(c) 1997-2000 SkyLine SoftWare - Alle rechten voorbehouden.

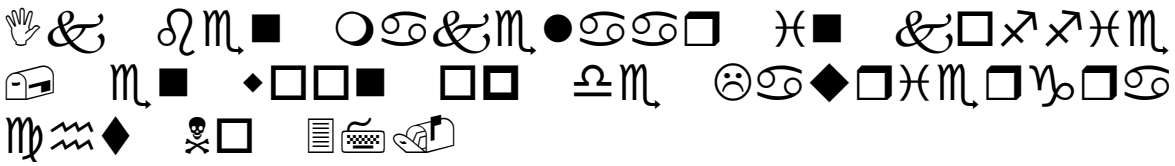
Theorie & Opdrachten

Inhoudsopgave

INHOUDSOPGAVE 3
1. GEHEIMSCHRIFTEN 4
2. CRYPTOSYSTEMEN 5
3. DOOR ELKAAR SCHUDDEN 6
4. KOLOMMEN 7
5. SUBSTITUTIE ALFABET 8
6. DELERS EN PRIEMGETALLEN 9
7. ALGORITME VAN EUCLIDES 10
8. DE GROOTST GEMEENSCHAPPELIJKE DELER 11
9. MODULO REKENEN 1 12
10. MODULO REKENEN 2 13
11. VERMENIGVULDIGEN 14
12. TOEPASSING ALGORITME VAN EUCLIDES 15
13. MACHTSVERHEFFEN 16
14. KLEINE STELLING VAN FERMAT 17
15. FUNCTIES 18
16. INVERSE FUNCTIE 19
17. EÉN OP ÉÉN FUNCTIES 20
18. DE WEG TERUG 21
19. GROTE LIJNEN 22
20. SYSTEMEN MET EEN OPENBARE SLEUTEL 23
21. ONE-WAY-FUNCTIONS 24
22. HET RSA-SYSTEEM 25
23. SLEUTELS MAKEN 26
24. SLEUTELS GEBRUIKEN 27
25. SIGNEREN 28
26. DE RSA CLUB 29
SAMENVATTING RSA-SYSTEEM 30

1. Geheimschriften

Veel mensen hebben in hun kindertijd wel eens een geheimschrift verzonnen. Je krijgt dan allerlei grappige effecten. Zoals de volgende regels:



Nu lijkt het misschien op het eerst gezicht moeilijk te ontcijferen, maar dat is het niet. Een veel gebruikte methode is om met behulp van tabellen te kijken welke letters vaak of minder vaak voorkomen. Voor de Nederlandse taal kun je de volgende tabel gebruiken:

Letterfrequenties per 10.000											
e	1586	d	512	h	232	f	123	.	76	:	4
spatie	1425	o	482	v	223	c	123	f	70	x	3
n	858	i	467	m	188	b	119	j	25	‘	2
a	633	s	351	k	187	z	116	-	10	?	2
t	556	l	310	u	159	ij	107	y	8	g	1
r	542	g	282	w	130	,	82	;	4		

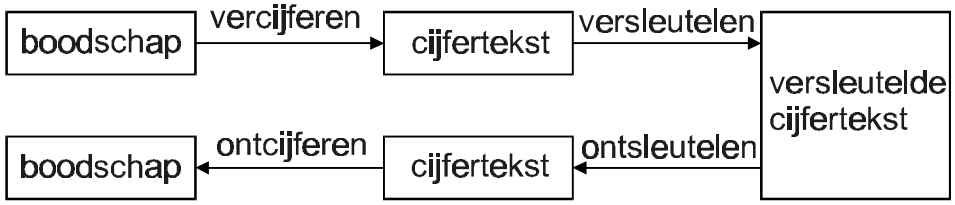
Naast de letterfrequenties zou je ook gebruik kunnen maken van de frequenties van tweetallen van letters of zelfs drietallen. Bovendien kun je kijken naar woorden die in de Nederlandse taal veel voorkomen.

Opdracht 1
Het valt niet mee om de regels hierboven met behulp van alleen de tabel te ontcijferen. Dit komt omdat je eigenlijk te weinig tekst hebt. Maar een paar letters kun je er toch wel uithalen.
Welk symbooltje wordt gebruikt voor de letter '**e**' ?
En welk symbooltje zal waarschijnlijk de letter '**n**' zijn ?

2. Cryptosystemen

In deze serie lessen hanteren we het volgende systeem. Let goed op de verschillende begrippen, want je zult ze in de volgende bladzijden zeer vaak tegenkomen.

Wij gaan uit van het volgende schema:



Het bovenste gedeelte van het schema betreft de zender. Dit is iemand die een geheime boodschap aan een ontvanger wil versturen. De ontvanger staat in het onderste gedeelte van het schema.

De zender:

In principe wordt een **boodschap** eerst vercijferd. Dit betekent dat men aan letters cijfers toekent. Dit levert de cijfertekst op. Met deze cijfertekst kun je wiskundig aan de slag. Met getallen kun je immers rekenen. Dit levert de **versleutelde cijfertekst** op.

De ontvanger:

De ontvanger moet eerst de **versleutelde cijfertekst** proberen te **ontsleutelen**. Dit levert weer de cijfertekst op. Deze kan dan worden omgezet in letters, zodat de **boodschap** weer leesbaar wordt.

De spion of kraker:

De spion of kraker is natuurlijk geïnteresseerd in het **ontsleutelen** van de boodschap. Maar ook in het **versleutelen**. Met behulp van die kennis kan hij of zij allerlei **valse boodschappen** de wereld in sturen.

Wij gaan ons vooral bezig houden met de verschillende aspecten van dit soort systemen. We beginnen met een paar 'eenvoudige' geheimschriften. Gaandeweg wordt duidelijk dat we wel een paar wiskundige technieken nodig hebben om zo'n geheimschrift nog een beetje moeilijk te maken. We eindigen met het zeer geavanceerde RSA-systeem. Het RSA is een cryptosysteem dat zeer veel gebruikt wordt.

3. Door elkaar schudden

Een klassieke manier om een tekst te versleutelen, zonder gebruik te maken van **cijfertekst**, is het door elkaar schudden van de letters. Bij deze methode verandert men de volgorde van de letters in plaats van de letters zelf. Een voordeel is dat een frequentieonderzoek, zoals we gedaan hebben op bij opdracht 1, niet veel zin heeft.

Kies een route
Laten we als voorbeeld de tekst "*Kom morgen niet op de afgesproken plaats!*" nemen. Deze zin bestaat uit 35 letters. Deze zin zetten we in een rechthoek van 5x7:

k	o	m	m	o
r	g	e	n	n
i	e	t	o	p
d	e	a	f	g
e	s	p	r	o
k	e	n	p	l
a	a	t	s	!

