De didactiek van informatica zonder apparatuur

Geurts, Joris

Award date:
2012

De didactiek van Informatica Zonder Apparatuur

Joris Geurts
Studentnummer: 205126
Informatica (10 ECTS)
Begeleiders: Kees Huizing, Jacob Perrenet

Abstract

Dit verslag beantwoordt de vraag of een zelf samengestelde module Informatica Zonder Apparatuur functioneert in het Nederlandse informatica onderwijs.
De gebruikte onderzoeksmethode is dat een lessenserie ontworpen is, die vervolgens uitgevoerd werd waarbij er metingen aan zijn verricht.
Het resultaat is dat de cryptografie activities van Computer Science Unplugged goed in het onderwijs passen, maar dat de modules vooraf gegaan dienen te worden door een inleiding om de noodzaak van cryptografie te verduidelijken (deze zou overigens goed passen in de Computer Science Unplugged bundel). En voor de liefhebbers van programmeren kan het onderwerp afgesloten worden met programma's voor RSA encryptie en decryptie.

1 Introductie

Informatica kan op verschillende manier gedoceerd worden. Allereerst natuurlijk met de computer. Het programmeren is daar natuurlijk het bekendste voorbeeld van. Daarnaast zijn er allerlei mogelijkheden voor simulaties (van logische poorten, processorarchitecturen tot het managen van containerterminals).
Informatica kan ook onderwezen worden zonder computers. Algoritmes worden ontdaan van hun computercontext en worden geplaatst in een alledaagse context. De leerlingen hoeven niet stil aan hun tafel te blijven zitten, maar worden onderdeel van het algoritme.

Deze laatste didactische werkvorm is onderwerp van dit onderzoek. We beginnen met een definitie:

> Informatica Zonder Apparatuur (IZA): activerend onderwijs van informatica zonder dat computers een essentiële rol spelen, en waarbij geen speciale voorkennis vereist is.

De laatste clausule van de definitie is nodig om te voorkomen dat (in het bijzonder in mijn onderzoek over cryptografie) bijvoorbeeld een flinke lading wiskunde toe wordt gepast.

De Canterbury University in New Zealand heeft een dergelijke onderwijsmethode ontwikkeld, genaamd Computer Science Unplugged (CSU) (**http://csunplugged.org/**). Dit is een verzameling informatica theorieën, uitgelegd als gewone dagelijkse zaken. Het programma is geschikt voor PO en VO (afhankelijk van het onderwerp). Het programma bestaat uit 26 modules waarbij leerlingen vaak in spelvorm de theorieën exploreren, steeds zonder dat er een computer aan te pas komt. CSU heeft zich verspreid over de hele wereld.

Beide termen, IZA en CSU, komen voor in dit onderzoek. IZA is de algemene term voor elk informatica onderwijs zonder computers, terwijl CSU een specifieke methode is. CSU is dus een deelverzameling van IZA.

De probleemstelling die de aanleiding is geweest van dit onderzoek luidt: informatica wordt vaak gezien als een moeilijk, ondankbaar, specialistisch vak voor nerds, en elk initiatief om dit patroon te doorbreken is welkom (Cutts, Brown, Kemp & Matheson, 2007, Marks, Freeman &

Leitner, 2001). Juist het ontbreken van computers kan aangewend worden om te verduidelijken dat informatica net zo gewoon als het dagelijkse leven is (Taub, Ben-Ari & Armoni, 2009).

Mijn eigen visie is dat ik een sterke voorstander ben van metaforen in het onderwijs. Dat kan op kleine punten (deadlock = vier auto's arriveren op een gelijkwaardige kruising), of op een heel concept (een cpu met rom + ram = een kok met een kookboek en pannen). Je merkt bij de studenten een duidelijke verankering, en als naderhand nog iets uitgelegd moet worden, dan bemerk ik dat het scheelt door naar de metafoor te refereren.

2 Theorie

Voorafgaand aan de ontwikkeling van het onderwijsmateriaal is eerst een literatuurstudie gedaan. Deze studie geeft een basis waarop vervolgens nieuwe onderzoeksvragen geformuleerd kunnen worden. De literatuurstudie is gedaan voor de volgende aspecten:

- wat zijn de achterliggende theorieën van IZA?
- wat zijn de praktijk ervaringen van IZA?
- past het programma van IZA in het Nederlandse onderwijs?
- welke onderzoeken zijn er gedaan naar cryptografie lesactiviteiten in het voortgezet onderwijs?

CSU (Bell, 2000) is ontwikkeld om leerlingen een breder beeld te geven van informatica dan uitsluitend Word, Excel & PowerPoint (Bell, Alexander, Freeman & Grimley, 2009). Veel landen zien een dalend aantal studenten kiezen voor informatica, terwijl de hedendaagse kenniseconomie er juist steeds meer nodig heeft (Heersink & Moskal, 2010). Voor meisjes (die toch al ondervertegenwoordigd zijn) is deze daling zelfs nog groter. Leerlingen hebben een slecht beeld van het beroep van informaticus.
CSU biedt een (gratis) programma om deze tendens om te buigen. Het is opgezet als een serie van activiteiten om de ideeën van informatica te onderwijzen, zonder hulp van computers (vandaar de naam *unplugged*). Doordat er geen gebruik wordt gemaakt van computers kan je enerzijds benadrukken dat de computer een middel is en geen doel, en anderzijds dat je geen lastige learning curve hoeft te nemen voor de vaardigheden van het programmeren.
CSU biedt de lesbrief van de activiteiten (Bell, Witten, Fellows, Adams & McKenzie, 2002) (met per activiteit: print-outs voor de leerlingen, en een checklist voor lespreparatie). Op de website zijn video's van de activiteiten, en achtergrond materiaal voor verdere diepgang.

Naast CSU zijn er ook andere IZA methodes.
Bell, Curzon, Cutts, Dagiene & Haberman (2011) doet een vergelijkend warenonderzoek naar vijf verschillende benaderingen. Een van die benaderingen is Bebras, die in Nederland bekend is als de jaarlijkse Beverwedstrijd.
Carmichael (2008) beschrijft een cursus met meisjes als doelgroep. Binnen deze cursus wordt wel gebruik gemaakt van computers (namelijk het programma GameMaker), maar het doel is om de awareness voor informatica bij meisjes te verhogen.
Marcu, Kaufman, Kate Lee, Black, Dourish, Hayes & Richardson (2010) beschrijft het ontwerp en de evaluatie voor een cursus voor meisjes op het voortgezet onderwijs. Het materiaal bestaat

uit Lego (met een visuele programmeertaal) en handenarbeid materialen (voor een creatieve inbreng). De begeleiding is voornamelijk door vrouwelijke studenten gedaan, vanwege het rolmodel.
Cutts, Brown, Kemp & Matheson (2007) hebben een serie van workshops ontworpen en geëvalueerd voor voortgezet onderwijs. Elke workshop begint met een alledaags voorbeeld en gaat dan de onderliggende informatica exploreren.
Marks, Freeman & Leitner (2001) geeft 5 cases voor studenten op universitair niveau.
Bergin, Keleman, McNally, Naps, Goldweber, Power & Hartley, S. (2000) beschrijft uitgebreide instructies voor onderwerpen zoals Object Oriented design en Algoritmiek (o.a. recursie).

Daarnaast zijn er diverse onderzoeken uitgevoerd om na te gaan of deze initiatieven überhaupt wel effect ressorteren.
Lambert & Guiffre (2008) onderzocht in het basisonderwijs een CSU deelprogramma. Testen voor en na de interventie tonen aan dat de leerlingen een beter zicht hebben verworven van informatica.
Taub, Ben-Ari & Armoni (2009) onderzocht het gehele CSU programma bij het voortgezet onderwijs. Zij merkten dat het niet meevalt om de gezichtspunten van leerlingen betreffende informatica te veranderen. Niet alle leerlingen konden uiteindelijk een vertaling maken van CSU activiteiten naar informaticaconcepten. Ook bleef het beeld dat de leerlingen kregen over de carrièremogelijkheden binnen de informatica achter bij de verwachtingen. De bevindingen zijn in lijn met de constructivistische leertheorieën (Valke, 2010) waar gesteld wordt dat nieuwe kennis vooral voortborduurt op al aanwezige kennis. Zo bleek dat bijv. de activiteiten rondom het binaire talstelsel beter verankerde dan andere activiteiten. Een van de aanbevelingen van de onderzoekers is dat de activiteiten beschreven moeten worden met in het achterhoofd een sterker bewustzijn van de aanwezige kennis van de studenten.

Om te achterhalen of het CSU programma in het Nederlandse onderwijs past, heb ik het CSU programma (Bell, Witten, Fellows, Adams & McKenzie, 2002) in tabelvorm vergeleken met het onderwijsprogramma voor informatica in Nederland (Schmidt, 2007). Zie de appendix 9.1.
Het CSU programma is geschikt voor het Nederlandse informatica onderwijs, maar niet alle domeinen van het examenprogramma worden afgedekt.

Keller, Scheuner, Serafini & Steffen (2011) hebben een cryptografie cursus voor het voortgezet onderwijs ontwikkeld. Deze cursus wordt gebruikt in het Zwitserse informatica onderwijs, juist als verbreding van het vak t.o.v. het (obligate) programmeren. Zij hebben de cursus een uitdagend karakter gegeven door het een tweestrijd te maken tussen de encrypter (de docent) en de codebrekers (de leerlingen). De cursus baseert zich expliciet niet op de onderliggende wiskunde.
In de cursus komen alleen de klassieke cryptografiesystemen aan bod.

Koblitz (1997) is een stap verder gegaan met zijn onderzoek naar public-key cryptografie voor het voortgezet onderwijs. Dit was de basis voor de CSU activiteit voor cryptografie (Bell, Thimbleby, Fellows, Witten, Koblitz & Powell (2003).

Keller, Komm, Serafini, Sprock and Steffen (2010) hebben vervolgens de effectiviteit van deze CSU activiteit in kaart gebracht.

Basisalgoritmes van public-key cryptografie zijn ontwikkeld door Bletchley Park (2004), Goebel (2010) en Kessler (2011). Deze algoritmes zijn eenvoudig in een programmeertaal (C, Java, Basic) om te zetten (of: de programmacode is eenvoudig te begrijpen als het kant-en-klaar aangeleverd wordt).

IZA is gebaseerd op de cognitivistische leertheorie: nieuwe kennis verankert het beste in het geheugen als er veel aanknopingspunten zijn om mee te associëren. Bovendien stimuleert IZA de volgende cognitivistische processen: waarnemen, herhalen, denken/reflecteren, problemen oplossen, herinneren en zich inbeelden (Valke, 2010).
De constructivistische leertheorie beschrijft dat nieuwe kennis wordt geconstrueerd boven op de bestaande kennis en gezichtspunten van de leerling (Ben-Ari, 2001). Als deze leertheorie gebruikt wordt bij evaluaties van uitgevoerde CSU lesactiviteiten, dan blijkt dat de CSU activities effectiever zouden zijn als zij expliciet de voorkennis van de leerling in acht nemen, en dat daarop voortgeborduurd wordt. (zie Taub, Ben-Ari & Armoni (2009), en Marcu, Kaufman, Kate Lee, Black, Dourish, Hayes & Richardson (2010)).

