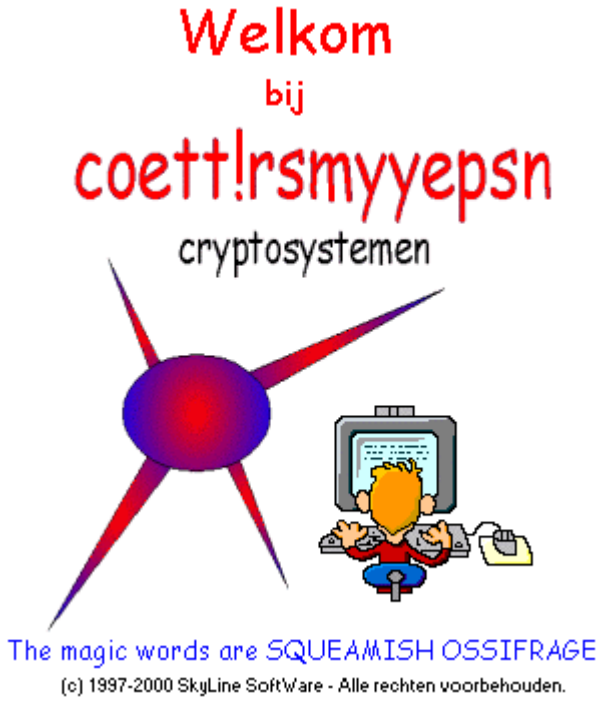

Studiewijzer

Inhoudsopgave

In deze serie lessen gaan we op zoek naar de wiskunde achter geheimschriften. Misschien denk je bij 'geheimschriften' aan iets van lang geleden. Niets is minder waar. Het is een heel actueel onderwerp. Hoe denk je dat een pinpasje in elkaar zit? Het moet toch behoorlijk moeilijk zijn zoiets na te maken. En wat dacht je van berichten over internet. Hoe kun je er voor zorgen dat niemand anders ze kan lezen?

Cryptografie heeft te maken met het geheim houden van bepaalde vormen van communicatie.. Dit is echter maar een klein deel van waar moderne cryptografie over gaat. Een belangrijk onderdeel van de moderne cryptografie heeft te maken met signeren van berichten. Dit is een manier om berichten te voorzien van een soort digitale handtekening.
Deze en andere moderne middelen worden bijvoorbeeld gebruikt bij het vaststellen van de identiteit van een pinpasgebruiker, een beveiligingssysteem en zelfs bij betaaltelevisie.

Een onderdeel van de wiskunde houdt zich bezig met gehele getallen. Het staat bekend onder de naam getaltheorie. In de getaltheorie proberen wiskundigen vat te krijgen op de gehele getallen, priemgetallen, delers en andere getalsystemen, maar vooral op hele grote getallen.

Na deze wiskunde, die voor de meeste van jullie helemaal nieuw zal zijn, gaan we ons bezighouden met verschillende voorbeelden van cryptosystemen. Sommige daarvan zijn heel eenvoudig en worden waarschijnlijk nergens meer gebruikt, maar je kunt er wel iets van leren. Na deze (eenvoudige) systemen kun je leren hoe een modern cryptosysteem, namelijk RSA in z'n werk gaat en zullen we zien dat het hier inderdaad mogelijk is berichten van een digitale handtekening te voorzien.

Bij deze serie lessen horen werkbladen, software en een studiewijzer. Je docent heeft ook antwoordbladen

Meer informatie kun je vinden op http://skyline.www.cistron.nl/crypto
Of stuur een email naar skyline@cistron.nl

Inleiding

Deze studiewijzer is bedoeld om je te helpen deze lessen in de moderne cryptografie met goed gevolg af te ronden.

In deze studiewijzer kun je suggesties vinden ten aanzien van planning. Voordat je aan iets begint is het meestal verstandig eerst een planning te maken. Vragen die je daarbij kunt stellen zijn bijvoorbeeld: Hoeveel tijd heb ik te besteden? Wanneer moet het werk af zijn?

Daarnaast hebben ik hier wat algemene tips opgenomen die je kunnen helpen bij het bestuderen van de theorie en het maken van de opdrachten. Eén van de moeilijke studievaardigheden is waarschijnlijk het zelfstandig kunnen werken. Maar ook weten wanneer je echt niet verder kunt of vaststellen dat je vast dreigt te lopen is belangrijk.

Veel leerlingen hebben de neiging om bij opgaven waar ze niet uitkomen bij de antwoorden te kijken. In het algemeen is dat niet verstandig. Om deze reden heb ik hier hints bij de opdrachten opgenomen. Dus als je een opdracht niet kunt maken, kijk dan eerst bij de hints.