Vervolgens kiezen we de letters er in een andere volgorde uit. Volgens één of ander systeem. Je zou bijvoorbeeld links onderaan kunnen beginnen dan naar boven, naar rechts, naar beneden, weer naar rechts, weer naar boven, enzovoort.
De versleutelde zin wordt dan:

akedi rkoge eseat npate mmnof rps!l ogpno

Maar het kan ook anders:

Opdracht 2
Uit de tabel hierboven halen we de volgende versleutelde zin:

!lstp ogrna aepfp noask eetno meedi gmork

a. Wat is de sleutel die we gebruikt hebben?
b. Gebruik deze sleutel om het volgende bericht te ontcijferen:

!o!ym mdeen rneos

c. Stel je wilt dit gebruiken om met iemand te communiceren. Welk onderdeel van dit eenvoudige cryptosysteem moet je per se geheimhouden voor anderen mensen?
Hoe moet je die andere duidelijk maken welke sleutel je wilt gebruiken?
Bedenk dat je altijd afgeluisterd kan worden en dat je niet weet of iemand je bericht misschien onderschept

4. Kolommen

Bij deze methode wordt de originele tekst eerst in een rechthoek gezet. Vervolgens neem je de letters er volgens kolommen van boven naar beneden uit. De volgorde van de kolommen wordt bepaald door een sleutel.
Meestal kiest men als sleutel een woord, waarbij de alfabetische volgorde van de letters uit het sleutelwoord de volgorde bepaalt.

Nemen we de zin "*kom om zeven uur naar Zwolle!*".
Deze zin bestaat uit 24 letters.
We zetten de letters in een 4x6 rechthoek, dus moeten een sleutelwoord van zes letters kiezen, bijvoorbeeld **tafels**.

sleutelwoord	**t**	**a**	**f**	**e**	**l**	**s**
volgorde	**6**	**1**	**3**	**2**	**4**	**5**
bericht	k	o	m	o	m	z
	e	v	e	n	u	u
	r	n	a	a	r	z
	w	o	l	l	e	!

Het versleutelde bericht ziet er dan zo uit:

ovno onal meal mure zuz! kerw

Het aantal verschillende versleutelde berichten dat je zo kunt maken is 6! = 720.
Je kunt echter niet weten welk formaat rechthoek is gebruikt.
In totaal zijn er 8, namelijk: 1x24, 2x12, 3x8, 4x6, 6x4, 8x3, 12x2 en 24x1
Bij 1x24 zou je een sleutelwoord moeten verzinnen van 24 letters! En bij 24x1 heb je maar één volgorde en dat lijkt me niet de bedoeling!
Ook een woord vinden van twaalf letters (alle letters maar één keer) is lastig! Dus 2x12 valt ook af.
De rest is in principe mogelijk.
Totaal zijn er 8!+6!+4!+3!+2! = 41.072 verschillende mogelijkheden.

Opdracht 3
Je ontvangt het volgende bericht:

iiene ekerg tmame

a. Op hoeveel verschillende manieren kan dit bericht (volgens bovenstaande methode) versleuteld zijn?
b. Het sleutelwoord is "douwe". Ontcijfer het bericht.
c. De titel van dit lespakket is **coett!rsmyyepsn**. Hoe komen we daar aan?

5. Substitutie alfabet

Bij een substitutiemethode wordt elke letter vervangen door een andere letter. Zo'n nieuw alfabet wordt wel **substitutie alfabet** genoemd.
Het 'kraken' van zo'n substitutiemethode is niet zo heel moeilijk. In plaats van één letter kun je ook twee letters of lettergrepen vervangen. Hierdoor wordt het 'kraken' van het geheimschrift iets moeilijker.

Julius Caesar methode
Een methode die in het Romeinse Rijk werd toegepast is het verschoven alfabet. Het vermoeden bestaat dat Julius Caesar zelf de ontwerper van dit geheimschrift is.

Voorbeeld:

ORIGINEEL	**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**
VERTALING	**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**

Op deze manier kun je maar 26 verschillende substitutie-alfabetten maken en deze methode is dus erg makkelijk te kraken. Als je één letter kent, weet je al hoe het zit.

Opdracht 4
Geef de originele tekst van deze geheime boodschap. (zie studiewijzer voor handige strookjes.)

no ukd jsd sx no lyyw

Opdracht 5
In de film "*2001, A Space Odyssey*" van *Stanley Kubrick* komt een computer voor met de naam '**HAL**'. Deze naam is een versleutelde naam van iets anders. Welke naam wordt er bedoeld ?

Je kunt voor de Caesar methode heel handig een **functievoorschrift** verzinnen. Je kent aan elke letter een getal toe. We noemen dit getal het **rangnummer**. De letter **A** krijgt rangnummer **0**, **B** rangnummer **1**, enzovoort. Met die rangnummers kun je gaan rekenen. De uitkomst van die berekening kun je opvatten als het rangnummer van het teken in het geheimschrift.

Voorbeeld:

ORIGINEEL	**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**
VERTALING	**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**

Bij **A** tot en **P** kun je bij het rangnummer steeds 10 optellen. Bij **Q** krijg je echter een probleem. **Q** heeft als rangnummer 16 en wordt 26. Omdat er maar 26 letters zijn, trek je hier 26 van af. Je krijgt dan 0, dus **Q** wordt **A**.

6. Delers en priemgetallen

Delers
Een geheel getal *b* heet een **deler** van a als er een ander geheel getal *c* bestaat zodat $a = b \cdot c$
Zo heeft 24 de delers: 1, 2, 3, 4, 6, 8, 12, 24.
Je kunt ook zeggen: *b* is een deler van *a*, als je *a* kunt delen door *b* zonder rest.
We praten in het vervolg alleen over **positieve** delers.

Opdracht 6
Waarom is het getal 0 geen deler van 24 ?

Een handige manier om alle delers van een getal te vinden is met behulp van een tabel als hiernaast.

De delers van 24 zijn: 1, 2, 3, 4, 6, 8, 12 en 24.

de delers van 24
1 x 24
2 x 12
3 x 8
4 x 6
klaar!

Opdracht 7
Geef de delers van:
a. 360 **b.** 1001 **c.** 1024 **d.** 17

Priemgetallen
Een priemgetal heeft geen echte delers. Omdat je een priemgetal alleen kunt delen door 1 en het getal zelf kun je priemgetallen opvatten als een soort bouwstenen.

De '**Hoofdstelling**' van de getaltheorie:

- **Elk positief geheel getal is op precies één manier als product van priemgetallen te schrijven**

In de *Disquisitiones arithmeticae*, het boek waarmee **Carl Friedrich Gauss** (1777-1855) in 1801 de moderne getaltheorie inluidde, is de hoofdstelling voor het eerst duidelijk geformuleerd en bewezen.