3 Onderzoeksvragen

Het doel van dit onderzoek is een voorbeeld module waarin informatica gedoceerd wordt zonder gebruik van een computer.
De verwachte opbrengst is dat er kennis opgedaan wordt of dit functioneert in het Nederlandse informatica onderwijs.

Op grond hiervan zijn de volgende onderzoeksvragen geformuleerd:
Hoofdvraag:

- Hoe functioneert een zelf samengestelde module IZA in het Nederlandse informatica onderwijs?

Nevenvragen:

- Welke kenmerken heeft dit materiaal? (o.a. werkvormen, aanwezigheid van metaforen)
- Kunnen leerlingen en docenten met dit materiaal overweg?
- Is er met IZA een efficiënte kennisoverdracht mogelijk?
- Levert het IZA model extra inzicht om de software die bij het onderwerp hoort te doorgronden?
- Wat zijn de praktische mogelijkheden voor dit onderwijs in Nederland (zoals: wat zijn de eisen rondom voorkennis (docent & leerling), voorbereidingstijd, ruimte in het curriculum)?

4 Methodes

4.1 Sample/respondents

Het onderzoek wordt uitgevoerd op de informatica klas VWO6 van het Lorentz Casimir Lyceum. De statistieken van deze klas:

- leerjaar 2011-2012
- 25 leerlingen
- 4 meisjes, 21 jongens
- profielen: 0 leerlingen Cultuur & Maatschappij, 10 leerlingen Economie & Maatschappij, 8 leerlingen Natuur & Gezondheid, 7 leerlingen Natuur & Techniek

4.2 Opzet

Het type van dit onderzoek is ontwerpgericht.
De opzet van het onderzoek kan op de volgende manier gestructureerd worden:

1. ontwerp van de module
2. uitvoering van de module
   dit behelst zes lessen in de klas, met de volgende onderverdeling:
   a. klasactiviteit: waarom hebben we cryptografie, welke facetten spelen een rol?
   b. vervolg klasactiviteit
   c. uitvoering van de CSU activity: tourist town
   d. uitvoering van de CSU activity: kid krypto
      in dit bronmateriaal bleek nog een fout te zitten, waarover gecommuniceerd is met de auteur, zie appendix 9.2.4
   e. uitvoering van de CIMT module: Public Key Cryptography
   f. implementeren van RSA met een programmeertaal (naar keuze)
3. meting van de module
   data collectie vindt plaats op de volgende wijze:
   a. schriftelijke enquête voorafgaand aan de interventie
   b. dezelfde schriftelijke enquête na afloop van de interventie
      het doel van deze enquêtes tezamen is om te meten of er kennisopbouw heeft plaatsgevonden
   c. observatie van de lessen door de docent
      het doel is om te meten of de leerlingen met het materiaal overweg kunnen, en om te meten of het IZA model inzicht verschaft om de software die bij het onderwerp hoort te doorgronden
   d. interview met enkele leerlingen na afloop van de interventie
      het doel is om te meten hoe het materiaal functioneert in het Nederlandse informatica onderwijs
   e. schriftelijke toets (als onderdeel van het schoolexamen)
      het doel is om te meten of er kennisopbouw heeft plaatsgevonden
4. analyse en evaluatie

Ad 2.: de CSU activiteiten worden aan de voorzijde en aan de achterzijde ondersteund. Hiervoor is gekozen vanwege de bevindingen van Taub, Ben-Ari & Armoni (2009). Om de inhoud van de CSU activiteiten te verankeren moet er net wat meer voorkennis aanwezig zijn, wat met de eerste twee lessen gerealiseerd wordt. En dit onderzoek wees uit dat niet altijd de koppeling gemaakt wordt tussen de CSU activiteit en de daadwerkelijke informatica technologie, wat in de laatste les aan de orde komt.
In appendix 9.2 is een uitgebreide beschrijving van de lesactiviteiten.

4.3 Instrumenten

De enquête is een lijst met statements met een 5-punts Likertschaal (Likert, 1932), in overeenstemming met de onderzoeken van Keller, Scheuner, Serafini & Steffen (2011), Lambert & Guiffre (2008), Carmichael (2008), Heersink & Moskal (2010), Marcu, Kaufman, Kate Lee, Black, Dourish, Hayes & Richardson (2010) en Taub, Ben-Ari & Armoni (2009).
Keller, Scheuner, Serafini & Steffen (2011) hebben een pre- en post-test gehouden bestaande uit vijf Likert vragen. Met Lucie Keller heb ik per e-mail contact gehad over de vragen in haar onderzoek. Op basis hiervan zijn mijn vragen grotendeels analoog opgezet.

De validiteit van mijn enquête is gebaseerd op de bevindingen van bovengenoemde ervaren onderzoekers die soortgelijke enquêtes afnemen. De betrouwbaarheid van mijn enquête staat onder druk omdat maar een kleine populatie deelneemt.

De vragenlijst:

	helemaal mee oneens	mee oneens	neutraal	mee eens	helemaal mee eens
ik weet wat cryptografie is	o	o	o	o	o
cryptografie vind ik interessant	o	o	o	o	o
cryptografie is belangrijk in het dagelijkse leven	o	o	o	o	o
iedereen moet kennis hebben van cryptografie	o	o	o	o	o
cryptografie is uitsluitend met wiskunde te begrijpen	o	o	o	o	o
versturen van encrypted boodschappen kan alleen als er *vooraf* geheime sleutels zijn uitgewisseld	o	o	o	o	o
ik weet dat je met https een veilige internetverbinding hebt	o	o	o	o	o
ik zorg voor een https verbinding bij vertrouwelijke internetcommunicatie	o	o	o	o	o
ik kan een computerprogramma	o	o	o	o	o

schrijven voor (eenvoudige) encryptie					

De observatie is in de vorm van een participerende observatie: ik verzorg de lessen, en observeer tegelijkertijd. De betrouwbaarheid staat onder druk omdat dit de eerste uitvoering van deze lessenserie is en omdat mijn hoofdtaak is om allereerst de les goed te laten verlopen. Bepaalde gebeurtenissen kunnen wellicht niet door mij waargenomen worden.
Als blijkt dat de lessen in een rustige sfeer hebben plaatsgevonden, dan is de observatie betrouwbaarder dan in een rumoerige lessfeer.
Het interview met leerlingen is een semi-gestructureerd interview, juist om de discussie te voeren over de aspecten die de deelnemers het belangrijkste achten (zie ook Marcu, Kaufman, Kate Lee, Black, Dourish, Hayes & Richardson, 2010).
Hoofdvragen van het interview zijn hoe ze de lessenopbouw vonden, en hoe de koppeling naar wiskunde en software ontwikkeling ervaren werd.
De validiteit staat onder druk als de leerlingen sociaal wenselijke antwoorden gaan geven, of als de omgeving niet neutraal is. Daarom worden de interviews tijdens de les gehouden (dan gaat het niet ten koste van hun vrije tijd), en worden geen incentives verstrekt (snoepgoed, of bonuspunten voor het examen).
Een typische duur van het interview is 30 minuten.

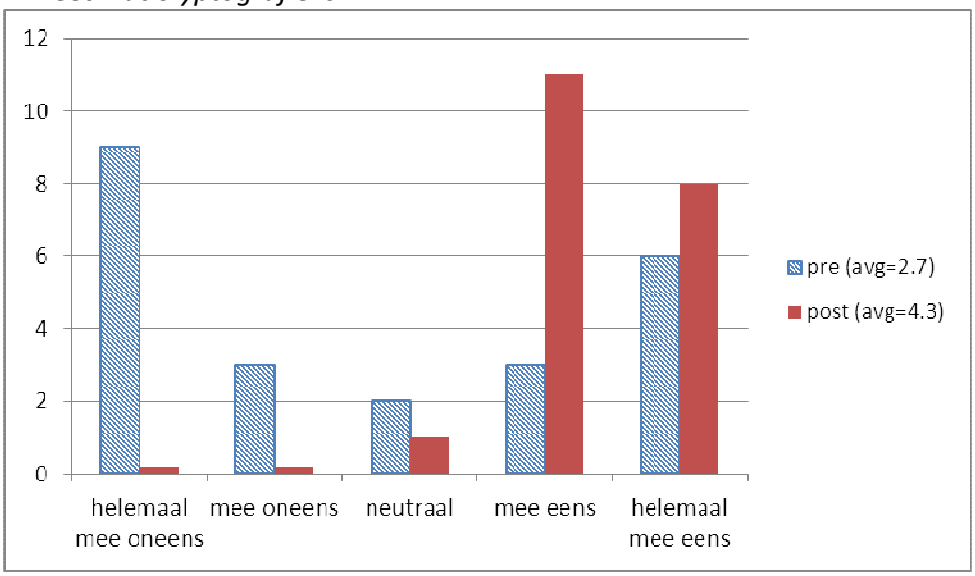
De schriftelijke toets is ontwikkeld op basis van het Stappenplan uit Vakdidactici Wiskunde (2011), en gereviewed door studenten van ESoE. Het uitgangspunt is een examen van 100 minuten met open vragen, waarbij een evenwichtige verdeling is tussen reproductie, toepassing en inzicht.
De validiteit en betrouwbaarheid van dit examen is verkregen door een review met een collega docent informatica op het Lorentz Casimir Lyceum.
De toets, de toetsmatrijs en de resultaten zijn in appendix 9.2.2 opgenomen.

5 Resultaten

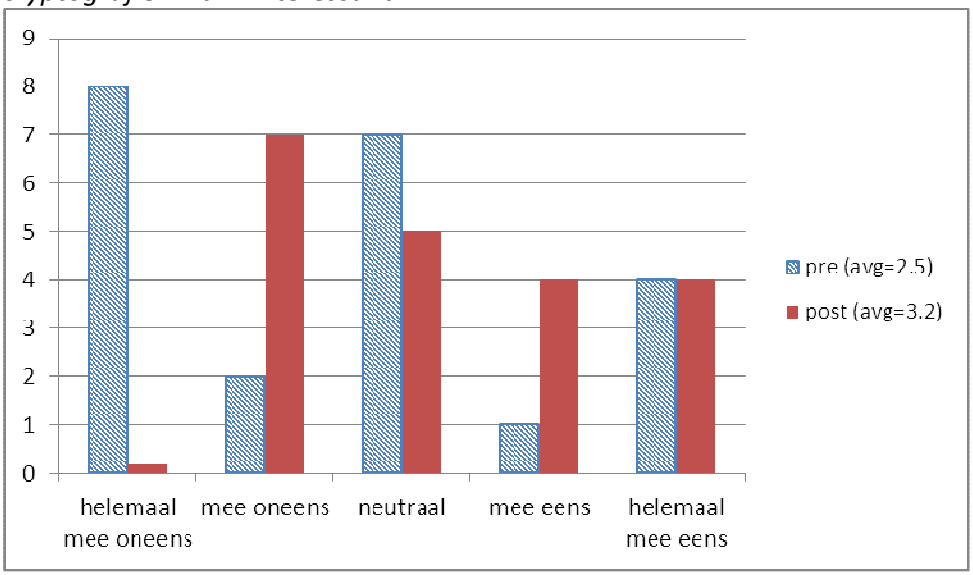
5.1 Schriftelijke enquête

De schriftelijke enquête is afgenomen op de dag direct voor de interventie (N=23), en op de dag direct na de interventie (N=20). Door ziekte was niet iedereen altijd aanwezig.
De uitslagen zijn verwerkt in een spreadsheet zodat grafieken gemaakt kunnen worden. In deze paragraaf wordt van elke vraag een grafiek getoond met daarin de antwoorden voor en na de interventie.
Tevens zijn de gemiddeldes uitgerekend per enquêtevraag. Als vereenvoudiging (van deze niet-numerieke schaal) is gekozen: helemaal mee oneens=1, mee oneens=2, neutraal=3, mee eens=4, helemaal mee eens=5.

