Een van de meest tot de verbeelding sprekende voorgestelde keuzeonderwerpen is cryptografie. Onafhankelijk van elkaar gingen **Monique Stienstra** en **Harm Bakker** aan de slag om lesmateriaal te ontwikkelen en te testen. Twee visies, twee experimenten, twee analyses. Dat kan, mag en moet eigenlijk in wiskunde D!

Lessenserie Cryptografie

Inleiding

Na een oproep van cTWO: 'docenten gezocht die een lessenserie willen schrijven voor wiskunde D' hebben wij, Monique Stienstra van het Stedelijk Gymnasium in Nijmegen en Harm Bakker van het CSG Liudger in Drachten, ons aangemeld om een lessenserie over cryptografie te schrijven. Hoewel we het over de inhoud eens waren, keken we wel op een verschillende manier naar het behandelen van de stof. Monique gebruikte de cryptografie als kapstok om de getaltheorie aan op te hangen. Leerlingen kennis laten maken met wiskunde zoals die op de universiteit onderwezen wordt, was het doel en cryptografie het middel om leerlingen te laten zien dat die abstracte wiskunde ook echt ergens voor gebruikt wordt. Harm zag meer als doel de leerlingen kennis te laten maken met een of meer cryptografische systemen. Daarbij zijn onderwerpen uit de wiskunde (getaltheorie, complexiteit van algoritmen) onmisbare hulpmiddelen om de werking en de veiligheid van deze systemen te begrijpen; een goede reden om daar uitgebreid aandacht aan te besteden.

Waarom cryptografie?

Cryptografie is de kunst van het beveiligen van berichten. Dit beveiligen van berichten doet men al eeuwenlang. Vertrouwelijke stukken van defensie, liefdesbrieven aan je minnaar, maar ook informatie die uitgewisseld wordt als je gaat pinnen bij de bank en berichten via internet of mobiele telefonie worden beveiligd.

Cryptografie is tegenwoordig zeer belangrijk en het belang neemt alleen maar toe. Het is tegelijk een onderwerp dat dichtbij leerlingen staat. De meeste leerlingen kennen het woord en hebben wel enig idee waar het voor gebruikt wordt en waarom het belangrijk is. Het is ook een onderwerp dat tot de verbeelding spreekt. Er wordt al snel aan spionnen en andere spannende zaken gedacht. In de cryptografie speelt wiskunde, met name getaltheorie, een belangrijke rol. Deze wiskunde zou zonder de context cryptografie waarschijnlijk door veel leerlingen saai gevonden worden en leerlingen zouden geen idee hebben waarom je je in dit soort abstracte wiskunde zou willen verdiepen. Maar als je ziet wat je er mee kunt, verandert het verhaal. Simpele dingen als het ontbinden van getallen blijken heel moeilijk te zijn en moeilijke dingen als getallen tot heel grote machten verheffen, blijken goed te doen. Dat is verrassend en als je dan ook nog ziet wat je er mee kunt, wordt het leuk.

Inhoud

Cryptografie heeft al een lange geschiedenis. Een aantal klassieke methoden om boodschappen zo te beveiligen dat onbevoegden de inhoud niet kunnen lezen of ontcijferen, passeren de revue. Deze eerste methoden zijn allemaal voorbeelden van symmetrische cryptografische systemen. Dat wil zeggen dat het omzetten van de oorspronkelijke boodschap in een geheimschrift (versleutelen) en het terughalen van de oorspronkelijke tekst uit de versleutelde versie (ontcijferen) in feite op dezelfde manier gebeurt: als je precies weet hoe een boodschap is versleuteld, dan is ook duidelijk hoe je moet ontcijferen. De meest bekende uit dit rijtje (Caesar-verschuiving) kent eigenlijk iedere leerling wel: vervang iedere letter uit je bericht door een letter die een vast aantal posities verder in het alfabet staat.