Voorbeelden:
$9191 = 7 \cdot 13 \cdot 101$
$2178540 = 22 \cdot 32 \cdot 5 \cdot 72 \cdot 13 \cdot 19$
$100895598169 = 112303 \cdot 898423$

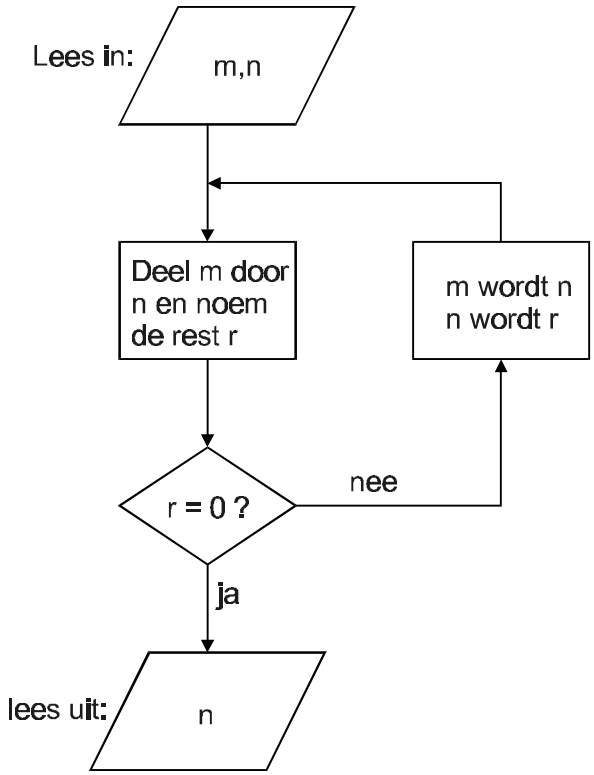
Een getal als **17** kun je niet schrijven als het product van twee (of meer) andere getallen.
Het getal **76534343653674768478 91** ook niet.
De vraag is natuurlijk: hoe kun je dat zeker weten?
Als je zou proberen alle delers op te schrijven, zoals je gedaan hebt op de vorige bladzijde zou dat lang duren: Is het deelbaar door 2? Door 3? 5 misschien? En 7? en...

Het probleem om een gegeven getal in priemfactoren te ontbinden wordt vaak in twee deelproblemen gesplitst. Gelukkig blijkt dat je met behulp van zogenaamde priemtests relatief makkelijk kan bepalen of een getal een priemgetal is. Veel moeilijker is om bij een groot getal de **ontbinding in priemgetallen** zelf te vinden.

Opdracht 8
Geef de priemontbinding van 1001 en 6378.

7. Algoritme van Euclides

Hieronder zie je het **stroomschema** dat hoort bij het **Algoritme van Euclides**.



m en n zijn twee natuurlijke getallen, waarbij m > n

Voorbeeld:
Je begint met: **m = 24 en n =15 dan r = 9**
Na één stap krijg je: **m = 15 en n = 9 dan r = 6**
Na de tweede stap: **m = 9 en n = 6 dan r = 3**
Een stap later: **m = 6 en n = 3 dan r = 0**
Nu is **r** gelijk aan 0, het algoritme stopt. **n** heeft de waarde 3.

Opdracht 9

a. Pas het algoritme toe op onderstaande voorbeelden:
   i. m = 35 en n = 15
   ii. m = 100 en n = 36
   iii. m 31 en n = 4

b. Wat berekent het algoritme bij twee gegeven getallen ?

8. De grootst gemeenschappelijke deler

Als je van twee getallen de delers vergelijkt kunnen ze best sommige delers gemeenschappelijk hebben.

Voorbeeld:
De delers van 30 zijn: 1, 2, 3, 5, 6, 10, 15 en 30.
De delers van 48 zijn: 1, 2, 3, 4, 6, 8, 12, 16, 24 en 48.
De grootst gemeenschappelijke deler is 6. We noteren dat als: ggd(30,48)=6
Met behulp van het **algoritme van Euclides** (zie vorige bladzijde) kun je de **g.g.d.** van twee getallen bepalen.

Opdracht 10
a. Vereenvoudig de breuk 60/96.
b. Bereken ggd(60,96).
c. Wat heeft ggd(60,96) te maken met vereenvoudigen van de breuk bij a. ?

Relatief priem
Het kan voor komen dat twee getallen, zeg *a* en *b* een g.g.d. hebben van 1. Dat wil niet zeggen dat de getallen zelf priemgetallen zijn, het betekent alleen dat deze twee getallen geen gemeenschappelijke delers hebben.
Twee getallen *a* en *b* waarvoor geldt **ggd (*a*,*b*)=1** noemen we **relatief priem**.

Opdracht 11
Welke van de volgende paren getallen zijn **relatief priem** ?

a	b	relatief priem ?
40	78	ja / nee
256	243	ja / nee
100	45	ja / nee
6	21	ja / nee
1001	1002	ja / nee
44	111111	ja / nee

9. Modulo rekenen 1

Modulo rekenen is rekenen met weinig getallen. 'Normaal' zijn er oneindig veel natuurlijke getallen. Als je alleen kijkt naar bijvoorbeeld '**de rest bij delen door 3**' zijn er voor elk willekeurig getal maar 3 mogelijkheden:

1. De rest bij delen door 3 is 0. (Het getal is deelbaar door 3.)
2. De rest bij delen door 3 is 1.
3. De rest bij delen door 3 is 2.

Andere mogelijkheden zijn er niet. Het aardige is nu dat je met deze resten kun je gewoon rekenen.

Voorbeeld:
Je zit op een test en je moet de volgende vraag beantwoorden:

Is de oppervlakte van een rechthoek van 123 cm bij 234 cm

A. 28781 cm^2
B. 28782 cm^2
C. 28783 cm^2

Als het goed is kun je het zo zien! Namelijk als je alleen naar de laatste cijfers kijkt. $3 \times 4 = 12$. Dus het antwoord moet eindigen op een 2.
In feite reken je dan met resten van 10, we zeggen dan dat je rekent **modulo 10**.
123 = 3 modulo 10 en 234 = 4 modulo 10.
$3 \times 4 = 12 = 2$ (modulo 10)
Conclusie: antwoord **B** is het juiste antwoord.

Het (merkw)aardige is dat allerlei regels, die voor 'normaal' rekenen gelden, nog steeds gelden:

$25 + 38 = 63$
25 = 1 (modulo 3), 38 = 2 (modulo 3) en 63 = 0 (modulo 3)
Er geldt: 1 + 2 = 0 (modulo 3)

$14 \cdot 89 = 1246$
14 = 2 (modulo 3), 89 = 2 (modulo 3) en 1246 = 1 (modulo 3)
$2 \cdot 2 = 4 = 1$ (modulo 3)

$5^3 = 125$
5 = 2 (modulo 3) en 125 = 2 (modulo 3)
$2^3 = 8 = 2$ (modulo 3)

Je kunt deze eigenschappen bijvoorbeeld gebruiken om snel antwoorden te controleren.