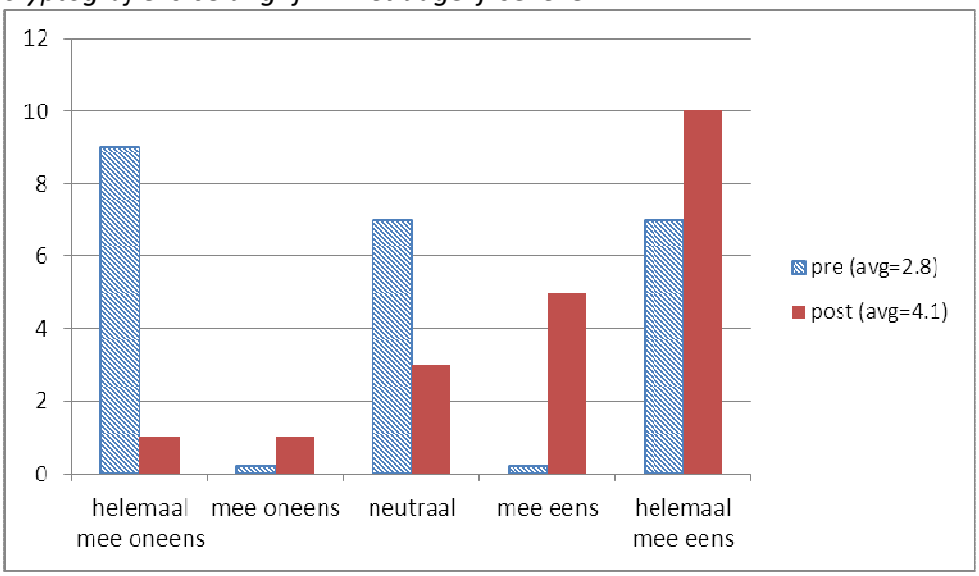
a. *ik weet wat cryptografie is*



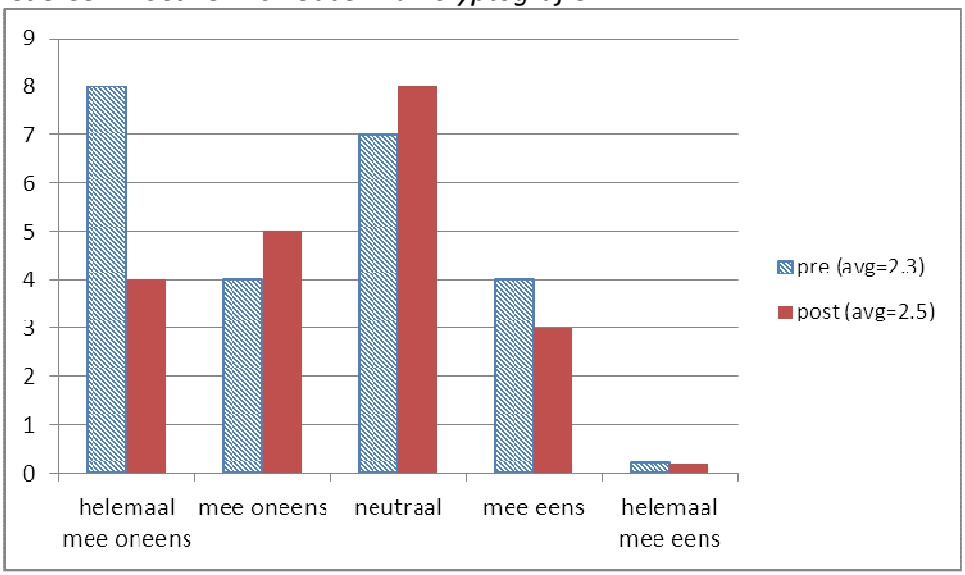
b. *cryptografie vind ik interessant*



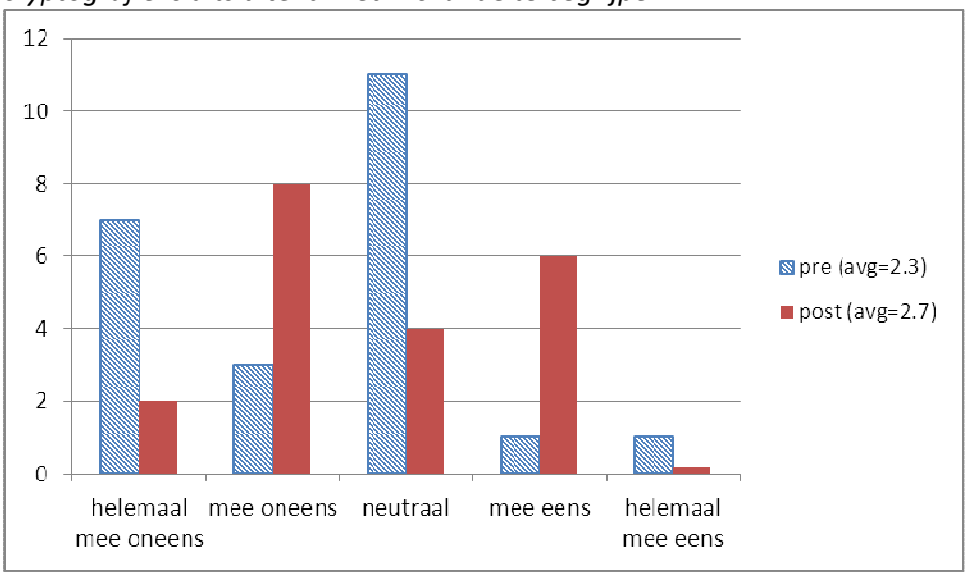
c. *cryptografie is belangrijk in het dagelijkse leven*



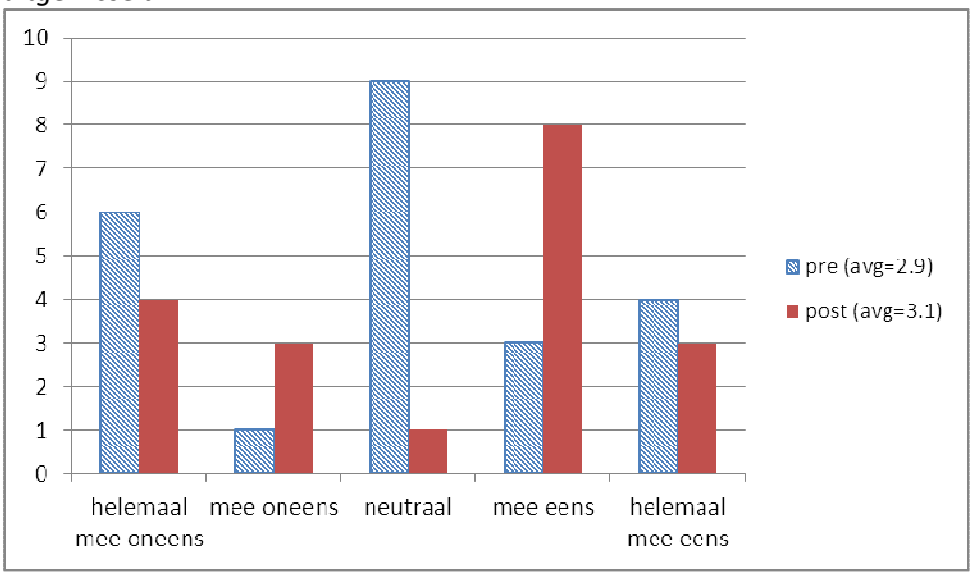
d. *iedereen moet kennis hebben van cryptografie*



e. *cryptografie is uitsluitend met wiskunde te begrijpen*



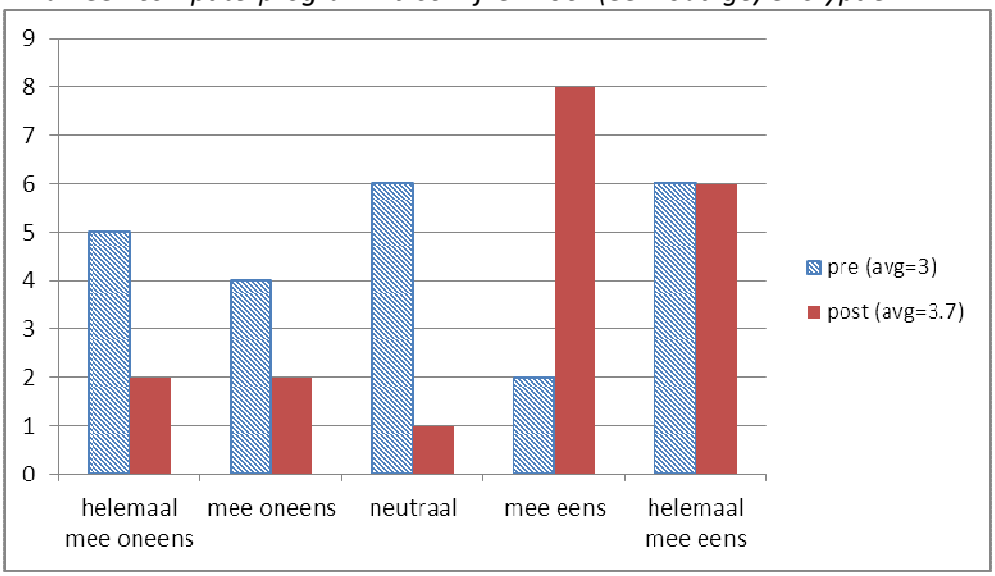
f. *versturen van encrypted boodschappen kan alleen als er vooraf geheime sleutels zijn uitgewisseld*



g. ~~*ik weet dat je met https een veilige internetverbinding hebt*~~
Vervallen omdat dit onderwerp niet in de interventie aan de orde is gekomen. Deze vraag is alleen gesteld in de enquête voorafgaand aan de interventie.

h. ~~*ik zorg voor een https verbinding bij vertrouwelijke internetcommunicatie*~~
Vervallen omdat dit onderwerp niet in de interventie aan de orde is gekomen. Deze vraag is alleen gesteld in de enquête voorafgaand aan de interventie.

i. ik kan een computerprogramma schrijven voor (eenvoudige) encryptie



5.2 Ooggetuigeverslag

Het ooggetuigeverslag is vanuit mijn eigen perspectief gemaakt. Direct na afloop van elk lesuur heb ik aantekeningen gemaakt, die als basis dienden voor dit verslag.
Alle lessen (behalve de laatste les) zijn gehouden in een regulier klaslokaal. Dit is bewust gedaan om los te koppelen van de computers.