Het werk bestaat grof gezegd uit 3 delen. In deze studiewijzer kun je een diagnostische toets vinden. De diagnostische toets geeft een goed beeld van wat moet kunnen. Je kunt de toets zelf nakijken, want de uitwerkingen van de toets staan achter in deze studiewijzer.

Planning

Het is natuurlijk heel moeilijk om voor iemand anders een planning te maken. Dat wil ik hier ook niet doen. Wat ik wel wil is een voorbeeld geven hoe je een planning zou kunnen maken.

> Neem aan dat je 10 klokuren voor dit onderdeel nodig hebt. Dit is inclusief opdrachten maken, computergebruiken, toetsing en evaluatie. Misschien dat er nog een eindopdracht bij komt.
> Met aftrek van de eindtoets betekent dit dat je nog 9 uur te verdelen hebt.
> Neem 2 uur voor de diagnostische toetsen en de voorbereiding op de eindtoets.
> Neem 2 uur de tijd om de software onder de knie te krijgen. Dat lijkt veel, maar uiteindelijk levert het inzetten van de software veel tijdwinst op.
> Al met al heb je voor de bestudering van de theorie en het maken van de opdrachten ongeveer 5 uur beschikbaar. Dat zijn 6 lesuren van 50 minuten.
> Het boekje bestaat uit 30 bladzijden, dus maak ongeveer 5 pagina’s per lesuur.

Belangrijk is dat je je aan je planning houdt. Nog belangrijker is om snel te reageren als je ziet dat je de planning niet gaat halen. Trek aan de bel bij je docent. In overleg kun je misschien onderdelen overslaan of samen eens kijken waar het mis gaat.

Hints bij de opdrachten

1. Welke letter komt het meeste voor? En welke letter dan?
2. a. Hoe schrijf je zoiets op..? Maak een tekening!
   b. Doe het bovenstaande in omgekeerde volgorde.
   c. Om over na te denken.
3. a. Het zijn 15 letters..... let niet op de spaties.
   b. Ook weer de omgekeerde volgorde.
4. Ook weer de omgekeerde weg....
5. Een verschoven alfabet.
6. Pas de definitie toe.
7. Op dezelfde manier als de delers van 24.
8. Zie opdracht 7.
9. a. 35 : 15 = 2 rest 5
   15 : 5 = 3 rest 0
   n = 5
   b. zie §8
10. Zoek naar een gemeenschappelijke deler.
11. Zoek naar een gemeenschappelijke deler.
12. +21 = -3
13. Gebruik wat boven de opdracht staat.
14. b. Maak eerst een vermenigvuldigingstabel van module 6.
15. Dit is lastig..... misschien op de CD kijken of op de website....
16. –
17. Boven de opdracht staat wat je moet doen.
18. De waarde van **a** doet er niet zoveel toe....
19. Volg het schema!
20. Achterstevoren!
21. Zie § 17
22. Denk aan §8
23. Haakjes wegwerken!
24. Welke letter komt het meeste voor? En daarna?
    Ze komen beide even vaak voor!
    Er zijn dan 2 mogelijkheden.
    Wat ligt het meest voor de hand?
    Wat is de inverse van... ?
25. Bij een symmetrisch systeem heb je voor elke mogelijke verbinding een andere sleutel nodig....
26. Maak een rekenschema!
27. Gebruik een computerprogramma!
28. Wat is eigenlijk het verschil met opdracht 25?
29. Zie onder “stap 4”
30. Zie eventueel §13.
31. Zie opdracht 30.
32. Zie opdracht 29.
33. Signeren betekent het aanbrengen van een soort handtekening.
34. –
35. Gebruik een computerprogramma.
36. a. Ga niet verder voordat je dit begrijpt.
    b. Welke functie moet je toepassen? (zie eventueel §23)
37. Zie het schema in §25.
38. –
39. –

Handige strookjes...

Hieronder vind je handige strookjes voor het vertalen van de geheime boodschappen uit het leerlingmateriaal.

Algemeen																									
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

Opdracht 4																									
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
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

Opdracht 19 en 20																									
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
19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
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

Opdracht 36 e.v.																									
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
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Diagnostische toets

Opdracht 1.

bereken ggd (570, 133)
geef alle delers van 120
ontbind 1365 in priemfactoren
bereken $134 \cdot 89 \pmod{13}$
bereken $12^{88} \pmod{7}$
bepaal de inverse van 13 (mod 29)

Opdracht 2.

