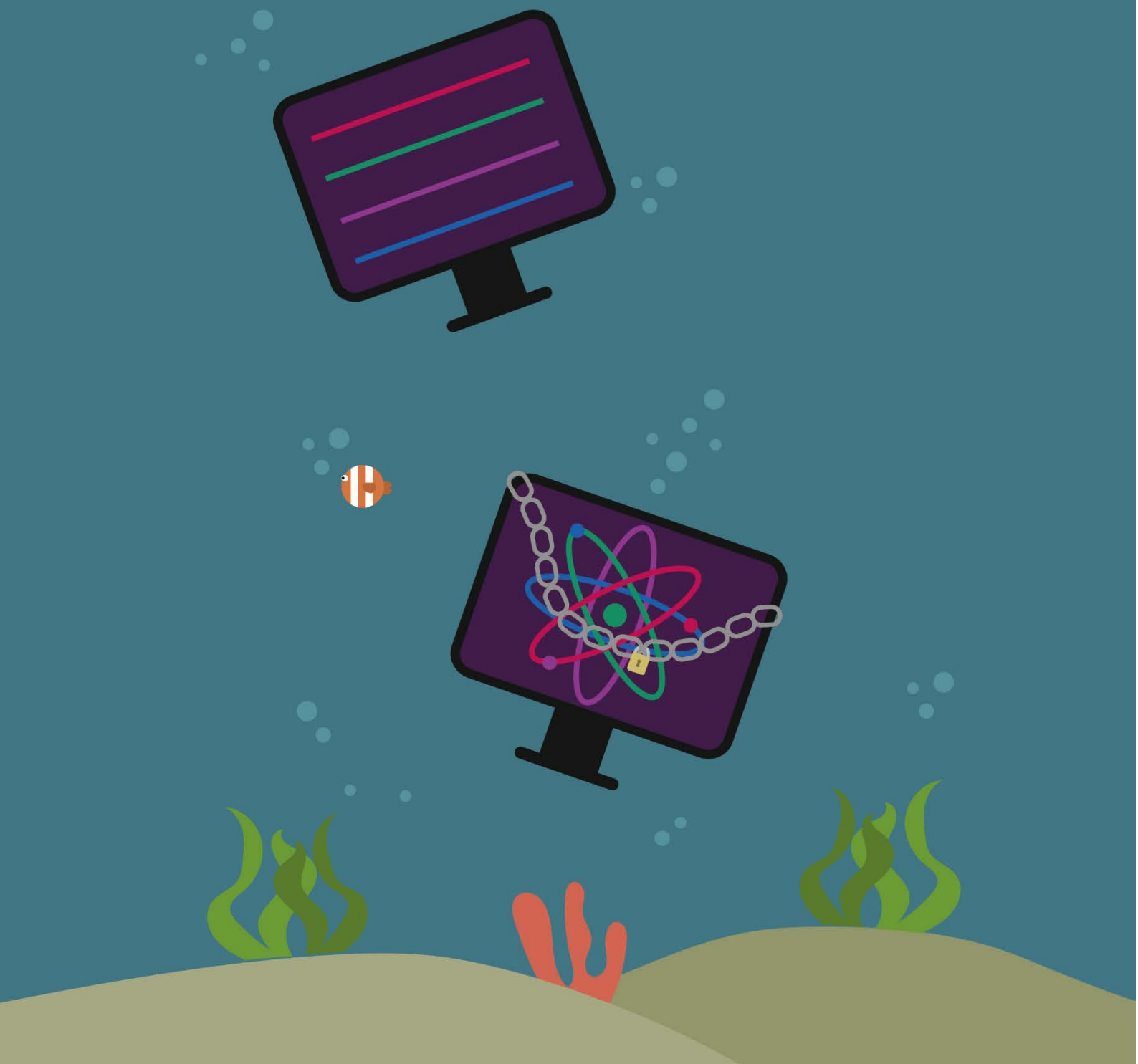
QuantumKeuzes

Deze lessen zijn ontwikkeld in samenwerking tussen
het **Quantum Rules! Lab** en **De Denkschool**



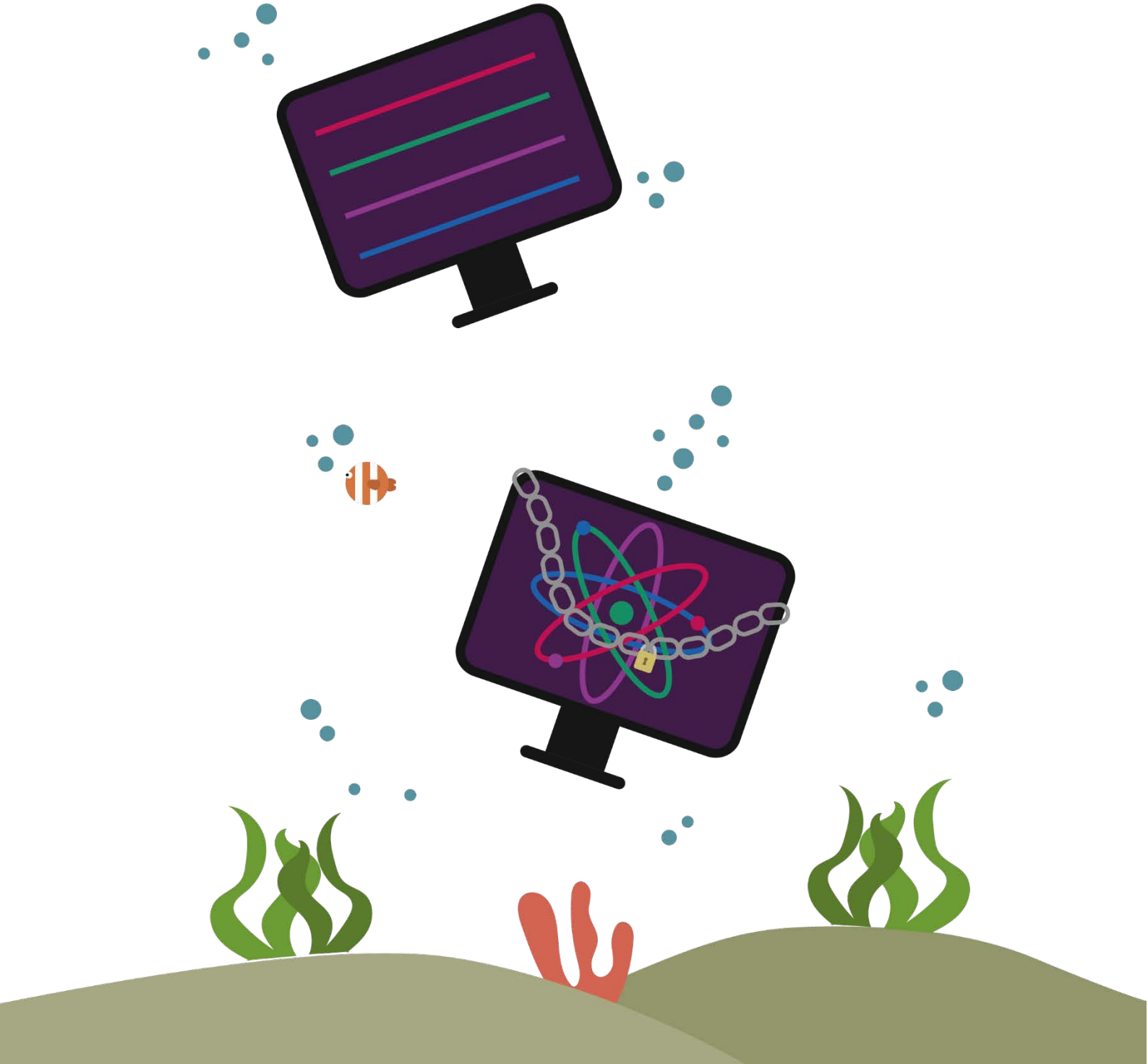
Colofon

Deze lesmodule is ontwikkeld in een samenwerking tussen het Quantum Rules! Lab en de filosofen van De Denkschool, met financiering van het Quantum Delta NL groeifonds.
Het doel van de module is om gesprekken over (quantum)technologie te voeren in de onderbouw van het voortgezet onderwijs, om leerlingen kennis te laten maken met quantum, ze voor te bereiden op toekomstige uitdagingen en te oefenen met burgerschapsvaardigheden.