5.2.1 lesuur 1

De klas is in drie groepen verdeeld, waarbij ik ervoor zorgde dat een meisje met een A ('Alice') in de linker groep zat, een jongen met een B ('Bob') in de rechter groep, en een jongen met een M ('Mallory') in de middelste groep. Zo kon ik consequent aan deze leerlingen refereren als ik een rol wilde aanduiden.
Ik heb een setting neergezet waarbij ik een actieve en kritische deelneming verwachtte, alsof het een universitair werkcollege betrof (over enkele maanden wordt dat voor hen de realiteit). Er was aan het begin nog duidelijk een afwachtende houding.
Ik had een scenario bedacht waarbij Mallory onderweg de boodschap zou wijzigen, waarbij ontvanger Bob dit niet zou bemerken. Pas na consultatie van verzendster Alice zou dit probleem aan het licht komen, waardoor vanuit de klas de wens tot authenticatie zou opborrelen. Maar de partijen waren er maar half bij met hun gedachten zodat ikzelf het authenticatie probleem moest openbaren.
De drie groepen hebben elk ca. 8 leerlingen; door die grote groepen is niet iedereen betrokken. Ondanks de initiële afwachtende houding wordt er (bij tijd en wijle) wel goed opgelet. Zo maakte ik een fout bij het decoderen van Vigenère en dat werd goed opgemerkt en juist gecorrigeerd door een leerling (juist iemand van wie ik een mindere inzet verwachtte).
Bij de Vigenère encoding hoopte ik dat de noodzaak voor een veilig kanaal zou opborrelen, maar groep-Alice en groep-Bob hadden met oogsignalen al een sleutel uitgewisseld zonder dat groep-Mallory het in de gaten had. Dat is op zich een nadeel dat je de regie niet super strak in handen hebt: de paden van het leerproces zullen dan anders lopen dan gedacht.

Er is altijd een strijd tussen 'de vaart in het verhaal houden' en 'de onderwerpen goed uitdiepen'. Mijn streven was om de vaart in het verhaal te houden; en als blijkt dat onderwerpen niet goed zijn aangekomen om die dan de dag erop bij de intro weer naar voren te halen.
Als cliffhanger naar de volgende les rekende ik voor dat voor symmetrische cryptografie wel erg veel sleutels nodig zijn en dat we daar wel wat aan willen doen. Dit kwam overeen met wat ik dacht dat behandeld zou kunnen worden in de les.

5.2.2 lesuur 2

De les begon met een herhaling van de stof van de vorige les. Uit de klas kwamen wel de goede antwoorden, dus samen weten ze het wel. Via het grote aantal sleutels kwamen we met een wensenlijst die public-key cryptografie kan bieden.
Dit is op een kwalitatieve manier besproken: 'er is een manier waarop het kan', waarbij ik de hoop uitsprak dat ze het enerzijds niet willen geloven, en dat ik ze anderzijds de volgende les kan overtuigen.
De uitleg over de hashfunctie heeft een te laag IZA gehalte; het is louter de theorie, en ik kreeg niet de indruk dat het goed aangekomen is. Er is een interactieve activiteit nodig om begrip te kweken.
Als klassenactiviteit moesten de groepen (van 4 leerlingen) een scenario uitwerken om berichten uit te wisselen met de drie kenmerken van cryptografie. Twee groepen gingen goed aan het werk; de andere vijf groepen deden eigenlijk helemaal niets; zelfs nauwelijks een poging. Persoonlijk de opdracht uiteenzetten en ze oppeppen werkte niet. Ik vertelde ze dat elke groep zijn oplossing op het bord moest zetten, maar dat werd niet als (extrinsieke) motivatie gezien. De twee serieuze groepen hadden een goede oplossing; de overige vijf groepen hadden niets.
Er was uiteindelijk geen tijd om HTTPS te behandelen; dat onderdeel is geschrapt uit de stof.

5.2.3 lesuur 3

Voor deze les had ik kopietjes gemaakt van bladzijde 149 van Bell, Alexander, Freeman & Grimley. (2009). Het oplossen van deze puzzel wordt beschreven als "*it is very hard to find the solution*", en: "*many groups will eventually give up*". Om de puzzel op te lossen zijn fiches nodig om op de knooppunten te leggen. Ik had M&M's gekocht. Dat is niet handig, want die rollen weg.
In groepjes van 2 gingen ze aan de slag. Binnen 5 minuten hadden 2 groepjes het al opgelost (van 1 groep had ik het wel verwacht; van de andere groep niet). Kort erna volgden andere groepen. Daarmee ging wel de hele boodschap van deze les verloren: "nagenoeg onmogelijk op te lossen behalve als je de achterdeur kent".
Hierna moesten de groepen zelf een kaart maken, deze doorschuiven, en de dan verkregen kaart oplossen. Dit verliep minder soepel dan verwacht om twee redenen: de kaart werd getekend op een klein stukje papier (op A4 is handiger) en de M&M's waren op.
Een leerling had al een algoritme bedacht hoe hij een willekeurige kaart zou kunnen oplossen (en daarmee alle NP-problemen dus ook kon oplossen). Helaas ging de theorie niet op bij een tweede kaart.
De actuele lesuitvoering was korter dan gepland.

5.2.4 lesuur 4

Omdat de kaart van bladzijde 149 in de vorige les zo snel was opgelost, besloot ik dat kaart 193 niet geschikt zou zijn voor deze les. Deze kaart zou waarschijnlijk ook snel gekraakt worden. Ik vreesde wel dat een grotere kaart een groter risico mee zou brengen inzake rekenfouten.
Klassikaal had ik de kaart van bladzijde 188 uitgelegd, uitsluitend het encoderen. Het decoderen heb ik bewust nog uitgesteld. Ik wilde hetzelfde effect bereiken als Keller et. al (2010): "*In the meantime, we demonstrate how easy the recipient can decrypt the message. We do this by decrypting the messages of the teams very fast and show them that we really found the corresponding plaintext. The students are usually very impressed how fast we can do that, as they have not been able to decrypt the given ciphertext, yet*". Maar door de grotere kaart werden er veel rekenfouten gemaakt, zodat mijn snelle antwoord niet in hun ogen het juiste antwoord was.
Hoewel deze activiteiten goed uitgevoerd werden, blijkt uit vragen vanuit de klas toch dat het totaalbeeld van public key cryptografie nog niet goed doorkomt. Het is niet duidelijk wat de activiteiten van Alice zijn, en van Bob, en wat er steeds overgestuurd wordt. Het is wel klassikaal verteld, maar er is geen kennis geconstrueerd bij de leerlingen.
De tijdsplanning kwam goed uit.

5.2.5 lesuur 5

Het principe van RSA uitgelegd, waarbij elke RSA stap gerelateerd werd aan de vorige les. Direct daarna heb ik een stencil uitgereikt waarmee de leerlingen zelf het RSA algoritme moesten uitrekenen. Het tweede gedeelte van het stencil bevatte opgaven waarvan de theorie nog niet besproken was, dit was bedoeld voor de snelleren. Maar die tekst bevatte blijkbaar net te weinig aanwijzingen om zelf de theorie te ontdekken.
Verder verwachtte ik dat sommigen er achter kwamen dat een combinatie E=3 en D=3 niet handig is (want dan is de sleutel al gekraakt).
De tijdsplanning kwam goed uit.

5.2.6 lesuur 6

Het hoofddoel van deze les was dat de leerlingen de afbeelding kunnen maken van de afgelopen lessen naar programmatuur. Maar om leerlingen met grote programmeeraversie niet de hele les te laten mokken had ik een alternatief bedacht: via Facebook moesten ze hun public key publiceren, en via Facebook moesten ze bij een ander een public key ophalen en die ander een gecodeerd bericht sturen. Dit bleek wonderbaarlijk goed te werken. Dit zette hen echt aan het denken hoe alle communicatiestromen liepen (dus: waar het in week 4 nog op vastliep). De les was te kort om echt heen en weer te communiceren.
Voor de groep die ging programmeren was de les ook te kort. De minder-ervarenen moesten toch hun programmeer-voorkennis weer activeren, en daarna moesten nieuwe programmaconstructies (zoals de modulo) geïmplementeerd worden.
Beide groepen zouden met een extra les een betere transfer realiseren.

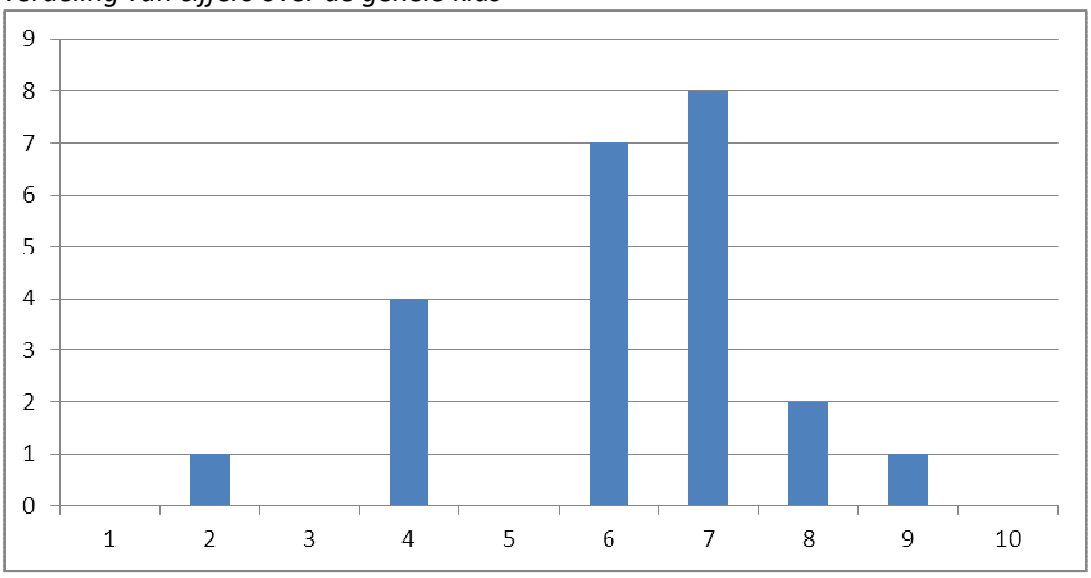
5.3 Interviews

Na afloop van de interventie zijn 8 leerlingen geïnterviewd. Het is een goede afspiegeling van de hele klas: 4 leerlingen met Maatschappij-profiel, en 4 leerlingen met Natuur-profiel; en: 2 meisjes en 6 jongens.
De interviews zijn semi-gestructureerd, juist om de discussie te voeren over de aspecten die de deelnemers het belangrijkste achten. Maar ik heb wel enige sturing uitgeoefend om het gesprek op gang te brengen en om enigszins in de buurt van mijn onderzoeksvragen te komen.
Alle leerlingen verklaren dat ze meer inzicht in cryptografie hebben gekregen.
Twee leerlingen vonden de praktijkopdrachten van de eerste les (proefondervindelijk de eisen van cryptografie ontdekken door het doorgeven van briefjes) verhelderend; voor de anderen had het niet gehoeven. Een leerling benoemde het als "een lage informatiedichtheid".
Bij de opdracht van de ijscokarretjes ervoeren de leerlingen geen duidelijke link met cryptografie; dat werd de les erop pas duidelijk. Het feit dat het kraken zo snel mogelijk was heeft hier aan bijgedragen.
Bij drie personen was de relatie van de ijscokarretjes met RSA niet duidelijk. Bij doorvragen voor verbeteringen gaf hij echter stappen die in mijn lesuitleg wel aanwezig waren.
De overgang van het RSA algoritme naar het programmeren was helder, alleen zouden ze meer tijd voor het programmeren willen hebben.
Kennis van de wiskunde werd niet belangrijk ervaren voor het begrip van cryptografie, maar wel voor de onderbouwing van de validatie.