Gegeven de substitutie met f(x) = ax + b (modulo 26), waarvoor geldt:

'b' wordt afgebeeld op 'a'
'y' wordt afgebeeld op 'h'

Bereken a en b.

Opdracht 3.

Geef de inverse functie van f(x) = 7x + 11 (modulo 29)

Opdracht 4.

Bij een RSA clubje heeft Joris de volgende openbare sleutels:

n = 12952003
e = 9067

Dit getal n is niet zo erg groot. Bereken de geheime sleutel van Joris.

Opdracht 5.

Janneke stuurt Joris het bericht HOI. Dit bericht vercijfert ze eerst naar 71408.
Welke cijfertekst stuurt Janneke naar Joris?
Welk berekening moet Joris uitvoeren om het bericht te kunnen onsleutelen?

Opdracht 6.

Janneke heeft de volgende openbare sleutels:

n = 11000641
e = 3685

Janneke wil opnieuw het bericht HOI naar Joris sturen, maar dan nu gesigneerd.
Welke cijfertekst stuurt Janneke nu naar Joris?
Welke berekeningen moet Joris uitvoeren om het bericht te kunnen ontsleutelen?

Uitwerkingen diagnostische toets

Opdracht 1.

ggd(570,133) = 19
De delers van 120 zijn 1-2-3-4-5-6-8-10-12-15-20-24-30-40-60 en 120
$1365 = 3 \cdot 5 \cdot 7 \cdot 13$
$134 \cdot 89 = 5 \pmod{13}$
$12^{88} = 2 \pmod 7$
inverse van 13 (mod 29) is 9

Opdracht 2.

Zet de letters eerst om in getallen. Er geldt: f (1) = 0 en f (24) = 7.
Invullen in de algemene vorm levert:
$0 = a \cdot 1 + b \quad (1)$
$7 = a \cdot 24 + b \quad (2)$
Trek (1) van (2) af.
$23 \cdot a = 7$
de inverse van 23 (modulo 26) is 17.
$a = 17 \cdot 7 = 15$ (modulo 26)
Invullen: 15 + b = 0, dus b = 11. a = 15 en b = 11

Opdracht 3.

De inverse van 7 (modulo 29) is 25.
Dus: $f^{-1}(x) = 25 \cdot (x - 11)$ (modulo 29)
$f^{-1}(x) = 25 \cdot x - 275$ (modulo 29)
$f^{-1}(x) = 25 \cdot x + 15$ (modulo 29)

Opdracht 4.

Maak eerst een tabel met p en q.
Zie eventueel §27.
p = 1049 , q = 12347
Bereken (p - 1)(q - 1) = 12938608
Bereken de inverse van 9067 modulo 12938608
d = 1427

Opdracht 5.

Bereken 714089067 modulo 12.952.003. Dat is 964872
Bereken 9648721427 modulo 12952.003. Dat is weer 71408

Opdracht 6.

Bereken eerst de geheime sleutel van Janneke. (d = 5965)
Bereken 714085965 modulo 11000641. Dit is 9670905.
Bereken 96709059067 modulo 12952003. Dat is 10822839.
Bereken 1080228391427 modulo 12952003. Dat is weer 9670905.
Bereken 96709053685 modulo 11000641. Dat is weer 71408.

UBasic

UBasic is geschreven door:
Prof. Yuji Kida van Department of Mathematics, Rikkyo University in Tokyo.

Version 8.74. (May 5, 1994.)

UBasic is 'basic', dus een programmeertaaltje. Het sterke van UBasic is dat deze variant kan rekenen met zeer grote getallen.

Als het programma is opgestart is het basisscherm te zien met onder in beeld een menubalk waarop achtereenvolgens:
load Dir" auto list run save xref append" edit cont
Deze commando's komen overeen met de toetsen F1-F10.
Als je een bestand wilt laden druk je F1.

Je kunt in het basisscherm ook rekenen. Als je een berekening invoert moet je eerst een "**?**" intikken.
Voorbeeld:
? 343536*3232323, vervolgens druk je op **<ENTER>** om de berekening uit te voeren.

Om unibasic af te sluiten tik je **system <ENTER>**

Je kunt hulp krijgen door in het basisscherm **help <ENTER>** in te tikken.