Al snel ontstaat de wens om niet met de lettertekens zelf, maar met hun posities in het alfabet, te rekenen. In plaats van alles in woorden te formuleren, kun je dan de operaties die je bij het versleutelen wilt gebruiken in formules uitdrukken. Naast het feit dat daarmee de operaties veel makkelijker eenduidig zijn te beschrijven, biedt dit de mogelijkheid om de systemen met wiskundige technieken te onderzoeken. Bijvoorbeeld: als je bij het versleutelen in plaats van bij de positie een vast getal op te tellen, het rangnummer met een vast getal gaat vermenigvuldigen, gaat dat dan altijd goed? Waarom wel, waarom niet? Wanneer wel, wanneer niet?
Om elkaar goed te begrijpen, is het nodig een aantal afspraken te maken: welke symbolen gebruiken we (met andere woorden, wat is het alfabet), hoe nummer je in dit alfabet, wat versta je onder een sleutel?

Bij het beoordelen van een cryptosysteem hanteren we het principe van Kerckhoff. Dit principe zegt dat je er altijd vanuit moet gaan dat een afluisteraar weet welk cryptosysteem wordt gebruikt (bijvoorbeeld Caesar), maar niet weet wat de sleutel is (het aantal posities dat is opgeschoven). Het kraken van een cryptosysteem komt er dan op neer dat je uit onderschepte boodschappen de sleutel moet afleiden. Leerlingen zien dat hierbij verschillende technieken een rol kunnen spelen. Zo kun je het ene systeem aanvallen met algebra en getaltheorie en heb je op andere momenten juist meer aan kansrekening en statistiek.

Voorbeeld: Vigenère-versleuteling

Tekst	CRYPTOGRAFIE IS BOEIEND
Sleutel	EUCLIDES
	CRYPTOGRAFIEISBOEIEND
	EUCLIDESEUCLIDESEUCLI
Getallen:	02 17 24 15 19 14 06 17 00 05 08 04 08 18 01 14 04 08 04 13 03 04 20 02 11 08 03 04 18 04 20 02 11 08 03 04 18 04 20 02 11 08
Versleuteld:	06 11 00 00 01 17 10 09 04 25 10 15 16 21 05 06 08 02 06 24 11
Sleuteltekst:	GLAABRKJEZKPQVFGICGYL

Bij symmetrische cryptografie is het zaak de sleutel geheim te houden. Als eenmaal duidelijk is wat de sleutel is, zijn alle onderschepte boodschappen eenvoudig te ontcijferen. Bovendien lukt het dan ook om je als iemand anders voor te doen. Bij Public Key Cryptosystemen ligt de zaak geheel anders. In zo'n systeem publiceert iedere deelnemer (een deel van) zijn sleutel. Iemand die deelnemer X een boodschap wil sturen, versleutelt deze boodschap met de door X gepubliceerde sleutel. Ontvanger X is echter de enige die, met het geheime deel van de sleutel, de versleutelde boodschap kan ontcijferen. De veiligheid van dit soort systemen is gebaseerd op het vertrouwen dat uit de kennis van het publieke deel van de sleutel het geheime deel niet is af te leiden. Het meest bekende Public Key systeem is RSA. De veiligheid van dit systeem is gebaseerd op de waarneming dat er geen snelle methoden bekend zijn om grote getallen (zeg 200 cijfers) in priemgetallen te ontbinden.

Om boodschappen te kunnen versleutelen en ontcijferen, en om de achtergronden van de diverse behandelde systemen te kunnen begrijpen is een flinke hoeveelheid (elementaire) getaltheorie nodig. Dit vormt dan ook het hart van de lessenserie. Kort gezegd gaat het hier om rekenen modulo een positief geheel getal, ofwel rekenen in $\mathbf{Z}_m$. Optellen en aftrekken gaat eenvoudig en ook vermenigvuldigen levert eigenlijk geen problemen. Delen, of eigenlijk het berekenen van een multiplicatieve inverse, gaat een stuk lastiger. Het (uitgebreide) algoritme van Euclides levert een goede manier om dit effectief uit te voeren.