Voorbeeld:
Is $12^9 = 5159780351$?
Antwoord: **nee!**
Uitleg: 12 = 0 (modulo3) en 5159780351 = 2 (modulo 3),
terwijl $0^9 = \mathbf{0} \neq 2$ (modulo 3)

10. Modulo rekenen 2

Voorbeeld:
Iemand vertrekt om 09.00 uur vanuit Nijmegen naar Italië. Ongeveer 14 uur later is zij in Basel, Zwitserland. Daar wordt 8 uur geslapen. Dan is het nog 9 uur naar de uiteindelijke bestemming.
Hoe laat komt zij aan?
Een mogelijke aanpak is:
9 + 14 + 8 + 9 = 40 = ...
of:
9 + (-10) + 8 + 9 = -1 + 17 = 16

Opdracht 12
Bereken op de tweede manier de aankomsttijd van een reis die begint om 10 uur en die uit een vliegreis van 21 uur bestaat, een bustocht van 14 uur en een voettocht van 74 uur.

Modulo rekenen
In het algemeen geldt:

$$a = b \pmod m \text{ als } a = b + k \cdot m$$

Voorbeeld:
$5 = 2 \pmod 3$ want $5 = 2 + 1 \cdot 3$
$7 + 9 = 1 + 0 = 1 \pmod 3$
$35 + 67 = 2 + 1 = 0 \pmod 3$

Voorbeeld:
$10 \pmod 9 = 1$
$100 \pmod 9 = 1$
$1000 \pmod 9 = 1$
enz....
$3287 = 3 \cdot 1000 + 2 \cdot 100 + 8 \cdot 10 + 7 \cdot 1 = 3 \cdot 1 + 2 \cdot 1 + 8 \cdot 1 + 7 \cdot 1 \text{ (modulo 9)}$
dus $3287 = 3 + 2 + 8 + 7 = 20 = 2 \text{ (modulo 9)}$
Uit bovenstaande blijkt dat, als een getal deelbaar is door 9, de som van de cijfers ook deelbaar door 9 moet zijn.

Opdracht 13
a. Is 1234 deelbaar door 9 ?
b. Is 1238983898919838819999 deelbaar door 9 ?
c. Is $1234 \times 8972 = 11072448$?
d. En is $12345 \times 54321 = 671492745$?

11. Vermenigvuldigen

Zoals gezegd kun je ook bij het **modulo** rekenen dezelfde bewerking uitvoeren als bij 'normaal' rekenen. Je kunt optellen, vermenigvuldigen en machtsverheffen.

Voorbeeld:
Neem aan dat we rekenen in **modulo 7**.
Hieronder staat de vermenigvuldigingstabel:

·	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Meer verschillende vermenigvuldigingen zijn er niet.

Twee eigenschappen:
1. De tabel is symmetrisch.
2. De getallen (0 t/m 6) komen precies één keer voor in elke rij en in elke kolom, met uitzondering van de rij en kolom van nul.

Opdracht 14
Je kunt met de tabel van modulo 7 ook gebruiken om terug te rekenen.
a. Met welk getal moet je 5 vermenigvuldigen om 3 (modulo 7) te krijgen ?
b. Met welk getal moet je 4 vermenigvuldigen om 3 (modulo 7) te krijgen ?

Geef de vermenigvuldigingstabel van modulo 6.

c. Kloppen bovengenoemde eigenschappen hier ?
d. Met welk getal moet je 5 vermenigvuldigen om 3 (modulo 6) te krijgen ?
e. Met welk getal moet je 4 vermenigvuldigen om 3 (modulo 6) te krijgen ?
f. Wat valt je op ? Hoe komt dat ?

12. Toepassing algoritme van Euclides

Voorbeeld:
Je hebt twee getallen, bijvoorbeeld 7 en 32.
Voor welke waarde van *a* geldt dat $a \cdot 7 = 1 \pmod{32}$

Om dit probleem op te lossen zou je een vermenigvuldigingstabel van modulo 32 kunnen maken. Handiger is om alle mogelijkheden waarbij je vermenigvuldigt met 7 'even' uit te rekenen. Je krijgt dan:

	…	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**…**
7	…	28	3	10	17	24	31	6	13	20	…

Je kunt hier dan mee door gaan tot je ergens 1 krijgt. Maar het kan ook anders:

We zoeken een *a* en een *b* zodat geldt: $a \cdot 7 + b \cdot 32 = 1$
Immers omdat we modulo 32 rekenen mag die 1 ook gerust 33 zijn, of 161.

We gaan uit van dit stelsel:
$0 \cdot 7 + 1 \cdot 32 = 32$ (1)
$1 \cdot 7 + 0 \cdot 32 = 7$

Zoals je ziet staat daar nog niets bijzonders. Wat we vervolgens gaan proberen is om aan de rechterkant van het =-teken een 1 te krijgen door de vergelijkingen op een slimme manier te combineren:
Van stelsel (1) maken we het volgende stelsel:
$0 \cdot 7 + 1 \cdot 32 = 32$ (2)
$4 \cdot 7 + 0 \cdot 32 = 28$
Waarbij de tweede regel uit (1) is vermenigvuldigd met 4. Vervolgens trekken we de tweede regel van (2) van de eerste af. Dan krijgen we:
$-4 \cdot 7 + 1 \cdot 32 = 4$ (3)
Om de 4 rechts van het =-teken nog kleiner te krijgen (er moet immers 1 uitkomen, want ggd(7,32) = 1) halen we (3) van de 2e regel van (1) af. Dan komt er te staan:
$5 \cdot 7 - 1 \cdot 32 = 3$ (4)
Nu zijn we er bijna. Namelijk: (3) - (4) levert:
$-9 \cdot 7 + 2 \cdot 32 = 1$ (5)

Hier staat de oplossing van ons probleem. Want regel (5) levert:
$-9 \cdot 7 = 1 - 2 \cdot 32$
Dat is vertaald naar het modulo-rekenen: $-9 \cdot 7 = 1 \pmod{32}$

Conclusie: $a = 23$. Dit noemen we de inverse van 7 (mod 32).
Inderdaad geldt: $7 \cdot 23 = 1 \pmod{32}$

Opdracht 15
Bepaal de inverse van 301 (mod 577)

13. Machtsverheffen

Niet alleen gaat vermenigvuldigen sneller dan normaal, ook machtsverheffen is veel sneller. Als bijvoorbeeld wordt gevraagd uit te rekenen 5^8 (mod 4), dan kun je net zo goed uitrekenen 1^8 (mod 4)
En dat klopt: $5^8 = 390625$ en dat is precies $97656 \cdot 4 + 1$,
kortom 5^8 (mod 4) = 1^8 (mod 4) = 1 (mod 4)

Opdracht 16
Controleer onderstaand voorbeeld met je rekenmachine.

3^{15} (mod 6) = $(3^3)^5$ (mod 6)
= 27^5 (mod 6)
= 3^5 (mod 6)
= $9 \cdot 9 \cdot 3$ (mod 6)
= $3 \cdot 3 \cdot 3$ (mod 6)
= 3 (mod 6)

Voorbeeld:
Hoe bereken je 2^{26} (mod 23) ?

Aanpak:
Schrijf de exponent 26 als 2 + 8 + 16
Elke getal is te schrijven als som van getallen uit de rij:
1, 2, 4, 8, 16, ..
Het gemakkelijkst doe je dat door eerst het grootst mogelijke getal te gebruiken en vervolgens het verschil met kleinere getallen op te vullen.
Van deze machten kun je eenvoudig de resten bepalen.

