 26 waarmee ze overeenkomen:
- 33 =
 - 45 =
 - 128 =
 - 213 =
 - 534 =

- ☰ We hebben al gezien dat het niet zo handig is om de rij hierboven als sleutel te nemen. In de volgende opgave neem je de rij van priemgetallen als sleutel. Eerst geven we nog alle priemgetallen onder de vijfhonderd.

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101
 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197
 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311
 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431
 433 439 443 449 457 461 463 467 479 487 491 499

- ✎ 4) Codeer een zelf bedachte zin met behulp van de rij van priemgetallen. Laat de spaties op hun plek en let op dat de sleutel zo lang is als de boodschap.
 Mijn zin is:

Mijn gecodeerde zin:

- ✎ 5) Verzend de gecodeerde zin uit opdracht 4 aan je buurman/-vrouw en ontvang zijn/haar zin. Decodeer zijn/haar zin met behulp van de rij priemgetallen.
 Het gecodeerde woord is:

Het gedecodeerde woord is:

Hoofdstuk 3 Tot slot

- ☰ Tijdens de tweede wereldoorlog versnelden de ontwikkelingen op het gebied van cryptografie. Toen in de jaren 70 de eerste computers ontstonden, werden alle tot dan toe bestaande codes gekraakt door de rekenkracht van de computers, omdat die alle mogelijkheden konden nagaan. Er werden nieuwe methoden om te coderen en te decoderen bedacht. De bekendste daarvan zijn DES en RSA.

DES is in 1974 ontwikkeld door IBM en RSA is in 1978 ontwikkeld door de wiskundigen Rivest, Shamman en Adleman. RSA is gebaseerd op het gebruik van grote priemgetallen van wel 200 cijfers lang. Uit hoe meer cijfers de priemgetallen bestaan, hoe moeilijker het systeem te kraken is. Om RSA en DES uit te leggen heb je iets meer tijd nodig dan een paar lessen. Hopelijk hebben jullie nu een idee gekregen van cryptografie en ook van wiskunde D.

Deze lessenserie is gebaseerd op:

*Cryptologie, Maurice Alberts en Joost Langeveld, Vierkant voor wiskunde
 Masterclass cryptografie, Rene Swarttouw, Vrije Universiteit Amsterdam*

Bijlage: hulptabellen

Opdracht 1 en 2 van hoofdstuk 1

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Opdracht 4 van hoofdstuk 1

u	s	w	k	s	j	o	s	k	v	w	z	w	w	j	k	w	j	n	s	f

z	w	l	j	g	e	w	a	f	k	w	j	a	b	c

Opdracht 5 van hoofdstuk 1

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Opdracht 7 van hoofdstuk 1

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z