Machtsverheffen is weer goed te doen, zelfs voor flink grote getallen. Maar worteltrekken en logaritme nemen gaan voor grote waarden ons vermogen te boven. Niet zo'n wonder als je bedenkt dat dit een van de grote problemen in de getaltheorie is en dat de veiligheid van sommige cryptosystemen juist gebaseerd is op het niet efficiënt kunnen uivoeren van deze bewerkingen.

Ervaringen op het Stedelijk Gymnasium Nijmegen

De lessenserie is op het Stedelijk Gymnasium Nijmegen getest in drie wiskunde B1 examenklassen en drie wiskunde B12 examenklassen, door in totaal zes verschillende docenten. In de B1-klassen werd redelijk wat klassikaal gedaan, in de B12-klassen werd het boekje meer in kleine groepjes doorgewerkt. Voor de lessen werd ongeveer evenveel huiswerk gegeven als leerlingen gewend zijn voor de andere lessen wiskunde. Als afwisseling in de lessen hebben wij een documentaire over de zoektocht van Wiles naar het bewijs van de laatste stelling van Fermat laten zien. In het boekje staan regelmatig stukjes over wiskundigen. Bij het stukje over Fermat wordt Andrew Wiles genoemd. De leerlingen waren gegrepen door het enthousiasme, de volharding en vooral de emoties van Wiles. Ook bleek het een echte eye-opener dat er in de wiskunde nog echt iets nieuws te bedenken is.

Het deel over de geschiedenis van de cryptografie werd zeer vlot doorgewerkt. Leerlingen vonden het interessant en vrij eenvoudig. Het vervolg ging minder snel, maar ook hier werd goed aan gewerkt. In de klas merkte ik vaak dat leerlingen verrast waren door de kracht van de getaltheorie. Een opgave als 'bereken $\bar{7}^{3843}$ in Z_{640}' ziet er best lastig uit, maar blijkt erg mee te vallen. De opgaven waar leerlingen het een en ander moesten bewijzen, waren wel voor veel leerlingen te hoog gegrepen. Met name in de B1-klassen, waar leerlingen niet gewend zijn aan formele bewijzen, kwamen leerlingen hier niet zelfstandig uit. Toen we in mijn B1-klas klassikaal het bewijs probeerden te vinden, konden veel leerlingen het wel volgen, maar vond slechts ongeveer de helft het leuk om te doen. Een voorbeeld van zo'n bewijsopgave is de volgende opgave die gaat over de stelling van Euclides:

Nu moeten we onderzoeken waarom het tweede deel werkt:
Voor $a > 0$ en $a \in N$ en $a > b > 0$ en $b \in N$ geldt $\text{ggd}(a, b) = \text{ggd}(b, a \bmod b)$.

§4.1 Opgave 7
Schrijf a als $qb + r$, waarbij $0 < b < r$ en q en r gehele getallen zijn. Dan moeten we dus bewijzen dat $\text{ggd}(a, b) = \text{ggd}(b, r)$.
a) Leg uit dat dat is wat we moeten bewijzen.
Stel dat $d|a$ en dat $d|b$.
b) Bewijs dat dan ook $d|r$. (Hint: gebruik opgave 5 van paragraaf 3.2.)
c) Leg uit dat je hiermee meteen bewezen (uitgelegd) hebt dat $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Het grootste deel van de opgaven is echter behoorlijk praktisch. De leerlingen vonden het goed te doen en de meesten vonden het ook leuk om te doen. Je kunt hierbij denken aan opgaven die duidelijk over cryptografie gaan zoals de volgende opgave over het affiene cryptosysteem:

§ 2.2 Opgave 7
Wanneer we weten hoe twee letters vercijferd worden, kunnen we het paar (a,b) achterhalen door deze gegevens in de encryptiefunctie in te vullen. We kunnen de sleutel dus kraken zonder alle sleutels te proberen. Achterhaal het paar (a,b) als je weet dat een D vercijferd een Q wordt en een N vercijferd een O wordt, dus dat $E_{(a,b)}(3) = 16$ en $E_{(a,b)}(13) = 14$.