$2^2 = 4$ (mod 23)
$2^4 = 16$ (mod 23)
$2^8 = 2^4 \cdot 2^4 = 16 \cdot 16 = -7 \cdot -7$ (mod 23) = 49 (mod 23) = 3 (mod 23)
$2^{16} = 2^8 \cdot 2^8 = 3 \cdot 3$ (mod 23) = 9 (mod 23)

Zodat we nu kunnen schrijven: $2^{26} = 4 \cdot 3 \cdot 9$ (mod 23)
= 108 (mod 23)
= 16 (mod 23)
Controle: $2^{26} = 67108864 = 16 + 2917776 \cdot 23$

Opdracht 17
Bereken: 3^{37} (mod 11)

14. Kleine stelling van Fermat

Je hebt gezien dat je voor een vergelijking als $7 \cdot x = 1 \pmod{26}$ een oplossing kunt vinden met het **algoritme van Euclides**.

Hoe zou je nu de waarde van x kunnen vinden als bijvoorbeeld geldt:

$3^x = 1 \pmod 7$

Het gaat in dit bestek ook te ver om volledig duidelijk te maken wat de achtergronden zijn van het resultaat waar we nu gebruik van gaan maken.
De stelling noemt men: **De kleine stelling van Fermat**.
(Er bestaat inderdaad ook een grote versie.)

De Kleine stelling van Fermat:

$a^p - 1 = 1 \pmod p$ (p is een priemgetal)

Als we dat narekenen voor de vergelijking

$3^x = 1 \pmod 7$

zou dus het getal 6 aan de vergelijking voldoen.

Controlerend:

$3^6 = 729 = 104 \cdot 7 + 1$ klopt!

Opdracht 18
Wat is waarde van *x* als
i. $5^x = 1 \pmod{13}$
ii. $12^x = 1 \pmod{1009}$
Kun je bovenstaande stelling ook gebruiken om $6^x = 1 \pmod{100}$ op te lossen?

15. Functies

Wiskundig gezien komt het voorbeeld van het eerder genoemde 'verschoven alfabet' neer op de functie:

f(*x*) = (*x* + *b*) mod 26

Hierbij is **x** dus het rangnummer van de originele letter en **f(*x*)** is het rangnummer van de letter voor het geheimschrift. Het getal ***b*** geeft de verschuiving aan.
De mod is de modulus-functie. Deze functie berekent de rest bij deling door 26.

Voorbeeld:
In ons voorbeeld was ***b*** gelijk aan 10.
Het functievoorschrift wordt: f (*x*) = (*x* + 10) mod 26

De substitutie-letter van '**t**' kun je zo uitrekenen:

vercijferen		*+10*		*mod 26*		*ontcijferen*		
t	→	**19**	→	**29**	→	**3**	→	**d**

Dus de letter '**t**' wordt in ons geheimschrift de letter '**d**'.

Opdracht 19
We kiezen voor ***b*** nu het getal 19. (zie studiewijzer voor handige strookjes)
Bereken f (12), f (20) en f (6).

Opdracht 20
We kiezen voor ***b*** weer 19. (zie studiewijzer voor handige strookjes)
Wat betekent dan deze geheime boodschap:
bd shn axm gbxm pxmxg

16. Inverse functie

Normaal gesproken berekent een functie bij een **origineel** het **beeld**. Een **inverse** functie doet precies het omgekeerde: de **inverse** functie berekent bij het beeld het origineel. Niet alle functies hebben een inverse. Vaak heeft een functie hetzelfde beeld bij verschillende originelen. Ook kan het voorkomen dat een functie wel een inverse heeft, maar dat je die functie niet zomaar even opschrijft. In je wiskundeboek kun je meer vinden over functies en inverse functies.

De inverse functie van f(*x*) = (*x* + *b*) mod 26
De inverse functie van f(*x*) = (*x* + *b*) mod 26 is de functie $f^{-1}(x) = (x - b) \bmod 26$.
En dat is wel heel mooi!
Kijken of het klopt: we weten al: het 'beeld' van '**t**' is '**d**'.

	vercijferen		*-10*		*mod 26*		*ontcijferen*	
d	→	**3**	→	**-7**	→	**19**	→	**t**

Het is mogelijk de Caesar substitutie aanzienlijk te verbeteren door aan het functievoorschrift een tweede coëfficiënt toe te voegen.

f(*x*) = (*a*x + *b*) mod 26

Nu is het alleen zo, dat je ***a*** niet willekeurig kan kiezen. Het heeft te maken met het feit dat bij deze functie elk beeld maar één origineel mag hebben.

Opdracht 21
Leg uit dat bij een vertaling met behulp van een of andere functie elk beeld maar één origineel mag hebben. Wat gaat er mis als dat niet zo is ?

17. Eén op één functies

We nemen als voorbeeld een substitutie met als functie:

f(*x*) = (2*x* + 1) mod 26

We rekenen voor alle letters 'even' de sleutelletters uit:

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**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	3	5	7	9	11	13	15	17	19	21	23	25	1	3	5	7	9	11	13	15	17	19	21	23	25
B	**D**	**F**	**H**	**J**	**L**	**N**	**P**	**R**	**T**	**V**	**X**	**Z**	**B**	**D**	**F**	**H**	**J**	**L**	**N**	**P**	**R**	**T**	**V**	**X**	**Z**

En dat kan natuurlijk helemaal niet. Als er in de geheime boodschap bijvoorbeeld een **P** staat was dat in de originele tekst dan een **H** of was het **U** ?

Uiteindelijk blijkt zo'n omzetting alleen maar zinvol als ***a*** en **26** geen delers gemeen hebben. Oftewel ***a*** en **26** moeten relatief priem zijn. Of ook ggd(*a*, 26) = 1. Dus voor *a* kun je bijvoorbeeld wel 3, 5, 7, 9, 11, enzovoort kiezen.

Opdracht 22
Hierboven staat 'enzovoort'. Maak het rijtje af.
Hoeveel verschillende keuzes zijn er voor *a* ?
Hoeveel verschillende keuzes zijn er voor *b* ?
Hoeveel verschillende keuzes zijn er in totaal ?

De inverse functie van f(*x*) = (*ax* + *b*) mod 26

Laten we voor de functie maar eens f(*x*) = (7*x* + 10) mod 26 nemen.
De vraag is nu: "**Wat is de inverse functie van f(*x*) ?**"

Om die vraag te kunnen beantwoorden zou je eerst naar de inverse moeten kijken van vermenigvuldigen met 7 (modulo 26).
Als je 1 met 7 vermenigvuldigt krijg je 7 (modulo 26).
Waarmee moet je nu 7 (modulo 26) vermenigvuldigen om weer 1 (modulo 26) te krijgen ?
Anders geformuleerd, de **inverse** van **7** (modulo 26) blijkt **15** te zijn.... (ga na !!!)
Kennelijk is de inverse functie van vermenigvuldigen met 7, vermenigvuldigen met 15.