De module is ontwikkeld door:
- Mirjam Poolster (Verhaal en redactie)
- Werner van Rossum (Stencils en redactie)
- Caroline van Twillert (Handleiding en redactie)

Verder werkten mee:
- Tessa (illustraties)
- Michiel Thijssen (redactie)

Docentenhandleiding



Docentenhandleiding

Voorwoord

Beste docent en geïnteresseerde,

Voor je ligt een lessenreeks van 5 lessen die je een handvat geeft om in het kader van mediawijsheid en burgerschap quantumcomputers te bespreken. Op een interactieve en speelse manier maken leerlingen in het voortgezet onderwijs kennis met het kraken van codes door encryptie, leren ze hoe een quantumcomputer verschilt van een klassieke computer en oefenen ze met morele vraagstukken waarbij ze nadenken over hun eigen verantwoordelijkheid.

Wat we vooral hopen te bereiken is dat je de leerlingen ruimte geeft om zelf te denken, zelf op onderzoek te gaan en af en toe een stap terug te zetten. Hoewel de lessenreeks genoeg inhoudelijke leerstof omvat, is het belangrijker dat de leerlingen vooral zelf de codes (en hun hersenen) kraken. Het moet geen reeks zijn die je even aftikt, neem er de tijd voor en handel als docent zoals Socrates zou doen: *neem aan dat het enige dat je zeker weet is dat je niets weet*.

Inleiding: wat heb je nodig en wat zit erin?

Wat heb je nodig voordat je begint?

- De lessen moeten opeenvolgend gegeven worden. Dit moet dus werkbaar zijn in je rooster.
- Je hebt internet nodig om de filmpjes te laten zien.
- Je hebt tekenmateriaal nodig voor de eindopdracht.
- Je hebt pen en papier nodig waarop de leerlingen opdrachten en argumenten kunnen maken.
- Je moet per les in de gaten houden welke stencils je moet uitdelen. Het is handig als de leerlingen een map of snelhechter meenemen naar school.
- Voor het gesprek met de leerlingen is het handig om een praatbal te gebruiken.

Wat zit erin?

- Een spannend verhaal met dilemma's.
- Iedere les krijg je verschillende vragen om een gezamenlijk onderzoek mee te starten.
- 4 stencils met informatie en extra verwijzingen naar filmpjes om de informatie te verduidelijken.
- 1 stencil met een eindopdracht.

Hoe is de lessenreeks opgebouwd?

Les 1	Je geld of je leven	De leerlingen komen erachter dat hun telefoon gehackt is.
Les 2	Codekrakers	De leerlingen moeten een oplossing maken en leren over codes kraken.
Les 3	Sticken of tikken	De leerlingen moeten bepalen welke oplossing het beste is.
Les 4	Wie, wat, waar?	De leerlingen denken na over wie er verantwoordelijk is voor het platleggen van het systeem op school.
Les 5	Red het systeem	De leerlingen worden op een creatieve manier uitgedaagd om een voorstel te doen voor een nieuw systeem op school, eentje die niet gehackt kan worden.

De lessenserie begint met het verhaal. Het verhaal is een gedachte-experiment. De leerlingen worden uitgedaagd om iets te denken, of over iets te willen denken, wat nog niet bestaat. Je zegt dus: “Stel je voor..” Uit ervaring weten we dat de leerlingen vaak meer geënthousiasmeerd worden als een verhaal op een spannende manier wordt verteld. Onze eerste keus zou zijn dat je het verhaal doorneemt, jezelf eigen maakt en in de klas op een theatrale manier vertelt. Een verhaal vertellen is een kunst en niet iedereen voelt zich daar even comfortabel bij, dus je kunt het verhaal natuurlijk ook (laten) voorlezen.

In het verhaal zitten verschillende momenten waarop de groep een gezamenlijke keus moet maken. Het is de bedoeling dat je hierover met de groep in gesprek gaat. We geven in deze docentenhandleiding precies aan wanneer deze momenten plaatsvinden. De vragen zijn zo bedacht en geformuleerd om de leerlingen na te laten denken en langer stil te laten staan bij hun overtuigingen, omdat we ze altijd verzoeken om hun beweringen en gedachtes uit te leggen of te beargumenteren. Het uitvragen van deze antwoorden gaat niet hetzelfde als bij een onderwijsleergesprek. We geven daarom hieronder een aantal richtlijnen zodat je het gesprek zo filosofisch mogelijk kunt maken.

Filosoferen met groepen: handvatten

Bij een filosofisch gesprek met leerlingen ben je als volwassene zo min mogelijk aan het woord. Jouw rol is die van gespreksleider. Je eigen mening laat je achterwege! Beschouw de uitspraken van de leerlingen niet als ‘goed’ of ‘fout’, maar als gedachten die door de groep onderzocht moeten worden. Vat regelmatig samen (of laat een leerling dat doen) wat er tot dan toe gezegd is. Zo kunnen de leerlingen standpunten vergelijken en blijft het gesprek het karakter behouden van een onderzoek in plaats van een discussie.
We maken onderscheid tussen een startvraag, een taakvraag en een genestelde vraag.
Een **startvraag** is niet filosofisch, maar betrekt de leerlingen bij het onderwerp. Het is een vraag in de jij-vorm waarop iedereen een antwoord kan geven. Bijvoorbeeld: “Wat denk je dat er aan de hand is?”
Een **taakvraag** is de centrale vraag voor het filosofisch onderzoek. We raden aan om de taakvraag op het bord te schrijven of projecteren. In deze serie zijn dit veelal dilemma’s, waarbij leerlingen gezamenlijk een keus moeten maken. Die keus moeten ze onderbouwen met argumenten. Jij hebt als gespreksleider de taak om die argumenten op tafel te krijgen.
Laat de leerlingen ‘ja’ of ‘nee’ antwoorden op het dilemma en vraag daarna: “want..?”, “hoezo?”, “leg uit?”. Als een leerling een bewering (een uitspraak waarmee je het eens of oneens kunt zijn) doet, kun je die letterlijk herhalen en eventueel teruggeven aan de groep met de vraag: “klopt dat?”, om de antwoordende leerling vervolgens weer om uitleg te vragen.
Ga tijdens het gesprek met regelmaat terug naar de taakvraag als centrale onderzoeksvraag. Zeg bijvoorbeeld: “En wat betekent dat nu voor deze vraag?”
Bij iedere taakvraag vind je in deze handleiding een lijstje **genestelde** vragen. Een genestelde vraag ligt impliciet besloten in de taakvraag. Deze vragen zijn een hulpmiddel voor jou om het gesprek te verdiepen, maar ze zijn niet noodzakelijk omdat de leerlingen het gesprek vaak zelf verdiepen.