Uitwerking:

$$\begin{cases} 3a + b = 16 + 26k \\ 13a + b = 14 + 26l \end{cases}$$

$$\begin{cases} b = 16 - 3a = 26k \\ b = 14 - 13a + 26l \end{cases}$$

$16 - 3a + 26k = 14 - 13a + 26l$
$10a = 26(l - k) - 2)$
$a = 5, l - k = 2$
$b = 1$

Of aan meer getaltheoretische opgaven zonder context, zoals:

§ 4.3 Opgave 20
a) Bereken $\text{ggd}(291, 105)$ met het algoritme van Euclides.
b) Bereken een oplossing van de lineaire Diophantische vergelijking $291x + 105y = \text{ggd}(291, 105)$.

c) Leg uit waarom $\overline{105}$ geen inverse in $\mathbf{Z}_{291}$ heeft.

De lessenreeks werd getoetst met een opgave in de laatste dossiertoets in klas 6. Deze dossiertoets ging over de gehele examenstof plus de stof van de lessenserie cryptografie. We hebben ons daarom beperkt tot een standaardopgave over cryptografie.

Opgave cryptografie

4.19 Los de volgende Diophantische vergelijking op met behulp van het uitgebreide algoritme van Euclides: $6191x + 12587y = 41$.

4.20 Bereken $\overline{37}^{290}$ in $\mathbf{Z}_{315}$.

Bob heeft als publieke RSA-sleutel het paar $(145, 69)$. Alice wil hem een geheime boodschap sturen. Het vercijferde bericht luidt '5' en dat stuurt ze op. De sleutel van Bob is echter makkelijk te kraken.

4.21 Bereken de geheime boodschap die Alice aan Bob wilde laten weten.

Deze opgave is door de meeste leerlingen goed gemaakt.

Na de lessenserie is zowel de leerlingenenquête van CTWO afgenomen als de docentenenquête. Een opvallend verschil tussen de B1- en de B12-leerlingen is dat de B12-leerlingen gemiddeld een 4,6 gaven voor de uitleg in het boekje en de B1-leerlingen gemiddeld een 7,0. In eerste instantie verbaasde dit me. B12-leerlingen zijn gemiddeld beter en zouden toch minder moeite met de uitleg in het boekje moeten hebben? Na hier wat over gesproken te hebben met mijn collega's, bleek dat in B12-groepen veel meer in groepjes en veel minder klassikaal was gewerkt. De uitleg van de docent in de B1-groepen zorgde ervoor dat de leerlingen de uitleg in het boekje beter begrepen. In het boekje staat veel op een manier uitgelegd die aansluit bij hoe dit in het eerste jaar op de universiteit gebeurt.

Voorbeeld:
Je zoekt een inverse $\bar{b}$ zodanig dat $\bar{a} \cdot \bar{b} = {}_m\bar{1}$, dus geldt $m|ab - 1$.
Dus is er een getal k zó dat $mk = ab - 1$, dus $ab - mk = 1$.

Voor leerlingen is dit erg moeilijk om zelfstandig door te werken. Er worden veel tekens en variabelen gebruikt. Het blijkt dat leerlingen dit wel begrijpen als het in de klas eerst met wat voorbeelden is uitgelegd. Voor zelfstandig doornemen is het minder geschikt.

Verder bleek uit de leerlingenenquête vooral dat de leerlingen veel nieuwe dingen geleerd hebben (gemiddeld cijfer op dit punt 8,6) en dat ze het iets heel anders vonden dan wat ze gewend waren. Of ze dat waardeerden, verschilt. Sommige leerlingen vonden het erg leuk, anderen hadden het idee dat je het nergens voor nodig had en hadden er geen zin in. Een aantal 'luie' leerlingen werd gegrepen door dit onderwerp. Ze maakten huiswerk en wisten in de klas precies waar het over ging, stelden vragen

en gaven heel veel antwoorden. Erg leuk om te zien en voor de leerlingen zelf was het ook erg leuk. Een leerling die al tijden vast overtuigd is biologie te gaan studeren, zei dat wiskunde misschien toch een optie was als biologie tegenviel.