Dus de inverse functie van f is **$f^{-1}(x) = (15(x - 10)) \bmod 26$**

Opdracht 23
Laat zien dat **(15(*x* - 10)) mod 26 = (15*x* + 6) mod 26**

18. De weg terug

Voorbeeld:
$f(x) = (7x + 10) \bmod 26$ en $f^{-1}(x) = (15x + 6)) \bmod 26$

W → 22 → 154 → 164 → 8 → I

Nu terug:

I → 8 → 126 → 22 → W

Het lijkt allemaal ingewikkeld. Toch blijkt de ontcijfering van een geheimschrift waarbij men gebruik maakt van deze methode in het algemeen redelijk eenvoudig te 'kraken'.
Vaak voegt men aan het alfabet drie leestekens toe.
Hierdoor heeft men de beschikking over meer sleutels, omdat men nu voor *a* alle getallen mag kiezen (modulo 29). Immers *a* mocht geen gemeenschappelijke delers hebben met 29, maar 29 is een priemgetal....

Voorbeeld:
Uit een frequentieonderzoek blijkt dat de letter **U** het meest voorkomt en daarna de letter **R**.
Je neemt in eerste instantie aan dat **U** het beeld is van **E** en dat **R** het beeld is van **S**.
Als je gebruik maakt van 29 lettertekens dan geldt:

$20 = (a \cdot 4 + b) \bmod 29$
$17 = (a \cdot 18 + b) \bmod 29$
Aftrekken levert: $-3 = (a \cdot 14) \bmod 29 = 26 = (a \cdot 14) \bmod 29$
De inverse van 14 (mod 29) is 27. Dus moet $a = 27 \cdot 26 = 6 \pmod{29}$
Het blijkt dat $a = 6$, invullen levert $b = 25$. (Ga na!!!)

Je vindt $f(x) = (6x + 25) \bmod 29$ en $f^{-1}(x) = (5 \cdot (x + 4)) \bmod 29$

Als je f^{-1} toepast op de geheime boodschap zal blijken of het uitgangspunt (U = E en R = S) terecht was of niet.

Opdracht 24
Je ontvang de volgende tekst:

rmxgemsglxx,sgm,gdxv

Je vermoedt dat hier gebruik gemaakt is van bovenstaande substitutiemethode met 29 lettertekens.
Bepaal door frequentieanalyse wat (vermoedelijk) het beeld is van **e** en de **spatie**.
Bepaal de waarde van *a* en *b*.
Ontcijfer **bovenstaande** boodschap.

19. Grote lijnen

We hebben nu voorbeelden gezien van eenvoudige geheimschriften. We spreken meestal van cryptosystemen. In al deze systemen spelen begrippen als vercijferen, versleutelen, ontsleutelen, e.d. een belangrijke rol.
De eenvoudige cryptosystemen hadden een belangrijk nadeel: ze zijn relatief eenvoudig te kraken. Vooral als je gebruik mag maken van geavanceerde computerprogramma's is het kraken van de meeste eenvoudige geheimschriften geen enkel probleem.

Voorbeeld:
Bij een substitutie-alfabet met 29 karakters zijn er heel wat verschillende functies te bedenken. Met een computerprogramma zou je natuurlijk alle mogelijkheden uit kunnen gaan proberen. Meestal gebruikt men hiervoor woordherkenningsprogramma's. De Nederlandse taal bestaat nu eenmaal voor een groot gedeelte uit de, het en een.

Vrijwel alle klassieke cryptosystemen zijn door computers gekraakt, maar de computer maakte het ook mogelijk geheel nieuwe ideeën en technieken uit de zuivere wiskunde toe te passen voor cryptografische doeleinden.
Het 'domme' werk kun je een computer laten doen. Heel verrassend is dat met name de getaltheorie daarbij zo'n prominente rol speelt. De allergrootste wiskundigen zoals Fermat, Euler, Gauss en Hilbert hebben zich met getaltheorie beziggehouden. Getaltheorie wordt ook wel de 'koningin van de wiskunde' genoemd.

Het meest bekend geworden cryptosysteem dat nu nog steeds gebruikt wordt is RSA, dat gebruik maakt van een hele mooie eigenschap van grote getallen:
Het is zeer moeilijk om bij een gegeven product van twee grote priemgetallen deze twee priemgetallen te vinden.....

Eind jaren zeventig daagde Rivest, één van de uitvinders van RSA, de wereld uit RSA-129 te kraken. Hij schatte dat het met de toenmalige middelen 1015 jaar zou duren! Nog geen 17 jaar later nam dit slechts 8 maanden in beslag.

20. Systemen met een openbare sleutel

In een openbaar sleutelsysteem is steeds sprake van twee sleutels: één sleutel voor het versleutelen en één sleutel voor het ontsleutelen. Het gaat daarbij om het omzetten van cijferteksten in andere cijferteksten. De ontvanger moet de originele cijfertekst weer terug zien te krijgen met een sleutel.

De sleutel waarmee de cijfertekst versleuteld wordt is in principe openbaar. Iedereen kan ervan kennis nemen en het gebruiken voor het versleutelen van een cijfertekst. Het basisidee van openbare-sleutelsystemen bestaat hierin, dat weliswaar iedereen een boodschap kan versleutelen, maar dat niet iedereen de aldus verkregen cijfertekst kan ontsleutelen (zelfs niet de versleutelaar). Er wordt namelijk voor gezorgd, dat de geheime sleutel niet uit de openbare sleutel is af te leiden. Zo'n systeem met een geheime en een openbare sleutel heet een asymmetrisch systeem.

De voorbeelden die we tot nu gezien hebben waren voorbeelden van symmetrisch systemen. Dit zijn systemen waarbij sprake is van één geheime sleutel, welke zowel voor het versleutelen als voor het ontsleutelen wordt gebruikt. Deze sleutel wordt gebruikt door de zender en door de ontvanger.
In zo'n symmetrisch systeem kan een persoon A alleen met één andere persoon, zeg B, corresponderen met die éne geheime sleutel. Het zou gevaarlijk zijn om een andere persoon, zeg C, van deze geheime sleutel op de hoogte te stellen, want dan zou C een boodschap tussen A en B kunnen onderscheppen en eerst ontsleutelen en daarna ontcijferen. Bij meer dan 2 personen zijn dus heel veel sleutels nodig.

Opdracht 25
Waarom zijn er bij meer dan 2 personen meer sleutels nodig?
Hoeveel sleutels zijn er nodig voor een groepje van 5 personen?
En voor 15? En voor 1000? En voor n?
Hoeveel sleutels heeft elke persoon zelf nodig voor een groepje van 2 personen ?
En voor 1000 ?

21. One-way-functions

Bij openbare-sleutelsystemen zijn de zogenaamde éénrichtingsfuncties (one-way functions) en 'trapdoor'-functies van belang.

Een éénrichtingsfunctie is een functie waarbij voor elk getal het beeld gemakkelijk is uit te rekenen, maar waarbij het bepalen van de inverse aanzienlijk moeilijker is. Denk maar eens aan machtsverheffen. Machtsverheffen is zelf vrij eenvoudig: het is herhaald vermenigvuldigen. De inverse van het machtsverheffen is worteltrekken en dat is heel wat ingewikkelder.