Hieronder staat een aantal genestelde vragen die je in ieder gesprek kunt stellen:

- Wat denk jij?
- Waarom denk je dat?
- Hoe weet je dat zo zeker?
- Hoezo?
- Is dat altijd zo?
- Kun je een voorbeeld geven?
- Geldt dat voor alles?
- Is iedereen het daarmee eens?
- Zou het ook anders kunnen zitten?

Stencils met informatie

We hebben bij het verhaal 4 stencils gemaakt met lesstof en opdrachten. Het uitgangspunt van deze reeks is dat leerlingen zelf aan het denken worden gezet, maar ze hebben natuurlijk ook input nodig om over quantumcomputers na te kunnen denken. Het was een uitdaging om de informatie op een zo duidelijk mogelijke manier uit te leggen. We raden aan om de stencils te bestuderen voordat je begint aan de reeks. Je kunt zelf bepalen hoe je de stencils inzet tijdens de lessen. Voor sommige groepen is het goed om ze aan de hand te nemen en de teksten samen te lezen en voor andere groepen is het juist beter is als ze er zelfstandig mee aan de slag gaan. Dit is aan jullie. Wij geven in deze handleiding wel suggesties voor momenten waarop de stencils uitgedeeld en gelezen kunnen worden.

Eindopdracht

We sluiten de lessenreeks af met een eindopdracht, waarin de thema's van de voorgaande lessen samenkomen. Voor de eindopdracht heb je uitsluitend een begeleidende rol. Je kunt er zelf voor kiezen of de leerlingen hun eindopdracht wel of niet presenteren.

Kleurenlegenda docentenhandleiding

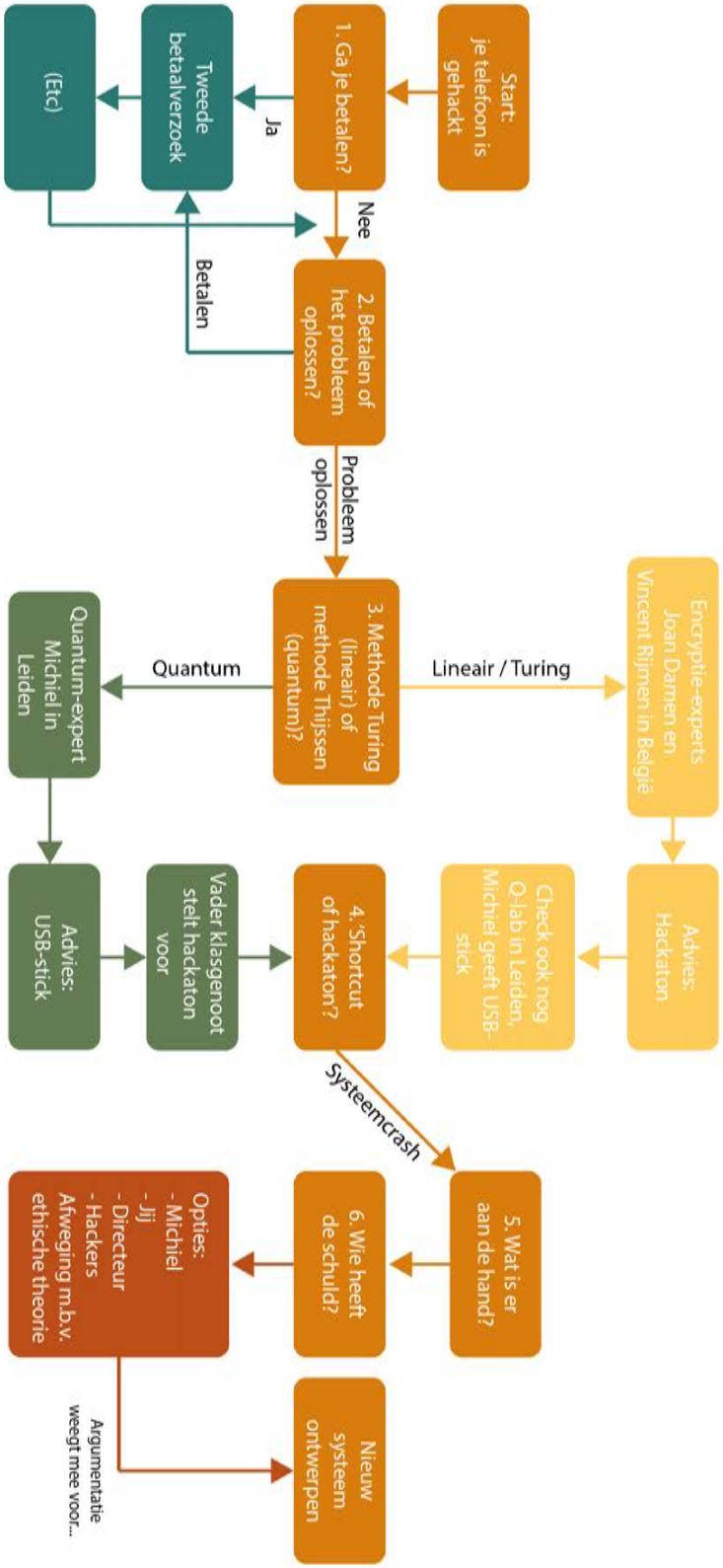
Doen

Spreken

Stencil uitdelen

Differentiëren

Schematisch overzicht van de keuzes in het verhaal



Les 1: Je geld, of je leven?

"We gaan een gedachte-experiment doen." Een gedachte-experiment is eigenlijk niet meer dan een verhaaltje dat begint met de woorden: stel je voor dat.."

Lees of vertel het verhaal (voor) tot en met: *Je kijkt om je heen en ziet anderen ook met een wit weggetrokken gezicht voor zich uit kijken.*

***"Wat kan er aan de hand zijn?"* (Startvraag)**

Leerlingen maken eerst hun eigen hypotheses. Ze hebben voldoende informatie om te weten dat hun telefoon gehackt is. Neem een aantal minuten om de verschillende hypotheses uit de klas te oogsten en vraag ze vooral op basis waarvan ze dat denken. "Hoe weet je dat?" Vat niet samen, geef geen antwoord, maar direct door naar het vervolg. **(maximaal 5 minuten)**

Lees of vertel het vervolg van het verhaal (voor): *Bericht 424 is een betaalverzoek. Je moet 1200 euro betalen. Bericht 425 zegt: "Je hebt 10 minuten om aan het vorige betaalverzoek te voldoen."*

"Ga je betalen?" (Taakvraag 1)

Indien nodig, stel je deze genestelde vragen:

- *Kun je betalen?*
- *Kun je het ged lenen?*
- *Moet je het geld lenen?*

"Het lijkt erop dat je data niet helemaal veilig zijn." "Hoe bescherm je je data?"
(5 min)

Deel stencil 1 over encryptie uit. Voor het VMBO kan het stencil als huiswerk gegeven worden. Dan moet je het uitdelen aan het einde van de les. Geef de leerlingen maximaal 5 minuten om het stencil te lezen. Bepaal zelf of je de leerlingen 1, 2 of 3 opdrachten laat maken of ze dit in de les doen of je deze als huiswerk meegeeft. Dat zal afhangen van de tijd die je hebt en het niveau van je leerlingen. We raden aan om in elk geval opdracht 1 en 2a te doen met je leerlingen.
(15 min)

Optioneel (o.a. voor VWO en Whatsapp-encryptie-stencil):
Laat onderstaand filmpje van 0:34-3:00 zien over de beveiliging in Whatsapp.
Kanaal: Bright
Titel: Gaan quantumcomputers jouw appjes en staatsgeheimen ontcijferen?
Link: https://youtu.be/BRNjOW7JUYI?si=c3c0D32usMMuiPBH&t=34

Lees of vertel het vervolg van het verhaal: Bericht 426 komt binnen. Je neemt een flinke hap lucht voordat je het openmaakt. Daar staat: "Ik heb de beschikking over een quantumcomputer. Jij bent aan de late kant. Je hebt nog één kans. Morgenochtend voor 7 uur wil ik die 1200 euro zien. "Zo niet, dan zet ik al je foto's online, zichtbaar voor iedereen."