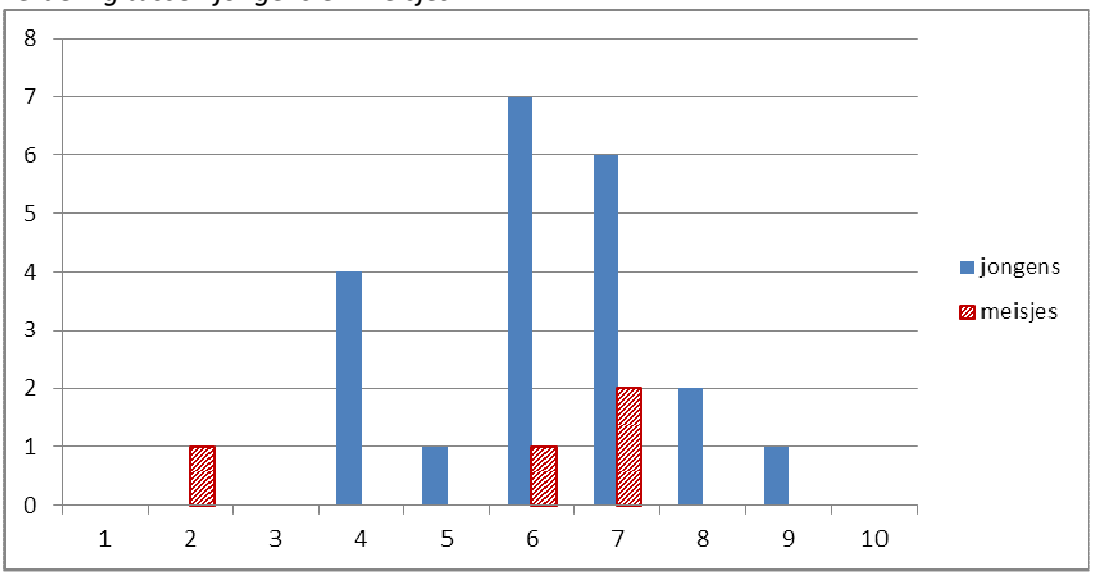
5.4 Schriftelijke toets

Het schoolexamen is gegeven op vrijdag 30 maart 2012.
De resultaten van de leerlingen zijn verwerkt in een spreadsheet waarmee de volgende tabellen zijn gegenereerd (N=23):

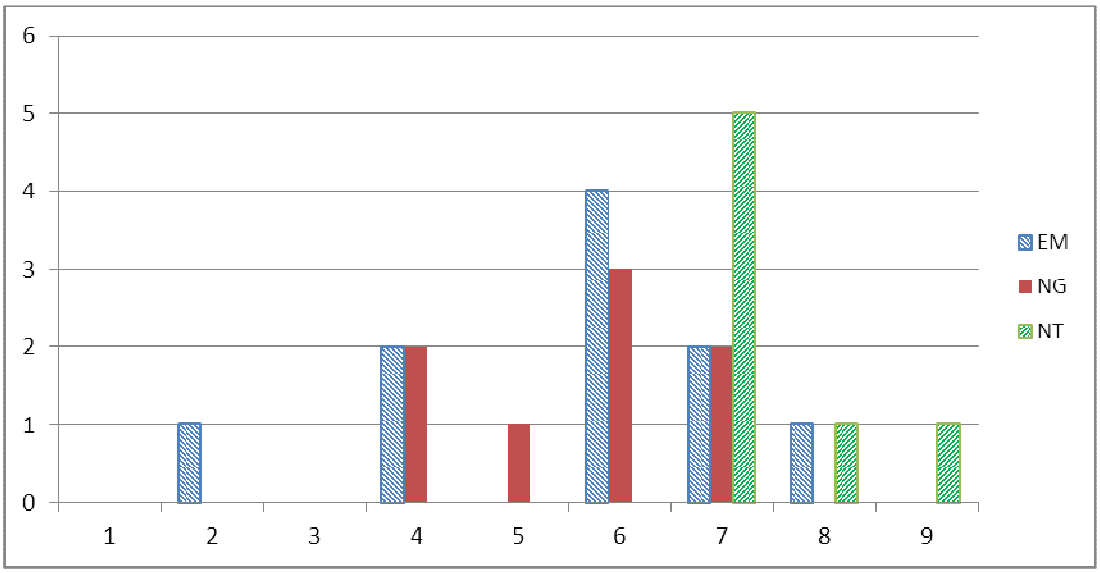
a. *verdeling van cijfers over de gehele klas*



b. *verdeling tussen jongens en meisjes*



c. *verdeling tussen de profielen Economie & Maatschappij, Natuur & Gezondheid, Natuur & Techniek*



6 Discussie

In dit hoofdstuk worden de onderzoeksvragen die gesteld zijn in hoofdstuk 3 beantwoord.

De samengestelde IZA module met cryptografie heeft gefunctioneerd in een Nederlandse VWO-6 klas. Dit is een reguliere klas op een reguliere school, zodat een voorzichtige conclusie getrokken kan worden dat het ook zal functioneren op andere scholen.
De nieuw te verwerven kennis sluit aan op de voorkennis, en de snelheid in de les sluit over het algemeen ook goed aan. Uit de interviews achteraf blijkt echter dat het voor sommigen te langzaam gaat, en dat sommigen de draad niet konden blijven volgen.

Het materiaal zit vol met metaforen, daar is IZA juist op gebaseerd. In de uitvoering zijn sommige zaken misgelopen (de metafoor van de one-way function was te snel te inverteren (het plaatsen van ijscokarretjes was snel voltooid), en de metafoor van het snel decoderen faalde door hoofdrekenfouten), maar die hebben geen nadelige invloed gehad op de over te brengen gedachte. Ik verwacht toch een sterkere impact van de lesstof als deze zaken wel goed verlopen.

Het is moeilijk te meten of een begrip van cryptografie zonder wiskunde goed mogelijk is. In de enquête voorafgaand aan de lessenserie had een grote groep een neutrale mening. In de enquête na afloop van de lessenserie is te zien dat deze groep in tweeën is gesplitst: de keuzes "mee oneens" en "mee eens" zijn sterk gestegen. Een aantal leerlingen vindt dat zij de wiskunde niet nodig hebben gehad, maar voor anderen wordt duidelijk dat wiskunde wel essentieel wordt om een stap verder in de cryptografie te maken (hier is wellicht de overgang van "onbewust onbekwaam" naar "bewust onbekwaam" gemaakt).

Het omzetten van de IZA manier van denken naar programmacode is geen triviale stap, vooral niet omdat de leerlingen (die weinig programmeerervaring hebben) in korte tijd hun programmeervoorkennis moesten activeren en de gewenste programmeerconstructies moesten bedenken. Leerlingen mochten nog een dag langer aan hun programma werken, en een aantal is er wel in geslaagd om een werkend programma te maken. De enquête wijst uit dat het vertrouwen van de leerlingen in het maken van een cryptografieprogramma wel gestegen is.

In zes lessen zijn de cruciale aspecten van moderne cryptografie aan de orde geweest. De enquête, het interview en het schoolexamen tonen aan dat het begrip van cryptografie en de interesse in cryptografie) significant gestegen zijn.
In de Handreiking Schoolexamen Informatica HAVO/VWO (Schmidt, 2007) wordt cryptografie niet expliciet genoemd. Maar het kan door scholen opgenomen worden in de domeinen A1 (Wetenschap en Technologie), A2 (Maatschappij) en C1 (Communicatie en Netwerken).
De huidige lessenserie is niet direct bruikbaar voor een volgende uitvoering. Diverse verbeteringen zijn nodig om een grotere effectiviteit te bereiken. Deze verbeterpunten zijn verzameld in appendix 9.2.2.

Het ware beter als er een parallelklas was waarbij het onderwerp op een klassieke wijze onderwezen zou worden, maar een dergelijke klas is niet voorhanden.
Het opdelen van de VWO6 klas in twee vergelijkbare groepjes is niet mogelijk vanwege de tijdsbelasting.
Anderzijds zou een VWO4, een HAVO4, een VWO5 of een HAVO5 klas als controlegroep kunnen functioneren. Maar deze klassen hebben een aanzienlijk andere achtergrond zodat resultaten niet met elkaar in verband gebracht kunnen worden.

Een lastig punt is een exacte definitie van IZA. De wens is om een IZA les zonder computers te kunnen uitvoeren, zonder voorbereidende lessen.

Daar zitten twee aspecten aan die lastig in een definitie te omvatten zijn: "zonder voorbereidende lessen" houdt in dat de voorkennis vanuit het dagelijks leven afdoende is, en die voorkennis groeit met de loop der jaren.
Eveneens is "zonder computers" een grijs gebied: de CSU activity Treasure Hunt kan bijvoorbeeld aantrekkelijker worden door het gebruik van GPS receivers, waarbij je het basis principe van de activity in tact laat. Dit is wat ik in mijn lessen ook bemerkte: het inzetten van Facebook om Public Keys te publiceren en om berichten te versturen vergroot het inzicht welke stappen door de partijen gedaan worden, en dat zij openbaar zijn (i.e. door iedereen te onderscheppen zijn). Maar in zo'n situatie ben je niet meer losgekoppeld van de computers. Ik neig naar de visie dat computers uitsluitend ingezet mogen worden als er geen krachtiger alternatief voor handen is (bijv. bij dit Facebook voorbeeld).
Maar er zijn nog meer grijze gebieden. Als oplossing voor de fouten bij het hoofdrekenen kan je een spreadsheetapplicatie maken waarbij de graaf in tabelvorm gerepresenteerd wordt. Alle optellingen kunnen zo automatisch (en foutloos) verricht worden. Hierbij vind ik ook dat we buiten de IZA definitie treden, al was het maar om een goed inzicht te krijgen in de onderliggende rekenvereisten voor encoderen, kraken en decoderen.

7 Voetnoten

(niet van toepassing)

8 Literatuur

Bell, T. (2000). A low-cost high-impact computer science show for family audiences. Australian Computer Science Conference, pp. 10-16

Bell, T., Alexander, J., Freeman, I. & Grimley, M. (2009). Computer Science Unplugged: school students doing real computing without computers. The NZ Journal of applied computing and information technology (Volume 13, Number 1), pp. 20-29

Bell, T., Curzon, P., Cutts, Q., Dagiene, V. & Haberman, B. (2011). Overcoming Obstacles to CS Education by Using Non-programming Outreach Programmes. Lecture Notes in Computer Science, Volume 7013/2011, pp. 71-81

Bell, T., Thimbleby, H., Fellows, M., Witten, I., Koblitz, N. & Powell, M. (2003). Explaining cryptographic systems. Computers & Education 40, pp. 199–215

Bell, T., Witten, I., Fellows, M., Adams, R. & McKenzie, J. (2002). Computer science unplugged : an enrichment and extension programme for primary-aged children. Canterbury

Ben-Ari, M. (2001). Constructivism in computer science education. Journal of Computers in Mathematics and Science Teaching, 20(1), 45-73

Bergin, J., Keleman, C., McNally, M., Naps, T., Goldweber, M., Power, C. & Hartley, S. (2000). Non-Programming Resources for an Introduction to CS. ITiCSE-WGR '00, pp. 89-100

Bletchley Park (2004). Public Key Cryptography. http://www.cimt.plymouth.ac.uk/resources/codes/default.htm

Carmichael, G. (2008). Girls, Computer Science, and Games. ACM SIGCSE Bulletin Volume 40 Issue 4, pp. 107-110

Cryptography (z.j.). Uit Wikipedia. Geraadpleegd Januari 2012. http://en.wikipedia.org/wiki/Cryptography

Cutts, Q., Brown, M., Kemp, L. & Matheson, C. (2007). Enthusing and informing potential computer science students and their teachers. ITiCSE '07 Proceedings of the 12th annual SIGCSE conference on Innovation and technology in computer science education, pp. 196-200

Fagin, R., Naor, M., Winkler & P. (1996). Comparing Information Without Leaking It. Communications of the ACM, Vol. 39, no. 5, pp. 77-85.