Een 'trapdoor'-functie (functie met valluik) is een éénrichtingsfunctie, waarbij de inverse bepalen gewoonlijk zeer moeilijk is, behalve als men over extra informatie beschikt.

In een systeem met openbare sleutels moet niet makkelijk de inverse bepaald kunnen worden van een gebruikte sleutel. In het begin van de zeventiger jaren is er aan dit soort functies veel aandacht besteed.

Voorbeeld
Het beeld van x bij de functie $f(x) = x^e \pmod m$ is zelfs voor grote waarden van e en m vrij eenvoudig uit te rekenen, althans met behulp van een computer.
De inverse van $f(x) = x^e \pmod m$ kan echter zeer moeilijk te bepalen zijn. Meestal kiest men voor m een produkt van twee hele grote priemgetallen. Om de inverse van f te bepalen heb je in ieder geval een ontbinding van m in priemfactoren nodig. We hebben al eerder opgemerkt dat ontbinden in priemfactoren van grote getallen juist erg moeilijk is. Dit is precies het soort functies dat een rol speelt bij het RSA-systeem.

Opdracht 26
In de analyse kennen we ook inverse functies. Schrijf van de volgende functies het functievoorschrift van de inverse functie op.
$f(x) = x + 2$
$f(x) = 2 \cdot x$
$f(x) = 2 \cdot \sqrt{x}$
$f(x) = 2 \cdot (x-3)^2$ met $D_f = [3,\rightarrow)$

22. Het RSA-systeem

Het RSA-systeem werd begin jaren zeventig bedacht door Rivest, Shamir en Adleman van het Massachusetts Institute of Technology (MIT). Dit systeem is gebaseerd op het feit, dat het eenvoudig is het produkt van twee priemgetallen te bepalen, maar dat het vinden van de priemgetallen uit zo'n produkt zeer moeilijk is. Je ziet: de heenweg is gemakkelijk, maar de terugweg is haast ondoenlijk, althans voor grote getallen !

Opdracht 27
Welke twee priemgetallen leveren het produkt 187 ?
En welke twee priemgetallen leveren 1147 ?
En welke twee priemgetallen leveren 16199 ?

Tot halverwege de zeventiger jaren namen cryptologen aan dat de wijze van versleutelen en ontsleutelen uit elkaar afgeleid kan worden. Dat is bij het RSA-systeem niet het geval en daar zit de winst. Je gebruikt daarbij iets wat je een éénrichting-algoritme zou kunnen noemen: het is (met de computer) gemakkelijk het algoritme de ene kant op toe te passen (versleutelen), maar het is praktisch onmogelijk de andere kant op te gaan, zelfs al heb je de krachtigste computers tot je beschikking en zelfs al weet je precies hoe het algoritme de ene kant op heeft gewerkt.
Vergelijk dit met het telefoonboek: je weet iemands naam en adres en kunt dan snel zijn telefoonnummer opzoeken, maar als je alleen iemands telefoonnummer weet, is het ondoenlijk zijn naam en adres te vinden alleen met dat telefoonboek. Opbellen gaat sneller!

Het RSA-systeem werkt als volgt. Een boodschap wordt verzonden van Adrie naar Bart. Adrie en Bart willen voorkomen dat de boodschap door anderen begrepen kan worden en daarom versturen ze een versleutelde cijfertekst. Bart heeft voor die versleuteling drie sleutels gemaakt, waarvan hij er twee openbaar maakt. De sleutels zijn getallen. Met die twee openbare sleutels kan Adrie de cijfertekst versleutelen. Adrie kan die twee openbare sleutels van Bart in een sleutelboek opzoeken. Zo'n sleutelboek is een soort telefoonboek waar je de openbare sleutels van personen kunt opzoeken. De derde sleutel houdt Bart echter geheim en daarmee ontsleutelt hij de ontvangen cijfertekst. Omdat een eventuele afluisteraar die derde sleutel niet kent (evenals Adrie die niet kent), kan hij de cijfertekst niet begrijpen en dus de boodschap niet achterhalen.

Opdracht 28
Hoeveel sleutels zijn er in het RSA-systeem nodig voor 2 personen?
En voor 5? En voor 1000? En voor n?
Hoeveel sleutels heeft elke persoon zelf nodig voor een groepje van 2 personen?
En voor 1000?

23. Sleutels maken

Bij het RSA-systeem ga je op een slimme manier sleutels maken. Niet alle willekeurig gekozen getallen zijn geschikt als sleutel, want zoals we al eerder zagen moet het getal wel een inverse hebben. Hier volgt het maken van de sleutels van Bart stap voor stap:

Stap 1:
Neem twee priemgetallen, zeg p = 73 en q = 103.
Deze priemgetallen zijn geheim.
Stap 2:
Bepaal het produkt $n = p \cdot q = 7519$.
Dit is één van de openbare sleutels!
Stap 3:
Kies een getal e zodanig dat $3 < e < (p - 1)(q - 1) = 7344$.
Let op: Zorg daarbij dat dit getal e relatief priem is ten opzichte van 7344, dus dat ggd(7344 ,e) = 1.
Neem bijvoorbeeld e = 13.
Dit is de andere openbare sleutel!
Stap 4:
Reken de inverse d van e (mod 7344) uit.
Er geldt dan $e \cdot d = 13 \cdot d = 1 \pmod{7344}$.
Dit is de geheime sleutel!

Opdracht 29.
Bepaal die geheime sleutel $d = e^{-1} \pmod{7344}$.

In het sleutelboek zijn bij Bart dus de sleutels n = 7519 en e = 13 te vinden.
Als iemand Bart een bericht wil sturen dan gebruik je als functie $f(x) = x^{13} \pmod{7519}$ om de cijfertekst te versleutelen.
Bart kan (en niemand anders!) met de functie $f^{-1}(x) = x^{d} \pmod{7519}$ de versleutelde tekst ontsleutelen, de cijfertekst omzetten in letters en het bericht lezen.

Voor een kraker is het de kunst om uit het produkt 7519 de twee priemgetallen 73 en 103 te halen. Pas dan is hij in staat om de geheime sleutel d te vinden en dus de cijfertekst te ontsleutelen.

In de praktijk werkt men echter niet met priemgetallen van twee of drie cijfers, maar van elk zo'n honderd cijfers. Hun produkt (een getal van zo'n 200 cijfers) wordt openbaar gemaakt. Het terugvinden van die grote priemgetallen is in een redelijke rekentijd niet te doen. Dus is het cryptosysteem niet te breken.

24. Sleutels gebruiken

Wat moet ik dan met de sleutels doen, die ik gemaakt heb?
Stel we hebben als cijfertekst het getal 62. Adrie wil Bart een bericht sturen en zoekt in het sleutelboek de twee openbare sleutels van Bart op.
Adrie berekent met de twee openbare sleutels 7519 en 13 het volgende: $6213 \pmod{7519}$.