"Wat ga je doen? Ga je betalen of ga je proberen het probleem op te lossen?" **(Taakvraag 2)**

Als er wordt gezegd: "We gaan het gewoon oplossen", dan vraag je: "Hoe dan?"
Als iemand zegt: "Ik vraag het geld wel aan m'n moeder/ouders ", "Ik ga het betalen want dan ben ik van het gedoe af." Dan stel je de tegenvraag: "Hoe weet je dat je de dag erna niet weer zo'n berichtje krijgt?" "Ben je ervan af als je betaald hebt?" "Waar is je vertrouwen op gebaseerd?" Laat de leerlingen een argument maken waarin ze uitleggen waarom ze kiezen voor het één of voor het ander.
(15 tot 25 minuten)

Advies voor VMBO-leerlingen. Geef de leerlingen kladblaadjes die je na afloop verzamelt. Omdat het geen 'officieel schrift' is, ontstaat er ook een soort 'klad-denken'. Dat haalt de prestatiedruk eraf, en maakt het voor leerlingen makkelijker om vrij te schrijven. Laat de blaadjes wel inleveren bij de docent. Wanneer de docent de argumenten heeft geoogst, laat je de leerlingen andermans argumenten vertellen of voorlezen.

Zorg dat je 'in de bel valt' zodat er geen tijd is om vandaag te stemmen welke keuze we maken.

“De stemming is pas volgende week: dus ik wil dat je onthoudt welke argumenten je voorbij hebt horen komen, met welke je het eens bent, met welke je het niet eens bent, en misschien bedenk je gedurende de week nog wel een nieuwe reden.”

Noteer de argumenten die voorbijkomen, zodat *jij* ze volgende week weet als zij ze niet kunnen herhalen.

Les 2: Codekrakers

Haal de argumenten uit de vorige les op. Laat daarna de klas stemmen. Je kunt de leerlingen bijvoorbeeld laten stemmen met vingers en die tellen.
(10 min)

Als de klas kiest voor betalen, dat kan namelijk, dan gaat het verhaal als volgt verder:

"Je maakt het geld over en wacht vol spanning af of je telefoon weer vrijgegeven wordt. Het is ook verdraaid onhandig dat je alleen maar kunt appen met degene die jou die akelige berichtjes stuurt. Je durft je telefoon ook niet weg te leggen, omdat je geen idee hebt wat er allemaal kan gebeuren. Na 5 minuten verschijnt het volgende bericht: "Dank voor je betaling, ik zie de volgende 1200 euro graag verschijnen voor vanmiddag 14:00 uur.""

Dit herhaal je totdat ze zelf ontdekken dat er geen einde komt aan de betalingsverzoeken en ze het probleem wel moeten oplossen.

Als je het probleem wilt oplossen, moet je begrijpen hoe codes worden gekraakt. Daarvoor lees je stencil 2. Je kunt ervoor kiezen dit samen of individueel te lezen.
(5 tot 10 min)

Voor het VMBO kan stencil 2 als huiswerk meegaan. Ga in dat geval direct door naar het filmpje.

Laat na het lezen van stencil 2 het filmpje zien van qubits die twee kanten tegelijk op kunnen in een doolhof (superpositie).
Kanaal: QuTech Academy
Naam van het filmpje: The maze | QuTech Academy
Link: https://www.youtube.com/watch?v=OQ-NkCiyj_c&ab_channel=QuTechAcademy

Voer een OLG naar aanleiding van het filmpje: wat zie je? Wat valt je op? Wat denk je dat deze computer kan? In het OLG moet duidelijk worden dat de leerlingen ongeveer weten wat een superpositie is (= een quantumdeeltje dat zich tegelijkertijd, theoretisch, op twee plaatsen tegelijk bevindt). Differentiëren: voor het VMBO leg je uit dat de linkerkant van het filmpje de methode Turing laat zien en de rechterkant gebaseerd is op de methode Thijssen (quantumcomputer).
(10 min)

Als je een oplossing met klassieke computers wilt, dan moet je naar België voor een gesprek met wetenschappers die voortbouwen op het werk van Alan Turing? Of kies je liever voor hulp van iemand die veel weet van quantumcomputers. Misschien moet je dan in de tijd vooruitreizen, maar je kunt beginnen in het Quantum Rules! Lab in Leiden, waar Michiel Thijssen werkt. Waar kiezen jullie voor: ga je het probleem oplossen met advies van iemand die alles weet van encryptie in klassieke computers of met advies van een quantum-expert?
(Taakvraag 4)

Laat leerlingen argumenten maken waarbij ze kiezen voor de methode Turing of de methode Thijssen. Je eindigt de les met argumenten en les 3 begint weer met een keuzemoment.
(20-25 min)

Les 3: Sticken of tikken

Haal de argumenten uit de vorige les op. Laat daarna de klas stemmen over taakvraag 3. Je kunt de leerlingen bijvoorbeeld laten stemmen met vingers en die tellen.
(10 min)

"Als je kiest voor de methode van Turing moet je even weten hoelang het duurt voordat je met gewone encryptie je telefoon weer tot je beschikking hebt." "Als je kiest voor Thijssen, dan weet je ook niet of die quantumcomputer ooit gaat werken."

Let op! Zorg dat dit duidelijk voor de leerlingen is: in beide gevallen blijft het risico dat alles op je telefoon online komt.

Als de klas kiest voor een gesprek met iemand die veel weet van encryptie.
Vervolg verhaal: *Jij en je buurman maken een afspraak met Joan Damen en Vincent Rijmen. Dit olijke duo uit België maakt het belangrijkste encryptie- algoritme dat we op dit moment kennen: AES, of wel Advanced Encryption System. Zij adviseren jullie om een hackathon met ethische hackers te organiseren. (Een hackathon is een langdurige sessie om codes te kraken met heel veel deelnemers.) Dan kunnen zij proberen om met z'n allen de code te kraken. Jullie kunnen trouwens ook nog bij het Quantum Rules! lab in Leiden langsgaan om te vragen of ze daar al een stukje code hebben waarmee je het probleem kunt oplossen.*
Jullie durven je telefoon nog steeds niet te gebruiken dus kunnen de klas pas morgen vertellen welk advies jullie hebben gekregen. De volgende ochtend stellen jullie in de klas voor om zo snel mogelijk een hackathon te organiseren. Daar moet je natuurlijk wel dingen voor regelen, zoals een heel goede wifi verbinding, veel stroomaansluitingen en eten een drinken voor de deelnemers. En: een beetje hackathon kost al gauw € 2500,- .