Goebel, G. (2010). Digital Ciphers & Public-Key Cryptography. Geraadpleegd januari 2012. http://www.vectorsite.net/ttcode.html

Heersink, D. & Moskal, B. (2010). Measuring high school students' attitudes toward computing. SIGCSE '10 Proceedings of the 41st ACM technical symposium on Computer science education, pp. 446-450

Keller, L., Komm, D., Serafini, G., Sprock, A. and Steffen, B. (2010). Teaching Public-Key Cryptography in School. Lecture Notes in Computer Science, 2010, Volume 5941/2010, pp. 112-123.

Keller, L., Scheuner, B., Serafini, G. & Steffen, B. (2011). A Short Introduction to Classical Cryptology as a Way to Motivate High School Students for Informatics. Lecture Notes in Computer Science, Volume 7013/2011, pp. 189-200

Kessler, G. (2011). An Overview of Cryptology. http://www.garykessler.net/library/crypto.html

Koblitz, N. (1997). CRYPTOGRAPHY AS A TEACHING TOOL. Cryptologia Volume 21, Issue 4, pp. 317-326

Lambert, L. & Guiffre, H. (2008). Computer Science Outreach in an Elementary School. Journal of Computing Sciences in Colleges Volume 24 Issue 3, pp. 118-124

Likert, R. (1932). A Technique for the Measurement of Attitudes. Archives of Psychology 140: pp. 1-55[1]

Marcu, G., Kaufman, S., Kate Lee, J., Black, R., Dourish, P., Hayes, G. & Richardson, D. (2010). SIGCSE '10 Proceedings of the 41st ACM technical symposium on Computer science education, pp. 234-238

Marks, J., Freeman, W. & Leitner, H. (2001). Teaching Applied Computing without Programming: A Case-Based Introductory Course for General Education. 32nd SIGCSE Technical Symposium on Computer Science Education, pp. 80-84

Schmidt, V. (2007). Handreiking schoolexamen informatica HAVO/VWO. Enschede: Stichting Leerplanontwikkeling (SLO)

Stienen, M., Bakker, H. (2008). Cryptografie. Commissie Toekomst Wiskunde Onderwijs. http://www.fi.uu.nl/ctwo/WiskundeD/MateriaalDomeinenWiskundeD/CryptografieVwo

Taub, R., Ben-Ari, M. & Armoni, M. (2009). The Effect of CS Unplugged on Middle-School Students' Views of CS. SIGCSE Bulletin 41 (3), pp. 99-103

United Nations (z.j.). Semi-structured Interview. Geraadpleegd januari 2012. http://www.fao.org/docrep/x5307e/x5307e08.htm.

Valke, M. (2010). Onderwijskunde als ontwerpwetenschap. Gent: Academia Press

Vakdidactici Wiskunde Technische Universiteiten (samenstellers). Handleiding Vakdidactiek Wiskunde (editie TU/e, 2011)

[1] vanwege de moeilijke beschikbaarheid van dit boek heb ik mij beperkt tot http://en.wikipedia.org/wiki/Likert_scale

9 Appendix

9.1 CSU vs. Handreiking Schoolexamen Informatica

In tabel 1 is een mapping gemaakt van de CSU activities op het Nederlandse informatica onderwijs. De rijen bevatten de CSU activities (in de benaming van CSU), en de kolommen bevatten de domeinen en subdomeinen van het Nederlandse informatica onderwijs (Schmidt, 2007). Een '1' in een cel geeft aan dat CSU activity past bij een subdomein.
Hier is te zien dat sommige subdomeinen niet bedekt worden door CSU. Dit betreft de subdomeinen a3, b4, c4 en c7.
Betreffende a3: CSU heeft geen expliciete activities die de studie en beroepsomgeving beschrijven, en onderzoek van Taub, Ben-Ari & Armoni (2009) wijst uit dat een volledige CSU cursus niet meer inzicht biedt.
Betreffende b4&c4: dit zijn lastige onderwerpen die niet zo snel in een paar lesuren goed te behandelen zijn. Ze vallen daarom buiten de scope van CSU.
Betreffende c7: databases zouden best op een CSU-achtige wijze geleerd kunnen worden. Het is niet duidelijk of dit onderwerp door de auteurs bewust gemeden is. Wellicht is dit een goede uitbreiding van CSU.

informatica onderwerp	*activiteit*	a1: wetenschap & technologie	a2: maatschappij	a3: studie & beroepsomgeving	a4: individu	b1: gegevensrepresentatie	b2: hardware	b3: software	b4: organisaties	c1: communicatie & netwerken	c2: besturingssystemen	c3: systemen in de praktijk	c4: informatiesysteemontwikkeling	c5: informatiestromen	c6: informatieanalyse	c7: relationele databases	c8: interactie mens-machine	c9: systeemontwikkeltraject	d: toepassingen in samenhang
representing information																			
binary numbers	count the dots					1	1			1	1								
image representation	colour by numbers					1				1									
text compression	you can say that again		1							1									
error detection	card flip magic					1				1									
information theory	20 guesses	1			1					1					1		1		
sound representation	sound unplugged		1							1									

algorithms																			
searching algorithms	battleships							1											
sorting algorithms	heaviest and lightest							1											
sorting networks	beating the clock							1						1					
minimal spanning tree	the muddy city	1																	
routing and deadlock	the orange game				1			1			1								
phylogenetics	phylogenetics unplugged	1	1									1		1	1				1
divide & conquer	santa's dirty socks							1											
procedures																			
finate state automata	treasure hunt				1			1						1	1		1		
programming languages	marching orders				1			1										1	
class simulation of a computer	-						1												
programming languages	harold the robot				1			1											
intractability																			
graph coloring	the poor cartographer							1							1				1
dominating sets	tourist town							1							1				1
steiner trees	ice roads							1		1					1				
cryptography																			
information hiding	sharing secrets	1						1											
cryptographic protocols	the peruvian coin flip	1																	
public key encryption	kid krypto	1						1											
interaction with computers																			
human interface design	the chocolate factory		1														1	1	1
the turing test	conversations with computers	1			1							1					1		
artificial intelligence	the intelligent piece of paper	1										1							

tabel 1: afbeelding van CSU activities op het Nederlandse informatica onderwijs

9.2 Interventies

9.2.1 Lesactiviteiten

Lesuur 1&2:
De klas wordt in drie groepen verdeeld, die elk in een eigen hoek van het lokaal gaan zitten. In de eerste groep zit een Alice, in de tweede groep zit een Mallory, en in de derde groep zit een Bob (vanwege de privacy worden gefingeerde namen gebruikt).
Het is belangrijk dat de leerlingen zelf de ontdekkingen doen, en dat de docent alleen de discussie in de goede banen leidt. Hier wordt in grote lijnen de uitkomst van de ontdekkingen gegeven. De onderlijnde woorden zijn kernbegrippen die gebruikt kunnen worden om het begrip van de leerlingen te toetsen.

Mallory stelt het grote-boze-internet voor, dus als Alice een boodschap naar Bob wil sturen, dan zal het via Mallory gaan. De eerste eis is geheimhouding: Mallory mag niet kunnen lezen wat de boodschap is.
Dit kan gerealiseerd worden via encryptie (http://nl.wikipedia.org/wiki/Encryptie), met een openbaar algoritme (http://nl.wikipedia.org/wiki/Algoritme) en geheime sleutels (http://nl.wikipedia.org/wiki/Sleutel_%28cryptografie%29).
De oorspronkelijke boodschap noemen we de plaintext, de encrypted boodschap noemen we de ciphertext.
De sleutels moeten via een veilig kanaal vervoerd worden. Dit betekent dat Alice en Bob elkaars identiteit kunnen valideren en dat de boodschap niet door Mallory gelezen kan worden.
Zomaar via internet versturen (dus als briefje door de klas) gaat dus niet. Wat wel mogelijk is: elkaar fysiek ontmoeten.

Een klassieke methode van encryptie: de Caesarrotatie (http://nl.wikipedia.org/wiki/Caesarcijfer). Hierbij wordt de ciphertext geconstrueerd door elke letter uit de plaintext een aantal posities op te schuiven. Het algoritme is *dat* er letters opgeschoven worden, de sleutel is *hoeveel* posities er geschoven wordt. Een sleutel van 3 betekent dat de A een D wordt, etc.

Caesar is makkelijk te kraken, bijvoorbeeld met frequentieanalyse (http://nl.wikipedia.org/wiki/Frequentieanalyse_%28cryptografie%29).
Een moeilijker systeem is Vigenère (http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer). De sleutel is een woord dat Alice zelf kan kiezen. De tabula recta wordt op de beamer getoond (of op papier uitgedeeld), en Alice en Bob kunnen een boodschap uitwisselen.
Ook hier geldt: de sleutel moet via een veilig kanaal zijn uitgewisseld.
Als de tekst lang genoeg is, dan kan de lengte van de sleutel met frequentieanalyse bepaald worden, en vervolgens de oorspronkelijke boodschap zelf.

Een andere manier om de ciphertext te kraken is brute force.
(http://nl.wikipedia.org/wiki/Brute_kracht)

Hoe veilig is dit als je het combineert met geheimzinnige teksten in contactadvertenties (en radioboodschappen in WOII)?
Geavanceerde symmetrische versleutelingen zijn DES (http://nl.wikipedia.org/wiki/Data_Encryption_Standard) en het verbeterde AES (http://nl.wikipedia.org/wiki/Advanced_Encryption_Standard).
Deze algoritmes worden niet besproken, dat gaat te ver.

Ook al kan Mallory de boodschap niet lezen, dan nog willen Alice en Bob niet dat Mallory de boodschap kan veranderen: er is een eis van integriteit (Alice en Bob zijn er zeker van dat de gegevens ongeschonden zijn).
Dit is vooral gewenst bij zakelijke en militaire transacties.
De tekst "er staan 100 tanks achter de heuvel" mag niet veranderen in "1000 tanks".

En Alice wil natuurlijk wel zeker weten dat de boodschap van Bob afkomstig is (en vise versa): er is een eis van authenticiteit. Jij wilt weten dat het niet de vijand is die een boodschap stuurt over het aantal tanks, en dat je echt met je eigen bank in contact staat.