Een tweede versie

In de eerste versie wordt een aantal onderwerpen nogal formeel behandeld. Als het je er om gaat te laten zien hoe wiskunde functioneert in een eigentijdse toepassing, dan is deze weg misschien wat te abstract. Zeker als je de bedoeling hebt om het ook voor leerlingen uit HAVO-klassen geschikt te laten zijn, dan kan bijvoorbeeld het modulo-rekenen beter op een wat meer mechanische manier worden aangereikt.

In de tweede versie is er voor gekozen om het modulo-rekenen te introduceren door middel van de binaire operator mod. In plaats van: 'twee getallen zijn equivalent modulo 5 als ze dezelfde rest bij deling door 5 hebben' (bijvoorbeeld $17 \equiv 2 \bmod 5$) de definitie: 'een geheel getal modulo 5 is de rest bij deling van dat getal door 5' (dus $17 \bmod 5 = 2$). Dat dit meer is dan een verschil in notatie, blijkt bijvoorbeeld uit de constatering dat in de eerste opzet $\mathbf{Z}_m$ een verzameling van restklassen is met bewerkingen die worden geërfd van de bewerkingen op $\mathbf{Z}$, terwijl in de tweede aanpak $\mathbf{Z}_m$ bestaat uit de getallen 0 tot en met $(m-1)$ waarop bewerkingen opnieuw moeten worden gedefinieerd met behulp van de mod-operator.

Een tweede reden om al voordat er ervaringen waren met de eerste versie een tweede versie te maken, was de wens om al in een vroeg stadium leerlingen ook opdrachten te laten uitvoeren die meer lijken op realistische situaties. Dan kom je er niet met alleen de 26 (hoofd)letters uit ons alfabet. Daarom wordt al snel de ASCII-tabel gebruikt, een standaard in het elektronische dataverkeer, die naast letters en cijfertekens ook leestekens en allerlei andere symbolen bevat. Naast het feit dat er nu realistische boodschappen behandeld kunnen worden, levert dit inspiratie om met grotere getallen te gaan werken. En dan kom je er ook niet meer met ad-hoc manieren van werken en zul je je moeten verdiepen in een aantal methoden en algoritmen uit de getaltheorie: het vinden van de multiplicatieve inverse van 17 in $\mathbf{Z}_{41}$ wil nog wel met uitproberen, maar voor het berekenen van de inverse van 147 in $\mathbf{Z}_{371252}$ kun je maar beter wat systematischer te werk gaan.

Bij het herschrijven is een aantal paragrafen naar de appendices verhuisd. De inschatting was dat, misschien met uitzondering van een enkele VWO B12-leerling, de bewijzen van de Kleine Stelling van Fermat en de stelling met betrekking tot de Euler-functie te moeilijk zijn. Opnemen in de lopende tekst levert dan al gauw teveel vertraging, zeker als leerlingen min of meer zelfstandig dit pakketje doorwerken.

Applets

Als je met wat grotere sleutels wilt gaan werken, dan loop je al gauw uit het bereik van de grafische rekenmachine. Her en der op internet zijn wel programma's te vinden om met grote gehele getallen te rekenen, maar het gebeurt nogal eens dat links opeens niet meer werken.
Daarom is er een eigen set applets gemaakt. De opleiding Wiskunde van de Rijksuniversiteit Groningen was zo vriendelijk om webruimte beschikbaar te stellen. De applets zijn nu te vinden op www.math.rug.nl/crypto.

Ervaringen in Drachten

Op CSG Liudger in Drachten is het experiment uitgevoerd binnen de kaders van een Praktische Opdracht. De ene helft van de klas heeft zich bezig gehouden met een lespakket Complexe Getallen; de andere helft heeft in vier groepjes het boekje Cryptografie doorgewerkt. In totaal waren er vijf weken met elk drie lesuren beschikbaar, plus natuurlijk de bijbehorende thuiswerktijd. Tijdens de geroosterde lesuren was steeds een docent beschikbaar om vragen te beantwoorden; er zijn geen klassikale momenten geweest.