Als de klas kiest voor een gesprek met Michiel Thijssen.
Vervolg verhaal: *Jij en je buurman maken een afspraak met Michiel Thijssen. Jullie gaan naar Leiden. Jullie lopen het Quantum Rules! lab van meneer Thijssen binnen, die jullie hartelijk welkom heet. Precies op dat moment begint je telefoon te piepen. Michiel vraagt: "Heb je ergens last van?" Jij zegt: "Ja, daar komen we voor. Ik krijg voortdurend berichtjes dat iemand al mijn foto's online wil zetten." Michiel: "Laat eens zien?!" Je aarzelt even. En geeft dan je telefoon.*
Michiel kijkt en zegt: "O, dat is niet zo heel erg moeilijk. Onze quantumcomputer kan hiervoor een code maken door de encryptiegetallen allemaal in één keer met elkaar te vergelijken. Het klinkt als tovenarij, maar er is al bewijs dat het in principe kan.
Kijk, dit filmpje legt je mooi uit wat het verschil is tussen een klassieke computer en een quantumcomputer."

Laat het onderstaande filmpje zien van 0:34 tot 3:44
Kanaal: Kurzgesagt
Titel: Quantum Computers Explained – Limits of Human Technology
Link: https://youtu.be/JhHMJCUmq28?si=uqxSpvWHdbrkldm7&t=34

Michiel vertelt verder: "We weten van veel wetenschappelijke berekeningen al hoe het moet, maar de klassieke computer kan al die mogelijkheden niet aan. Hier werken we eraan om die barrière weg te halen: door quantumcomputers te maken die anders rekenen. Als het ons lukt, kunnen we gaan uitrekenen welk molecuul het perfecte geneesmiddel is voor een ziekte. We zouden dan ook veel dure experimenten kunnen vervangen door bijna perfecte quantumcomputersimulaties. Dat is natuurlijk uiteindelijk veel goedkoper."
"Terug naar jouw probleem: daar kan onze quantumcomputer wel bij helpen. Ik kan je wel een stukje code geven waardoor hacker niet meer bij jouw gegevens kan. Misschien kan dat stukje code er zelfs wel voor zorgen dat jij erachter komt wie het is!"
Michiel haalt uit zijn bureaulade een USB-stick met een verloopje zodat je het op je telefoon kunt aansluiten. Jullie gaan opgelucht terug naar huis en kunnen bijna niet wachten om de rest te vertellen dat het probleem bijna opgelost is. De volgende ochtend in de klas vertellen jullie dat jullie een USB-stick hebben gekregen met een stukje code erop..

Vervolg verhaal
Een van je klasgenoten vertrouwt het zaakje niet. Hij wil eerst overleggen met zijn vader, die een IT-specialist is. Hij spijbelt het 3e uur en gaat bij zijn vader langs om te vragen wat jullie het beste kunnen doen. Zijn vader zegt: "Nooit zomaar codes kopiëren, dan is Turings manier een stuk veiliger."

"Kies je de shortcut (met het USB-stickje) van Michiel of de hackathon (die wel een week of 2 kan duren)? **(taakvraag 4)**

Genestelde vragen:
- Wie vertrouw je meer: de ethische hackers of Michiel Thijssen?
- Op grond waarvan vertrouw je de ethische hackers of Thijssen?
- Kun je weten of de code gaat werken?
- Wil je weten wie de hacker is?

Laat de leerlingen argumenten maken voor het een of voor het ander. Wat wil je? Methode Turing of methode Thijssen?
(10 min)

Laat het vervolg van het filmpje zien vanaf 2:49 tot 7:16 over het verschil tussen klassieke computers en quantumcomputers.
Kanaal: Kurzgesagt
Titel: Quantum Computers Explained – Limits of Human Technology
Link: https://youtu.be/JhHMJCUmq28?si=vf7n0Tk8KIVdLpnm&t=169

Je gaat terug naar de taakvraag 4: kies je voor een shortcut of hackathon? Controleer of de informatie uit het filmpje iets verandert aan hun argumenten.

Geef stencil 3 mee naar huis en laat ze de bijbehorende opdracht maken.

Les 4: Wie, wat, waar?

Bespreek eerst de opdracht: laat ze in ieder geval hun antwoord op vraag 2 (de verschillen tussen klassieke computers en quantumcomputers) vertellen. Dan haal je de argumenten terug die ze in de vorige les gegeven hebben. Laat daarna de klas stemmen over taakvraag 4: kiezen ze de shortcut of de hackathon?
(15 min)

Als leerlingen kiezen voor de hackathon.
Vervolg verhaal: *Je bestelt eten, drinken en een enorme capaciteit LAN-verbinding. Jullie regelen dat er een grote groep in de school terecht kan en niet gestoord wordt terwijl ze aan het werk zijn. Twee weken lang horen jullie niets anders dan het getyp op toetsenborden en het kraken van pizzadozen. Dan begint er iemand te schreeuwen: Ik heb het! Echt waar! het werkt! Jij wordt aan je schouders richting een computer geduwd. Leg je telefoon neer', zegt degene achter het toetsenbord. Een beetje verbaasd leg jij je telefoon naast zijn computer. Hij verbindt jouw telefoon met zijn computer en je ziet dat er een bestandje geladen wordt. Kennelijk hebben de hackers een code gevonden. Het laad icoontje verdwijnt en jij verstuurt het bestand naar degene die jou voortdurend berichtjes heeft gestuurd.*

Als de leerlingen kiezen voor de USB-stick:
Vervolgverhaal: Je sluit de USB-stick aan op je telefoon en er verschijnt een icoontje. Je klikt erop en ziet wat computertaal `</%RUN_CODE#\>` *. Je haalt diep adem en sleept het bestandje naar je WhatsApp en verstuurt het naar de hacker.*

Vervolg verhaal (in beide gevallen)
Drie minuten later gaan de lichten in het lokaal uit, het digibord houdt ermee op en ergens begint een irritant piepje. De docenten komen hun lokalen uit, lopen over de gang en zoeken Henk, die jullie ICT beheert. Niemand heeft meer een idee wat ie moet doen en uiteindelijk loopt de hele school te zoeken naar de directeur. Mensen rennen over trappen (want de lift doet het ook niet meer), deuren slaan dicht en gaan weer open, mensen duwen en trekken en op de achtergrond klinkt dat piepje. Vlak voor de eerste pauze vinden jij en een klasgenoot de directeur in de kelder. Hij zit te hameren op het toetsenbord voor zijn neus terwijl het kwijl uit zijn mond loopt.
"Meneer, wat bent u aan het doen?"
De directeur kijkt enigszins verdwaasd op en zegt: "Hoe moet ik dat weten?"
"Meneer, u moet naar boven komen. Alle techniek ligt eruit. We hebben geen internet, geen computer werkt, de digiborden weigeren en de 6e heeft een toets maar kan hem niet maken want daar hebben ze een laptop bij nodig."
De directeur veegt zijn mond af, stommelt overeind en loopt voor je uit de trap op naar de docentenkamer.
"Wat is er aan de hand?", vraagt de ICT-beheerder.
De directeur zegt: "Ik heb een berichtje gekregen, dat heb ik geopend en sindsdien ligt alles op zijn gat."
"Heeft u op een link geklikt?"
"Nee, natuurlijk niet. Ik heb alleen het berichtje geopend. Kennelijk zat er een virus in."