Allerlei berekeningen die je nodig hebt bij de opdrachten kun je met dit programa uitvoeren. Hieronder volgen de belangrijkste:

modpow(a, b, n)

Met deze functie kan je machtsverheffen modulo een gegeven getal.
Deze functie berekent $a^b \pmod{n}$

Voorbeeld 1:
Je wilt $12345^{678910} \pmod{22334455}$ berekenen. Met een gewone rekenmachine gaat dat niet, maar met de functie **modpow** gaat heel gemakkelijk:
Je toets in:
?modpow(12345,678910,22334455)
uiteraard weer gevolgd door **<enter>**.
Het antwoord verschijnt op het beeldscherm: **224520**

Voorbeeld 2:
Je kunt deze functie ook gebruiken voor het vereenvoudigen van bijvoorbeeld 324234 (mod 2324). Neem dan voor *b* de waarde 1.
Je toets in:
?modpow(3242324,1,2324)
gevolgd door **<enter>** en op het beeldscherm verschijnt:
344
OK

modinv(a, n)

Met deze functie kun je de inverse van *a* modulo *n* uiterekenen.
De functie geeft de oplossing voor *x* van $(a \times x) \bmod n = 1$

Voorbeeld:
Bereken de inverse van 23 modulo 45.
Je toetst in:
?modinv(23,45)
gevolgd door <**enter**> en op het beeldscherm verschijnt:
2
OK

nxtprm(x)

Deze functie geeft het kleinste priemgetal dat groter is dan *x*.

Voorbeeld:
?nxtprm(12251)
12347
OK
Kennelijk is het eerstvolgende priemgetal 12347.

prm(n)

Deze functie geeft het *n*-de priemgetal.

Voorbeeld:
?prm(12251)
131071
OK

gcd(m,n)

Hiermee bereken je de g.g.d. van *m* en *n*.

Voorbeeld:
?gcd(634808394,869085089789070)
66
OK

Gebruik eventueel het overzicht op bladzijde 13 achter in deze studiewijzer voor een snel overzicht van de bovenstaande functies.

Bestandsfuncties

Bovenstaande functies zijn **ingebouwde** functies. Daarnaast kun je met UBasic programmeren. Bij een standaard installatie heb je de beschikking over zo'n 50 programma's die je kan gebruiken.

Het uitvoeren van een programma gaat als volgt:
Toets eerst **NEW**. Het programmageheugen is nu schoon. Toets **F5**. Je krijgt dan de volledige lijst van programma's te zien. Met de pijltjestoetsen kun je door dit lijstje 'wandelen'. Kies een bestand met de **<enter>** toets.

Je kunt een programma onderbreken met **crtl-c**.

MPQSX

Dit programma ontbindt een getal in factoren. Het is niet geschikt voor al te grote getallen. De methode is wel erg zeker, maar niet erg snel.

ECM en ECMX

Deze programa's doen hetzelfde als MPQSX, maar is veel sneller en daarom geschikt voor grotere getallen.

PRTEST1

Dit programma zoekt uit of een gegeven getal een **priemgetal** is. Het maximum aantal cijfers van zo'n getal is 127.

APRT-CL

Idem als PRTEST1, maar een stuk sneller. Dit programma kan getallen van maximaal 300 cijfers aan.

Op de CD-rom en de website staat meer informatie over deze functies en programma's.

Overzicht functies en programma's UBasic.

ingebouwde functies:	**berekent:**
MODPOW(*a*, *b*, *n*)	$a^b \pmod n$
MODINV(*a*, *n*)	de inverse van *a* modulo *n*
NXTPRM(*x*)	het kleinste priemgetal na *x*
PRM(*n*)	het *n*-de priemgetal
GCD(*m*, *n*)	de g.g.d van *m* en *n*

programma's:	**berekent:**
MPQSX	ontbinding in factoren (langzaam)
ECM en ECMX	ontbinding in factoren (snel)
PRTEST1	of getal priem is
APRT-CL	of getal priem is

belangrijkste commando's	**werking:**
NEW	programmageheugen wissen
?	geeft het resultaat van een berekening
print	geeft het resultaat van een berekening
F5	programma uitvoeren (geheugen of van schijf)
ctrl-c	programma onderbreken
system	ubasic afsluiten

Overzicht van het programma Numbers:

In het programma kan men kiezen uit verschillende menu's. Hieronder staan enkele voorbeelden van wat het programma kan:

- Rekenen met (of zonder) modulus, vermenigvuldigen, machtsverheffen en ggd of kgv bepalen, inverse bepalen van n modulo m.
- Priemtests, ontbinden in priemfactoren, priemgetallen zoeken.
- Versleutelen en ontcijferen, ook RSA.
- Frequentieanalyse uit laten voeren op teksten.
- En nog veel meer...

Kortom van alles en nog wat.....

Tabel van priemgetallen tussen 0 en 1000

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	503	509	521
523	541	547	557	563	569	571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659	661	673	677	683	691	701
709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977	983	991	997