Het inleidende hoofdstuk en het hoofdstuk over symmetrische cryptografie is door de leerlingen voortvarend aangepakt en aan het eind van de daarvoor geplande eerste week waren ze inderdaad wel zo ongeveer door deze hoofdstukken heen. Het hoofdstuk over getaltheorie leverde aanzienlijk meer problemen op. Er waren veel vragen en het tempo was er behoorlijk uit. Maar wat erger is, het is ons min of meer ontgaan dat aan het eind van de derde week eigenlijk niemand echt door de stof was gekomen. Toen in de vierde week de public key systemen aan de orde kwamen, liepen de leerlingen voortdurend vast op zaken die ze zich in het vorige hoofdstuk eigen hadden moeten maken.
In deze week hebben de leerlingen een uitvoerig practicum gedaan rond RSA. Eén van de leerlingen heeft een e-mail account aangemaakt en die beschikbaar gesteld aan alle deelnemers. Via deze account hebben de groepjes hun publieke sleutel gepubliceerd en elkaar vervolgens versleutelde berichten (met elektronische handtekening) gestuurd. Ontvangen berichten werden met de eigen geheime sleutel ontcijferd. Omdat iedereen toegang had tot de account, was het geen enkel probleem om berichten die voor anderen bestemd waren te onderscheppen. Maar ontcijferen is een heel ander verhaal.

Eén van de groepjes is het gelukt om de sleutel van een ander groepje te kraken, maar ze willen niet zeggen hoe ze dit hebben gedaan. Het vermoeden bestaat dat het ene groepje een deel van het verslag (met hun sleutels!) op een van de laptops heeft laten staan en dat het andere groepje dat is tegengekomen. Want een getal van zo'n tachtig cijfers ontbinden, gaat echt niet zo makkelijk.

Omdat dit project werd uitgevoerd als een praktische opdracht, is er geen toets afgenomen. De afronding bestond uit een RSA-practicum, waarbij de groepjes hun publieke sleutels publiceerden en elkaar vervolgens versleutelde berichten (met digitale handtekening) stuurden.

Als eindproduct hebben de groepjes een rapport gemaakt met daarin opgenomen de uitwerkingen van de opgaven en een verslag van het afsluitende RSA-practicum. Vooral dit laatste is keurig uitgewerkt.

Uit de afgenomen enquête blijkt dat de leerlingen met plezier aan dit onderwerp hebben gewerkt, maar dat ze het wel erg moeilijk vonden. Het zelfstandig werken aan zo'n geheel nieuw onderwerp viel flink tegen. Ze geven ook aan dat ze het heel lastig vinden om zonder mondelinge toelichting het schriftelijk materiaal te begrijpen. De gemiddelde waardering voor het lesmateriaal is wel voldoende, maar ze hadden graag wat meer hulp gehad. Alle leerlingen geven aan dat dit onderwerp helemaal niet aansluit bij wat ze bij wiskunde gewend zijn. Ze vinden wel dat ze wat nieuws geleerd hebben, maar de meesten denken niet dat ze nu beter zijn voorbereid op een vervolgopleiding.

Het RSA-practicum was een prima uitsmijter. Diverse leerlingen noemen dit expliciet als het leukste deel van het project.

Conclusie

Al met al kunnen we dit experiment als eerste test als geslaagd beschouwen. De leerlingen vonden het onderwerp interessant en ze hebben een beter beeld van wat voor een wiskunde ze in het vervolgonderwijs kunnen tegenkomen. Ook is hen duidelijk geworden dat er echt nog wel iets te doen is op dit vlak. We denken dat het behandelen van een onderwerp als cryptografie kan bijdragen aan het vergroten van de aantallen wiskundestudenten.

Wel hopen we dat we door CTWO in de gelegenheid gesteld zullen worden de lessenserie te verbeteren, zodat er boekjes komen te liggen die ook door andere scholen gebruikt kunnen worden zonder dat er eerst aan gesleuteld hoeft te worden. Deze lessenserie is aardig als eerste experiment, maar zeker nog geen eindproduct.

Harm Bakker, CSG Liudger, Drachten
Monique Stienstra, Stedelijk Gymnasium, Nijmegen