“Wat kan er aan de hand zijn?” (Taakvraag 5)
Laat de leerlingen hypotheses maken en vraag de hypotheses terug.
(10 min)

“Wie heeft de schuld van wat er aan de hand is?" (Taakvraag 6)
1. Michiel Thijssen, want het was zijn code.
2. Ethische hackers, want die hebben de code geleverd.
3. Jij, want je hebt hem doorgestuurd.
4. De directeur, want die heeft het bericht geopend.
5. De quantumcomputer, die mogelijk fouten heeft gemaakt?)
(5 min)

Deel stencil 4 uit. Welke ethische stroming heb je gebruikt om iemand verantwoordelijk te houden? Utilisme, plichtethiek of deugdethiek?
(5 min)

“Wie heeft de schuld van wat er aan de hand is?" Controleer of de extra informatie iets verandert aan hun argumenten.
(5 min)

Maak duidelijk: Wie de schuld ook heeft, dat zorgt niet dat het systeem weer opstart.

Les 5: Red het systeem!

Haal de argumenten uit de vorige les op. Laat de leerlingen kiezen wie de schuld heeft: Thijssen, ethische hackers, jij of de directeur. Laat daarna de klas stemmen. Je kunt de leerlingen bijvoorbeeld laten stemmen met vingers en die tellen. Voor het vervolg maakt deze keuze niet uit.
(10 min)

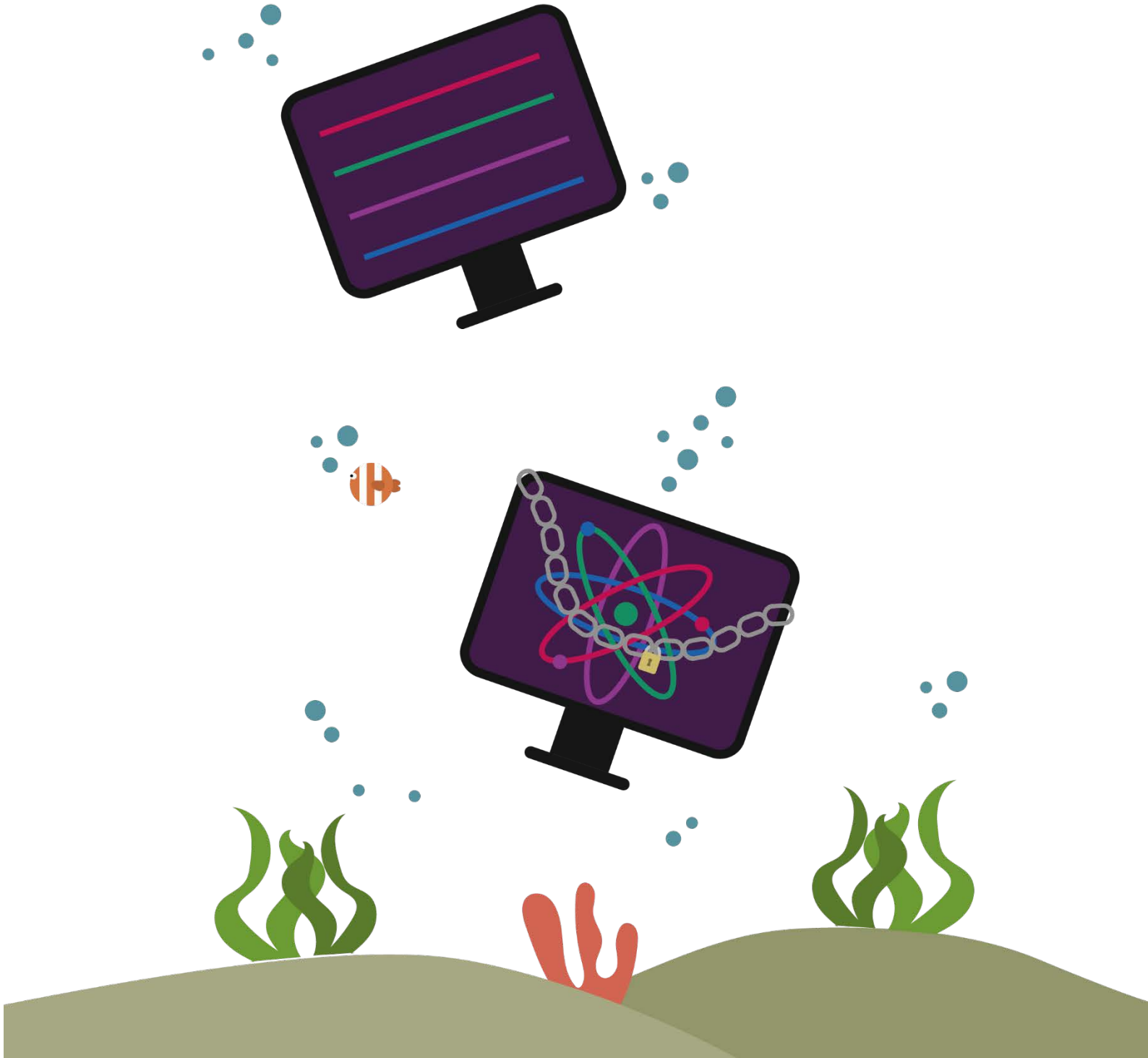
Tip: als leerlingen vragen waarom de directeur dit heeft gedaan kun je vertellen dat hij wilde dat de school een 100% score zou halen in het leerlingvolgsysteem.

Het hele digitale systeem van de school is kapot! Om het systeem weer aan de praat te krijgen heeft de school een compleet nieuwe digitale infrastructuur nodig. Niemand wil dat dit soort ellende zich nogmaals kan voordoen. Het is absoluut nodig dat jullie encryptie veilig is, ook voor iemand die het misschien goed bedoelt. Om te voorkomen dat dit soort ellende zich ooit nog kan afspelen en dat heel slecht uitpakt gaan jullie een computer laten bouwen die tegen hacken is bestand en misschien ook nog wel een positieve bijdrage kan leveren aan het oplossen van energieproblemen in de buurt.

Zorg dat er tekenmateriaal in de klas is en deel stencil 5 uit met de opdracht. Laat de leerlingen werken in groepjes van twee of drie.

Tijdens het maken van de opdracht biedt de docent hulp op maat. Eventueel kun je de laatste 10 minuten van de les gebruiken om de ontwerpen te bespreken.
(30 min)

Het verhaal



Het verhaal

Les 1: Je geld, of je leven?

We gaan een gedachte-experiment doen. Een gedachte-experiment is eigenlijk niet meer dan een verhaaltje dat begint met de woorden: stel je voor dat. Dus daar gaan we:

Stel je voor dat: het is zo'n dag, je voelt het al wanneer je wakker wordt. Je zet je benen net buitenboord en je stapt in een plas water. "Is het wel water?" Vraag je jezelf af. Het heeft gelekt.
Je loopt naar de badkamer, zet de douche aan en doet een stap naar achteren, want het duurt wel even voor hij warm is. Maar vandaag sta je daar al zeker drie minuten te bibberen en dat rotwater wordt maar niet warm. Licht chagrijnig draai je de kraan dicht, stopt je hoofd bij de wastafel onder de koude kraan, poetst je tanden, kleedt je aan en gaat naar beneden om te ontbijten. Je had het kunnen weten: brood op.
Nu moet je ook nog gaan opschieten, want anders kom je te laat, en je hebt het eerste uur een toets. Ik zei het al: het is zo'n dag.
Je springt op je fiets, maar voelt dat je achterband zacht is. Je hebt geen tijd meer om 'm op te pompen. Staand op de pedalen race je naar school. Vlak voor de tweede zoemer/bel ren je het lokaal in. De docent deelt de toetsen uit en zegt: "Ok, dames en heren, telefoons uit en in de tas alsjeblieft." Je pakt je telefoon om 'm uit te zetten en op dat moment zie je dat er 423 berichtjes zijn binnengekomen. Natuurlijk heb je nu geen tijd om ze te lezen, zo'n dag is het nou eenmaal. Je drukt 'm uit, ruimt je telefoon op, pakt je pen en wacht tot je aan je toets mag beginnen.