Stel dat niet alleen Alice en Bob onderling willen communiceren, maar dat er veel meer mensen zijn. Bij n personen is er een uitwisseling van n*(n-1)/2 sleutels nodig. Dit is bij alle symmetrische versleutelingen (http://nl.wikipedia.org/wiki/Symmetrische_cryptografie).
Een oplossing voor de integriteit, de authenticiteit en de grote hoeveelheid sleutels is asymmetrische versleuteling (http://nl.wikipedia.org/wiki/Asymmetrische_cryptografie): iedere persoon heeft twee sleutels: een public key (http://nl.wikipedia.org/wiki/Publieke_sleutel) (die openbaar is) en een private key (http://nl.wikipedia.org/wiki/Geheime_sleutel)

Scenario's:
Als Alice een boodschap naar Bob wil sturen:

- Alice neemt een private key en een bijbehorende public key
- Alice publiceert haar public key (en houdt haar private key geheim)
- Alice versleutelt haar boodschap ('hallo') met haar *private key*, de ciphertext is dan bijv. 'wdoinz9', en stuurt het op
- Bob decrypt deze ciphertext ('wdoinz9') met de *public key van Alice*, en dat levert de plaintext 'hallo' op.
- Let op: Mallory kent de public key van Alice, en kent de ciphertext 'wdoinz9', maar kan met deze informatie niet de plaintext 'hallo' construeren.

Als Bob een bericht terug wil sturen:

- Bob encrypt zijn plaintext ('tot ziens') met de *public key van Alice*, en dat levert (bijv.) de ciphertext '&^jkq{}AHW' op.
- Alice decrypt de ciphertext ('&^jkq{}AHW ') met haar *private key*, en zij verkrijgt daarmee de plaintext 'tot ziens'
- Let op: ook hier Mallory kent de public key van Alice, en de ciphertext, maar kan met deze informatie niet de plaintext construeren.

RSA (http://nl.wikipedia.org/wiki/RSA_%28cryptografie%29) is een voorbeeld van asymmetrische versleuteling. Bij n personen is er een uitwisseling van n (publieke) sleutels nodig. Deze sleutels hoeven bovendien niet persoonlijk overhandigd te worden, maar kunnen gewoon via internet gepubliceerd worden.

Hoe realiseren we integriteit?
Manieren om klassikaal uit te voeren: (van eenvoudig naar complex) (a) tel het aantal letters, of (b) tel de ASCII waarde van de letters op, of (d) schuif alle getallen een plekje op (x10, of x2) voor de optelling.
Dit getal is de digitale handtekening. (http://nl.wikipedia.org/wiki/Digitale_handtekening)
Bij bovenstaande voorbeelden is het gemakkelijk om de brontekst te wijzigen zonder dat de handtekening verandert. Dat is niet wenselijk want zo kan Mallory de inhoud van het bericht van Alice aanpassen zonder dat Bob het in de gaten heeft.
Een hashfunctie (http://en.wikipedia.org/wiki/Cryptographic_hash_function) is een algoritme om wel een goede digitale handtekening te maken: de hashfunctie produceert een getal uit de brontekst, waarbij het welhaast onmogelijk is om na het wijzigen van de tekst hetzelfde getal te verkrijgen.
MD5 is een voorbeeld (http://en.wikipedia.org/wiki/Md5#MD5_hashes).

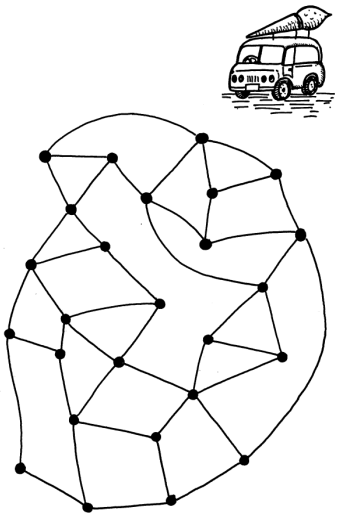
Vraag aan het publiek: hoe kan Alice nu een boodschap naar Bob sturen zodat Bob weet dat het zeker van Alice afkomstig is (authenticiteit), en dat de boodschap onveranderd is (integriteit)?
Oplossing:
Alice encrypt de plaintext met Bobs public key, en stuurt naast deze ciphertext ook de versleutelde waarde van de handtekening van de plaintext (versleuteld met haar private key);
Bob herhaalt de stappen op zijn locatie: hij decrypt de ciphertext (met zijn private key), berekent de handtekening van deze plaintext, en vergelijkt dit met de decrypted handtekening (decrypted met Alice' public key). Als gevolg hiervan: Alice kan niet meer ontkennen dat ze het bericht verstuurd heeft (onweerlegbaarheid).

Verschil tussen symmetrische en asymmetrische versleuteling: moeilijk sleutelmanagement bij symmetrische versleuteling, en rekenintensieve versleuteling bij asymmetrische versleuteling.
Verschil tussen encryption en de hashfunctie: de hashfunctie moet een kort antwoord opleveren en moet niet omkeerbaar zijn (een one-way function (http://en.wikipedia.org/wiki/One-way_function)); encryption: moet wel omkeerbaar zijn, maar uitsluitend als je in het bezit van de sleutel bent (een one-way function with trapdoor (http://en.wikipedia.org/wiki/Trapdoor_one-way_function)).

HTTPS (http://nl.wikipedia.org/wiki/HTTPS, http://en.wikipedia.org/wiki/HTTPS) is HTTP communicatie tussen server en client, waarbij alle data encrypted is. Een client kan bij een Certificate Authority (CA) (http://en.wikipedia.org/wiki/Certificate_authorities) een certificaat van de server opvragen. In dit certificaat zit o.a. de public key van de server.
De gebruiker moet wel vertrouwen hebben in de CA en in zijn browser.

HTTPS is gebaseerd op asymmetrische en symmetrische versleuteling. In het begin worden symmetrische keys uitgewisseld via asymmetrische encryption. Vervolgens kan alle verkeer symmetrisch encrypted worden (hetgeen minder rekenkracht vergt).

Lesuur 3:
http://csunplugged.org/sites/default/files/activity_pdfs_full/unplugged-14-dominating_sets_0.pdf
Doel van de les: begrip van one-way functions zonder wiskunde. De opdracht luidt (in het kort): zet de ijscokarretjes strategisch op enkele kruispunten zodat elk andere kruispunt verbonden is met (precies) een ijscokarretjeskruispunt. Dit is een ondoenlijke zaak om op te lossen, tenzij je zelf de kaart gemaakt hebt door eerst de ijscokarretjes + belendende knooppunten te plaatsen, en door daarna verbindingslijnen te trekken. Zie de tekening hiernaast:



Lesuur 4:
http://csunplugged.org/sites/default/files/activity_pdfs_full/unplugged-18-public_key_encryption_0.pdf
Doel van de les: public key versleuteling zonder wiskunde. De opdracht luidt (in het kort): zet op elk knooppunt een getal, zodanig dat de som hiervan het te coderen getal voorstelt. In een tweede stap: zet per knooppunt de som van het getal op dit knooppunt en de belendende knooppunten. Deze laatste getallen worden openbaar verstuurd. De ontvanger (en alleen hij) weer het oorspronkelijke getal te reconstrueren, omdat hij de enige is die weet hoe de ijscokarretjes strategisch op de kaart gezet moeten zijn.

Lesuur 5:
Doel van de les: het RSA algoritme met pen en papier uitvoeren (Public Key Cryptography op http://www.cimt.plymouth.ac.uk/resources/codes/default.htm).
De opdracht in het kort: bepaal de *E*, *D* en *m* uit twee priemgetallen *p* en *q*. Encodeer X via X^E mod *m*, en decodeer Y via Y^D mod *m*.

Lesuur 6:
RSA implementeren in een programmeertaal (Basic, Java, JavaScript, etc.), of: met een aangeleverde RSA implementatie (in RobotBasic) de encryptie/decryptie van een stuk tekst verzorgen.

Om na afloop uit te delen aan de leerlingen als samenvatting van de lesstof, en als voorbereiding op het examen:

Terminologie
geheimhouding
integriteit
authenticiteit

encryptie (http://nl.wikipedia.org/wiki/Encryptie)
algoritme (http://nl.wikipedia.org/wiki/Algoritme)
sleutels (http://nl.wikipedia.org/wiki/Sleutel_%28cryptografie%29)
veilig kanaal
Caesarrotatie (http://nl.wikipedia.org/wiki/Caesarcijfer)
frequentieanalyse (http://nl.wikipedia.org/wiki/Frequentieanalyse_%28cryptografie%29)
Vigenère (http://nl.wikipedia.org/wiki/Vigen%C3%A8recijfer)
brute force (http://nl.wikipedia.org/wiki/Brute_kracht)
DES (http://nl.wikipedia.org/wiki/Data_Encryption_Standard)
AES (http://nl.wikipedia.org/wiki/Advanced_Encryption_Standard)
n*(n-1)/2 sleutels
symmetrische versleutelingen (http://nl.wikipedia.org/wiki/Symmetrische_cryptografie)
asymmetrische versleuteling (http://nl.wikipedia.org/wiki/Asymmetrische_cryptografie)
public key (http://nl.wikipedia.org/wiki/Publieke_sleutel)
private key (http://nl.wikipedia.org/wiki/Geheime_sleutel)
RSA (http://nl.wikipedia.org/wiki/RSA_%28cryptografie%29)
n (publieke sleutels)
digitale handtekening. (http://nl.wikipedia.org/wiki/Digitale_handtekening)
hashfunctie (http://en.wikipedia.org/wiki/Cryptographic_hash_function)
MD5 (http://en.wikipedia.org/wiki/Md5#MD5_hashes)
onweerlegbaarheid
one-way function (http://en.wikipedia.org/wiki/One-way_function)
one-way function with trapdoor (http://en.wikipedia.org/wiki/Trapdoor_one-way_function)
HTTPS (http://nl.wikipedia.org/wiki/HTTPS, http://en.wikipedia.org/wiki/HTTPS)
CA (http://en.wikipedia.org/wiki/Certificate_authorities)

Lessen

http://csunplugged.org/sites/default/files/activity_pdfs_full/unplugged-14-dominating_sets_0.pdf
http://csunplugged.org/sites/default/files/activity_pdfs_full/unplugged-18-public_key_encryption_0.pdf
http://www.cimt.plymouth.ac.uk/resources/codes/codes_u10_text.pdf

Online tools

http://web.forret.com/tools/rot13.asp
http://www.counton.org/explorer/codebreaking/vigenere-cipher.php
http://sharkysoft.com/misc/vigenere/
http://people.eku.edu/styere/Encrypt/RSAdemo.html (nadeel: je kan niet je eigen priemgetallen kiezen)
http://www.r-krell.de/if-k-rsaapplet.htm
http://www.jensign.com/JavaScience/www/messagedigestj2/index.html

9.2.2 Verbeterpunten voor de lessen

In deze paragraaf wordt een aantal verbeterpunten gegeven die zijn waargenomen tijdens de uitvoering van de lessen.

les 1:

- een situatie ensceneren waarvoor daadwerkelijk cryptografie vereist is.
- meer tijd inruimen om te verduidelijken dat de sleutel via een veilig kanaal uitgewisseld moet worden.
- meer tijd inruimen voor Vigenère (alle aspecten: encoderen, decoderen, en kraken)
- kleinere groepen zodat iedereen wel betrokken kan zijn

les 2:

- een goede IZA voor hashfuncties

les 3:

- een kaart die werkelijk moeilijk is om op te lossen
- gebruik van (platte) Smarties, in plaats van (ronde) M&M's

les 4:

- een kaart die moeilijk is om op te lossen, maar die wel weinig punten heeft, zodat er weinig kans is op hoofdrekenfouten.
- de leerlingen zelf de communicatiestromen laten ervaren (bijvoorbeeld: de Facebook methode van week 6)

les 5:

- verruiming van uitleg van het uitdeelpapier, zodat snelle leerlingen zelf de verkorte methode van machtsverheffen kunnen uitvoeren.
- omlijsten met echte nieuwsartikelen over de geldelijke waarde van grote priemgetallen

les 6:

- meer tijd voor het programmeren (minstens 2 lesuren)
- meer tijd voor Facebook uitwisselingen (het plaatsen van je eigen Public Key, en het verzenden van gecodeerde berichten naar anderen)

9.2.3 Uitbreidingsmogelijkheden

Indien gewenst kan de lessenserie uitgebreid worden. De volgende onderwerpen sluiten goed aan:

- Aandacht voor de achterliggende wiskunde (zie Stienen & Bakker, 2008)
  Hierin worden de bewijzen uitgewerkt van het RSA algoritme. Officieel zou je dit IZA kunnen noemen (er worden geen computers gebruikt, noch wordt er specifieke wiskunde voorkennis vereist (behalve het begrip priemgetal))
- Aandacht voor Zero-knowledge Proof (zie Fagin, Naor & Winkler, 1996)
  Zero-knowledge Proof is het bewijzen van een uitspraak zonder de details van die uitspraak te onthullen. Dit artikel geeft een aantal IZA methoden.

De lessenserie zou ook uitgevoerd kunnen worden in twee parallelklassen, waarbij de ene klas op traditionele manier les krijgt, en de andere klas met IZA methode. Hiermee wordt een beter inzicht verkregen in hoeverre IZA echt helpt bij de kennisvergaring.

9.2.4 Verbeteringen voor het CSU materiaal

In het materiaal van Computer Science Unplugged (Bell et al., 2002) zat een fout in de tekening van de dominating sets. De dag voorafgaand aan mijn les heb ik deze ontdekt en aan Professor Timothy Bell (University of Canterbury, New Zealand) gemaild. De tien uren tijdsverschil zouden nu juist gunstig moeten zijn, maar Tim zat in een conferentie. Ik heb zelf een aanpassing gemaakt, zie figuur 1:

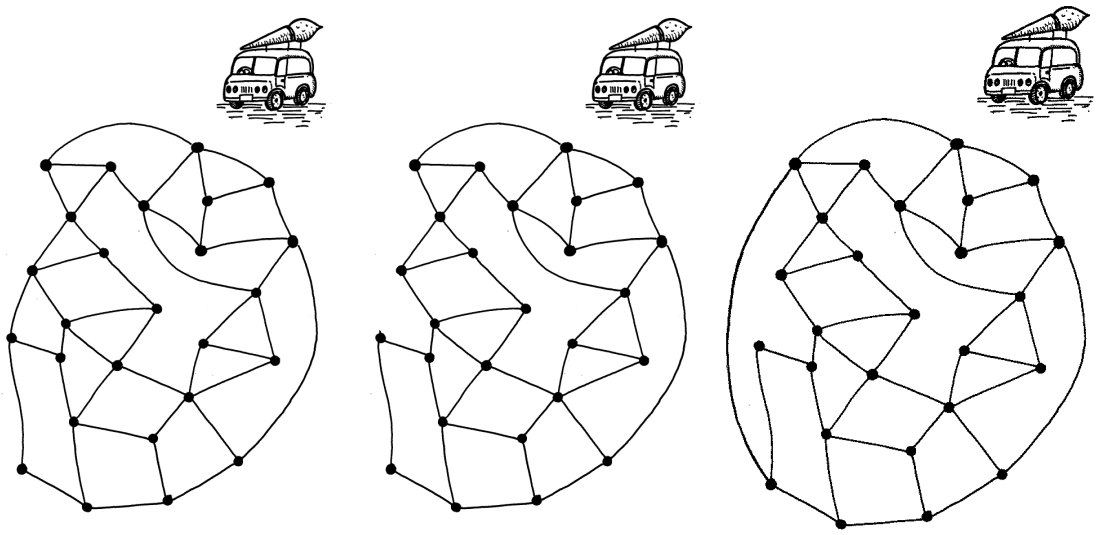


figure 1: drie varianten van de Tourist Town map; links: de orginele versie, midden: de versie zoals gebruikt in mijn les; rechts: de versie zoals nu aangeboden op Computer Science Unplugged

Met Tim heb ik ook mijn ervaringen gedeeld betreffende het snelle oplossen van de Tourist Town, en de rekenfouten bij Kids Krypto. Tim zei me dat de activities eigenlijk voor een iets jongere doelgroep bedoeld waren. De (New Zeelandse) doelgroepaanduiding in het lesmateriaal was "Junior High and up", en ik heb me vooraf niet intensief genoeg bezig gehouden met de schoolniveauaanduidingen in alle landen.
Ook beaamt hij het risico van rekenfouten, en heeft hij een extra notitie voor docenten aan het lesmateriaal toegevoegd.

9.3 Schoolexamen

Het schoolexamen is ontwikkeld volgens de Handleiding Vakdidactiek Wiskunde (Vakdidactici Wiskunde (2011)).

9.3.1 Leerdoelen

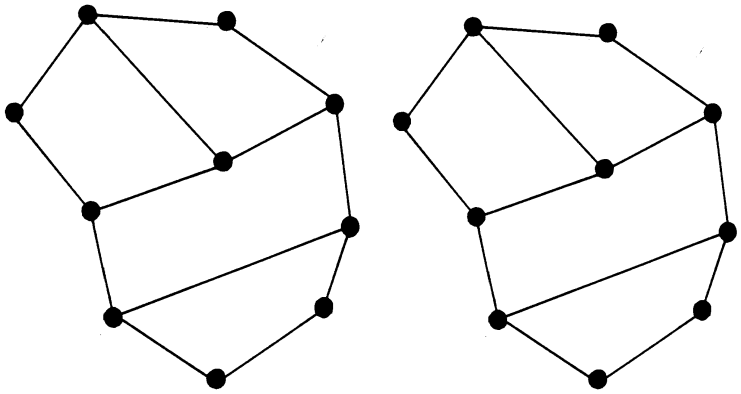
De volgende leerdoelen worden getoetst:

1. De leerling weet wat cryptografie is
2. De leerling weet wat het belang van cryptografie is
3. De leerling kent de karakteristieken van de belangrijkste cryptografie methoden
4. De leerling kan cryptografie technieken toepassen

9.3.2 Opgaven

Het examen bevatte de volgende vragen:

1. (4p) Wat zijn de belangrijkste drie eisen van cryptografie?
   Leg uit wat er mee bedoeld wordt.
2. (3p) Geef drie voorbeelden uit het dagelijks leven waarbij cryptografie onmisbaar is.
   Leg uit wat er verandert als er geen cryptografie zou zijn.
3. (3p) Beschrijf welke handelingen twee personen (bijvoorbeeld Alice en Bob) moeten ondernemen om met behulp van symmetrische cryptografie boodschappen uit te wisselen.
4. (3p) Wat zijn nadelen van symmetrische cryptografie ten opzichte van asymmetrische cryptografie?
5. (2p) Wat is een brute force attack?
6. (1p) Noem de namen van twee symmetrische versleutelingen die tegenwoordig veel gebruikt worden.
7. (3p) Op het tweede vel papier staat de Vigenère tabel.
   Versleutel de eerste zes letters van je eigen voornaam (+ event. achternaam), met 'BLOEM' als sleutel.
8. (3p) Je ontvangt het versleutelde Vigenère bericht 'ZBFQNMNASV', waarbij 'LORENTZ' de sleutel is.
   Wat is de oorspronkelijke boodschap?
9. (3p) Op de allerlaatste bladzijde staat de Public Map van Alice. Encodeer in die map het getal 35 om het naar haar te versturen. De linker afbeelding kan je als kladblad beschouwen, de rechter afbeelding als definitieve versie.
   Lever het blad in.



10. (5p) Construeer een Private Map voor Bob (methode 'ijscokarretjes', met in totaal ca. 10 stippen, maar niet gelijk aan bovengenoemde tekening), en maak de bijbehorende Public Map.
    Beschrijf wat Bob moet doen als hij een geëncodeerde boodschap ontvangt (je kunt een voorbeeld geven)
11. (6p) Gegeven zijn de priemgetallen 3 en 11.
    Construeer een Public Key en een Private Key.
    Neem E = 3 (om het rekenwerk te vergemakkelijken)
    Beschrijf hoe je deze keys hebt berekend.
    We gebruiken de volgende omzetting van letters naar getallen (en omgekeerd): A→1, B→2 (zie de tabel op het tweede vel).
    Encodeer het woord TOP
    Decodeer de boodschap 16 – 26 – 4. Welk woord is dit?
12. (3p) Het blijkt dat encoderen en decoderen van boodschappen met Public Key cryptografie aanzienlijk meer rekentijd van de computer kost dan met symmetrische cryptografie.
    Bedenk een methode zodat Alice en Bob toch boodschappen kunnen uitwisselen met de voordelen van Public Key cryptografie en de voordelen van symmetrische cryptografie.
    Beschrijf je methode.
13. (3p) In de Middeleeuwen leefden freule Beatrice en graaf Adelbrecht ver uit elkaar. Zij houden niet van reizen.
    Zij hebben de beschikking over een gemeenschappelijke kist (van degelijke kwaliteit), en ze hebben hangsloten om de kist mee af te sluiten. Van elk hangslot is maar 1 sleuteltje beschikbaar. Als er hangsloten aan de kist zitten, dan kan de kist niet geopend worden (ook niet door kwaadwillenden).
    Beschrijf een methode hoe Beatrice en Adelbrecht op een handige manier boodschappen kunnen uitwisselen die niet onderschept kunnen worden.

9.3.3 Toetsmatrijs

Op basis van de leerdoelen en de examenvragen is de volgende toetsmatrijs gemaakt (de cijfers in de cellen geven het aantal te behalen punten per vraag weer). Zo wordt gevalideerd dat de verhouding reproductie/productie in lijn is met het schooltype (voor VWO moet dat rond de 33%/67% liggen), en dat alle doelen aan de orde komen. Vraag 12 en vraag 13 zijn

inzichtvragen, die vanwege het format van deze toetsmatrijs in de categorie productie geplaatst zijn.

	reproductie				productie				
opgave	doel 1	doel 2	doel 3	doel 4	doel 1	doel 2	doel 3	doel 4	
1	4								
2						3			
3			3						
4			3						
5	2								
6	1								
7								3	
8								3	
9								4	
10								5	
11								5	
12					3				
13					3				
totaal punten:	7	0	6	0	6	3	0	20	42
percentage:	17	0	14	0	14	7	0	48	

per doel	doel 1	doel 2	doel 3	doel 4
(repro+pro samen)	31%	7%	14%	48%

reproductie: 31%
productie: 69%