Opdracht 30
Hoeveel is $62^{13} \pmod{7519}$?

Een eventuele afluisteraar heeft niets aan dit getal, want hij kan het met de twee openbare sleutels niet ontsleutelen en zo 62 terug vinden. Bart kan er echter wel iets mee, want hij heeft de geheime sleutel d = 565.

Hij berekent: $5376^{565} \pmod{7519}$.

Opdracht 31
Bepaal $5376^{565} \pmod{7519}$.

Voorbeeld:
Piet stuurt aan Quinten een boodschap. Piet zoekt in het sleutelboek Quinten's openbare sleutels n = 5617 en e = 11 op. De versleutelde cijfertekst die Piet naar Quinten stuurt is 10. Quinten gaat die boodschap terugvertalen met zijn geheime sleutel d.

Opdracht 32 is alleen op te lossen als de priemgetallen p en q, waarvoor geldt n = pq, zijn te vinden. Dit kan eventueel met behulp van de computer. Het is ondoenlijk om met alleen het produkt n en het getal e de geheime sleutel d te berekenen. Dit kan alleen als p en q bekend zijn en dat zijn ze nu net niet voor buitenstaanders.

Opdracht 32
Wat is d in dit geval?
Bepaal indien mogelijk de originele cijfertekst die Piet naar Quinten verzonden heeft.

25. Signeren

Een belangrijk probleem is dat Quinten zeker wil weten dat het ontvangen bericht van Piet is en niet van een of andere spion. Om daar voor te zorgen moet Piet zijn bericht van een soort handtekening voorzien. Dit noemt men signeren.

Het gaat als volgt te werk:
Eerst versleutelt Piet de cijfertekst - zeg x - met haar eigen geheime sleutel GP.
Het resultaat noemen we GP(x).

Daarna volgt er nog een versleuteling met Quintens openbare sleutel Oq.
Dit resulteert in Oq(Gp(x))

Deze dubbel versleutelde cijfertekst krijgt Quinten. Quinten laat daar zijn geheime sleutel op los en krijgt Gq(x).

Hij verwacht een bericht van Piet en laat er daarom de openbare sleutel Op.van Piet op los en verkrijgt zo x. Alleen Quinten kan dus de boodschap begrijpen en hij weet zeker dat het een boodschap van Piet is.

Schematisch:

$x \rightarrow G_p(x) \rightarrow O_q(G_p(x)) \rightarrow G_q(O_q(G_p(x))) \rightarrow O_p(G_q(O_q(G_p(x)))) \rightarrow O_p(G_p(x)) \rightarrow x$

Het ziet er ingewikkeld uit, maar als je goed kijkt komt het precies uit.

Opdracht 33
Welk bewerkingen moet je weglaten als je het bericht niet wilt signeren ?

Opdracht 34
Welke cijfertekst moet Quinten bewaren als bewijs dat het bericht dat hij ontvangen heeft inderdaad van Piet afkomstig was ?

26. De RSA club

Hieronder staat een lijst met de gegevens van vier deelnemers aan een RSA-club. De getallen zijn zo gekozen dat 'kraken' van codes mogelijk is.

	n	e	p	q	(p-1)(q-1)	d
Adrie	12.952.003	9.067				
Bart	11.000.641	3.685				
Catja	9.947.939	10.225				
Dinie	11.242.573	16.103				

Opdracht 35.
Vul de tabel in. Let op: Om te voorkomen dat je vastloopt bij de volgende opdrachten, moet je eerst je antwoorden controleren.

Opdracht 36.
Dinie stuurt het bericht kom aan Adrie. Eerst vercijfert ze kom in een getal 111513. Ze stuurt de versleutelde cijfertekst naar Adrie, maar signeert het bericht niet.
Hoe komt Dinie aan het getal 111513 ?
Welke cijfertekst stuur Dinie naar Adrie ?
Zou Catja deze cijfertekst kunnen ontsleutelen ?

Opdracht 37.
Dinie stuurt een gesigneerde versleutelde cijfertekst aan Bart: 6119501 3408095.
Welke boodschap stuurt Dinie aan Bart ? (dit zijn twee afzonderlijke getallen)

Opdracht 38.
Catja stuurt een niet gesigneerde versleutelde cijfertekst aan Bart: 542837 2208657.
Welke boodschap stuurt Catja ?

Opdracht 39.
Bart stuur de volgende gesigneerde versleutelde cijfertekst terug: 947995 9024876 5333126
Welk antwoord stuurt Bart aan Catja ?

Samenvatting RSA-systeem

Bij het RSA-systeem, zoals dat in het lespakket ter sprake is gekomen, spelen de variabelen *n*, *e* en *d* een belangrijke rol.
Iedere persoon heeft drie sleutels, twee openbare sleutels (*n* en *e*) en één geheime sleutel (*d*). Deze sleutels leveren de exponenten en de modulus voor de twee functies waarmee cijferteksten versleuteld en ontsleuteld kunnen worden.

$f(x) = x^e \pmod n$
$g(x) = x^d \pmod n$

Hierbij is x de cijfertekst die versleuteld of ontsleuteld moet worden.

Nu is het, in het algemeen, niet mogelijk om de geheime functie g af te leiden uit de openbare functie f. Deze functie g is in feite de inverse van f.

Voorbeeld:
$f(x) = x^5 \pmod{4198350484237446659}$
Wat is de inverse van f ?

Dit lijkt een eenvoudig probleem, maar dat is het niet. Voor het vinden van de inverse van f heb je in ieder geval een priemontbinding nodig van de modulus. Als men nu deze modulus groot genoeg kiest, is het vinden van de inverse van f niet te doen, omdat het vinden van de priemontbinding voor hele grote getallen niet te doen is.

In het geval men wel de priemontbinding van de modulus vindt:
$n = 4198350484237446659 = 133990427 \cdot 31333212217$
$p = 133990427$
$q = 31333212217$
$(p - 1)(q - 1) = 133990426 \cdot 31333212216 = 4198350452770244016$

Nu geldt dat
$d = \text{MODINV}(5, 4198350452770244016) = 3358680362216195213$

Waarmee de inverse van f gelijk is aan

$g(x) = x^{3358680362216195213} \pmod{4198350484237446659}$

Nu hebben we hier te maken met een modulus van slechts 20 cijfers. In dat geval in het vinden van de priemontbinding van n nog wel te doen.

Als Arnie een bericht wil sturen aan Bert, dan past Arnie op de cijfertekst de openbare sleutel van Bert toe en verstuurt het bericht. Bert past op het ontvangen bericht zijn geheime sleutel toe en krijgt zo de sleuteltekst van het bericht terug.
Als Arie het bericht wil signeren, dan past hij eerst zijn eigen geheime sleutel toe, dan de openbare sleutel van Bert en verstuurt het bericht. Bert past op het ontvangen bericht eerst zijn eigen geheime sleutel toe, daarna de openbare sleutel van Arnie. Op deze manier krijgt hij de originele cijfertekst terug.

DIT IS HET EINDE