Je begint aan je toets met een steen in je maag. Dat helpt in elk geval tegen de honger. Na tien minuten heb je eigenlijk geen idee meer wat je zit te doen. Je kauwt op je pen, doodlet op je papier, vult af en toe iets in en denkt alleen maar: "hoe laat is het, hoe laat is het, hoe laat is het…" Aan alles komt een end. Ook aan een uur waarin je toetsen maakt. Dus gelukkig gaat ook dit voorbij. De docent haalt de toetsen op en jullie mogen het lokaal uit. Iedereen is met zijn telefoon aan het klooien. Die moet aan, iedereen moet even checken wat hij gemist heeft het afgelopen uur. Ook jij bent zeer benieuwd waar die 423 berichtjes vandaan komen en waar ze over gaan.
Alle berichtjes beginnen met: "Beste jij, ben je gehecht aan deze telefoon? Ben je gehecht aan je privacy? Hoe interessant zou het zijn als ik al jouw foto's online zou zetten?" De steen in je maag maakt een sprongetje. 423 keer hetzelfde bericht. En 423

keer zonder afzender. Je kijkt om je heen en ziet anderen ook met een wit weggetrokken gezicht voor zich uit kijken.

Wat kan er aan de hand zijn?

Vervolg verhaal:
Bericht 424 is een betaalverzoek. Je moet 1200 euro betalen. Bericht 425 zegt: “Je hebt tien minuten om aan het betaalverzoek te voldoen.”

Ga je betalen?

Vervolg verhaal:
Bericht 426 komt binnen. Je neemt een flinke hap lucht voordat je het openmaakt. Daar staat: “Ik heb de beschikking over een quantumcomputer, dus ik kan de encryptie van je hele telefoon hacken. Jij bent aan de late kant met betalen. Je hebt nog één kans. Morgenochtend voor 7 uur wil ik die 1200 euro zien. Zo niet, dan zet ik al je foto’s online, zichtbaar voor iedereen.”

Wat ga je doen? Ga je betalen of ga je proberen het probleem op te lossen?

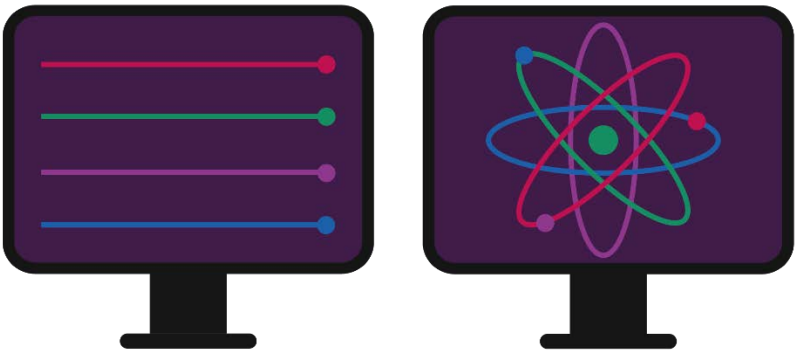
Les 2: Codekrakers

Als de klas kiest voor betalen gaat het verhaal als volgt verder:

Je maakt het geld over en wacht vol spanning af of je telefoon weer vrijgegeven wordt. Het is ook verdraaid onhandig dat je alleen maar kunt appen met degene die jou die akelige berichtjes stuurt. Je durft je telefoon ook niet weg te leggen, omdat je geen idee hebt wat er allemaal kan gebeuren. Na 5 minuten verschijnt het volgende bericht: Dank voor je betaling, ik zie de volgende 1200 euro graag verschijnen voor vanmiddag 14:00 uur.:
Je maakt het geld over en wacht vol spanning af of je telefoon weer vrijgegeven wordt.

Als de klas kiest voor niet betalen:
Oké, we gaan niet betalen. We zijn per slot van rekening niet gek. Maar dan moeten we het probleem wel op de één of andere manier oplossen. Een paar klasgenoten weten wel dingen van computers, maar dat is op dit moment niet genoeg. Je kunt natuurlijk proberen om de encryptie te kraken van degene die jouw telefoon heeft gehackt. Maar je weet al dat het kraken van encryptie verdraaid lastig kan zijn. Je zou natuurlijk advies kunnen vragen aan Alan Turing. Dan moet je op reis door de tijd naar 1939. In dat jaar bouwde Turing de *bombe*, de beste codekraker van zijn tijd. Maar tijdreizen is nog altijd heel lastig. Gelukkig zijn er ook vandaag de dag heel goede encryptiekrakers. De meest vooraanstaande heten Joan Damen en Vincent Rijmen uit Leuven in België. Maar je kunt natuurlijk ook advies vragen bij hedendaagse quantumwetenschappers. Dan kun je waarschijnlijk het beste naar Michiel Thijssen van het Quantum Rules! Lab in Leiden gaan.

Waar kiezen jullie voor: Ga je het probleem oplossen met advies van iemand die alles weet van encryptie in **klassieke computers**, **of** met het advies van een **quantumexpert**?



Les 3: Sticken of tikken?

Als de klas kiest voor een gesprek met iemand die veel weet van encryptie.
Jij en je buurman maken een afspraak met Joan Damen en Vincent Rijmen. Dit olijke duo uit België maakt het belangrijkste encryptie- algoritme dat we op dit moment kennen: AES, of wel Advanced Encryption System. Zij adviseren jullie om een hackathon met ethische hackers te organiseren. (Een hackathon is een langdurige sessie om codes te kraken met heel veel deelnemers.) Dan kunnen zij proberen om met z'n allen de code te kraken. Jullie kunnen trouwens ook nog bij het Quantum Rules! lab in Leiden langsgaan om te vragen of ze daar al een stukje code hebben waarmee je het probleem kunt oplossen.

Jullie durven je telefoon nog steeds niet te gebruiken dus kunnen de klas pas morgen vertellen welk advies jullie hebben gekregen. De volgende ochtend stellen jullie in de klas voor om zo snel mogelijk een hackathon te organiseren. Daar moet je natuurlijk wel dingen voor regelen, zoals een heel goede wifi verbinding, veel stroomaansluitingen en eten een drinken voor de deelnemers. En: een beetje hackathon kost al gauw € 2500,- .

Als de klas kiest voor een gesprek met Michiel Thijssen.
Jij en je buurman maken een afspraak met Michiel Thijssen. Jullie gaan naar Leiden. Jullie lopen het Quantum Rules! lab van meneer Thijssen binnen, die jullie hartelijk welkom heet. Precies op dat moment begint je telefoon te piepen. Michiel vraagt: "Heb je ergens last van?" Jij zegt: "Ja, daar komen we voor. Ik krijg voortdurend berichtjes dat iemand al mijn foto's online wil zetten." Michiel: "Laat eens zien?!" Je aarzelt even. En geeft dan je telefoon.

Michiel kijkt en zegt: "O, dat is niet zo heel erg moeilijk. Onze quantumcomputer kan hiervoor een code maken door de encryptiegetallen allemaal in één keer met elkaar te vergelijken. Het klinkt als tovenarij, maar er is al bewijs dat het kan."

Michiel vertelt verder: "We weten van veel wetenschappelijke berekeningen al hoe het moet, maar de klassieke computer kan al die mogelijkheden niet aan. Hier werken we eraan om die barrière weg te halen: door quantumcomputers te maken die anders rekenen. Als het ons lukt, kunnen we gaan uitrekenen welk molecuul het perfecte geneesmiddel is voor een ziekte. We zouden dan ook veel dure experimenten kunnen vervangen door bijna perfecte quantumcomputersimulaties. Dat is natuurlijk uiteindelijk veel goedkoper."

“Terug naar jouw probleem: daar kan onze quantumcomputer wel bij helpen. Ik kan je een stukje code geven waardoor hacker niet meer bij jouw gegevens kan. Misschien kan dat stukje code er zelfs wel voor zorgen dat jij erachter komt wie het is!”
Michiel haalt uit zijn bureaulade een USB-stick met een verloopje zodat je het op je telefoon kunt aansluiten. Jullie gaan opgelucht terug naar huis en kunnen bijna niet wachten om de rest te vertellen dat het probleem bijna opgelost is. De volgende ochtend in de klas vertellen jullie dat jullie een USB-stick hebben gekregen met een stukje code erop.

Vervolg van het verhaal:
Eén van je klasgenoten vertrouwt het zaakje niet. Hij wil eerst overleggen met zijn vader die een IT-specialist is. Hij spijbelt het 3e uur en gaat bij zijn vader langs om te vragen wat jullie het beste kunnen doen. Zijn vader zegt: “Nooit zomaar codes kopiëren, dan is Turings manier een stuk veiliger.”

Taakvraag 4: kies je de shortcut (met het USB-stickje van Michiel) **of de hackathon** (die wel een week of 2 kan duren)**?**

Les 4: Wie, wat, waar?

Als de leerlingen kiezen voor de hackathon:
Je bestelt eten, drinken en een enorme capaciteit LAN-verbinding. Jullie regelen dat er een grote groep in de school terecht kan en niet gestoord wordt terwijl ze aan het werk zijn. Twee weken lang horen jullie niets anders dan het getik op toetsenborden en het kraken van pizzadozen. Dan begint er iemand te schreeuwen: Ik heb het! Echt waar! het werkt! Jij wordt aan je schouders richting een computer geduwd. Leg je telefoon neer', zegt degene achter het toetsenbord. Een beetje verbaasd leg jij je telefoon naast zijn computer. Hij verbindt jouw telefoon met zijn computer en je ziet dat er een bestandje geladen wordt. Kennelijk hebben de hackers een code gevonden. Het laadicoontje verdwijnt en jij verstuurt het bestand naar degene die jou voortdurend berichtjes heeft gestuurd.

Als de leerlingen kiezen voor de USB-stick:
Je sluit de USB-stick aan op je telefoon en er verschijnt een icoontje. Je klikt erop en ziet wat computertaal `</%RUN_CODE#\>` . Je haalt diep adem, sleept het bestandje naar je Whatsapp en verstuurt het naar de hacker.

In beide gevallen:
Drie minuten later gaan de lichten in het lokaal uit, het digibord houdt ermee op en ergens begint een irritant piepje. De docenten komen hun lokalen uit, lopen over de gang en zoeken Henk die jullie ICT beheert. Niemand heeft meer een idee wat ie moet doen en uiteindelijk loopt de hele school te zoeken naar de directeur. Mensen rennen over trappen (want de lift doet het ook niet meer), deuren slaan dicht en gaan weer open, mensen duwen en trekken en op de achtergrond klinkt dat piepje. Vlak voor de eerste pauze vinden jij en een klasgenoot de directeur in de kelder. Hij zit te hameren op het toetsenbord voor zijn neus terwijl het kwijl uit zijn mond loopt.

Meneer, wat bent u aan het doen?
De directeur kijkt enigszins verdwaasd op en zegt: "Hoe moet ik dat weten?"
"Meneer, u moet naar boven komen. Alle techniek ligt eruit. We hebben geen internet, geen enkele computer werkt, de digiborden weigeren en de 6e heeft een toets maar kan hem niet maken want daar hebben ze een laptop bij nodig."
De directeur veegt zijn mond af, stommelt overeind en loopt voor je uit de trap op naar de docentenkamer.
"Wat is er aan de hand?", vraagt de ICT-beheerder. De directeur zegt: "Ik heb een berichtje gekregen, dat heb ik geopend en sindsdien ligt alles op zijn gat."
"Heeft u op een link geklikt?"
"Nee, natuurlijk niet. Ik heb alleen het berichtje geopend. Kennelijk zat er een virus in."

Taakvraag 5: Wat kan er aan de hand zijn?

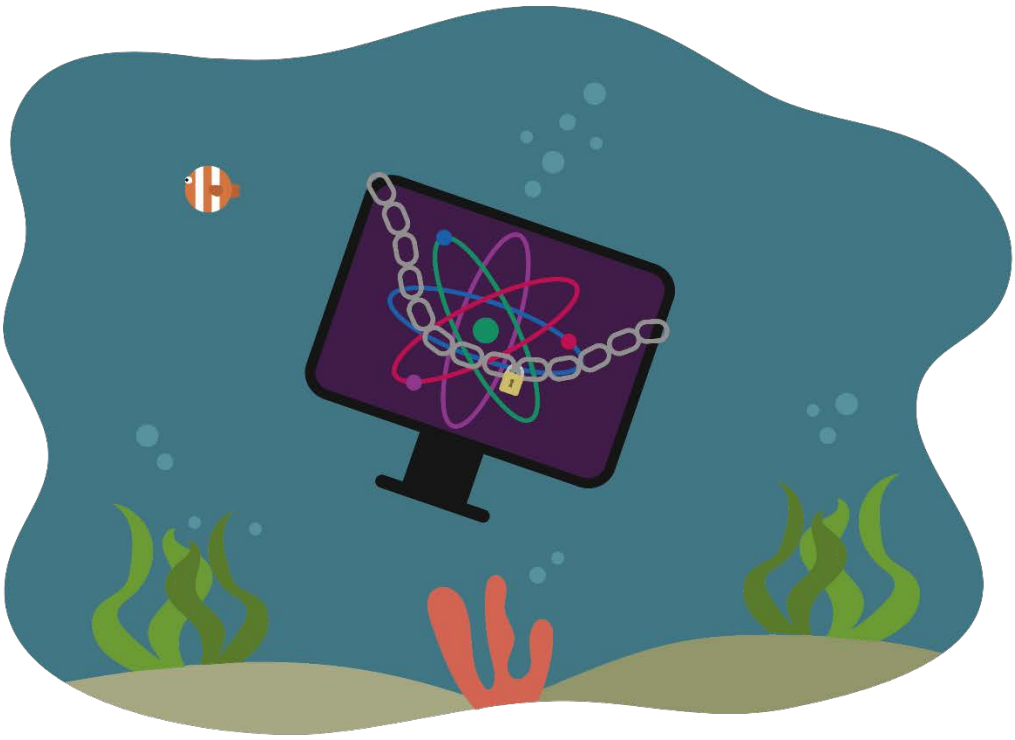
Taakvraag 6: wie heeft de schuld van wat er aan de hand is?
1. Michiel Thijssen, want het was zijn code.
2. Ethische hackers, want die hebben de code geleverd.
3. Jij, want je hebt hem doorgestuurd.
4. De directeur, want die heeft het bericht geopend.
5. De quantumcomputer, die mogelijk fouten heeft gemaakt?

Les 5: Red het systeem!

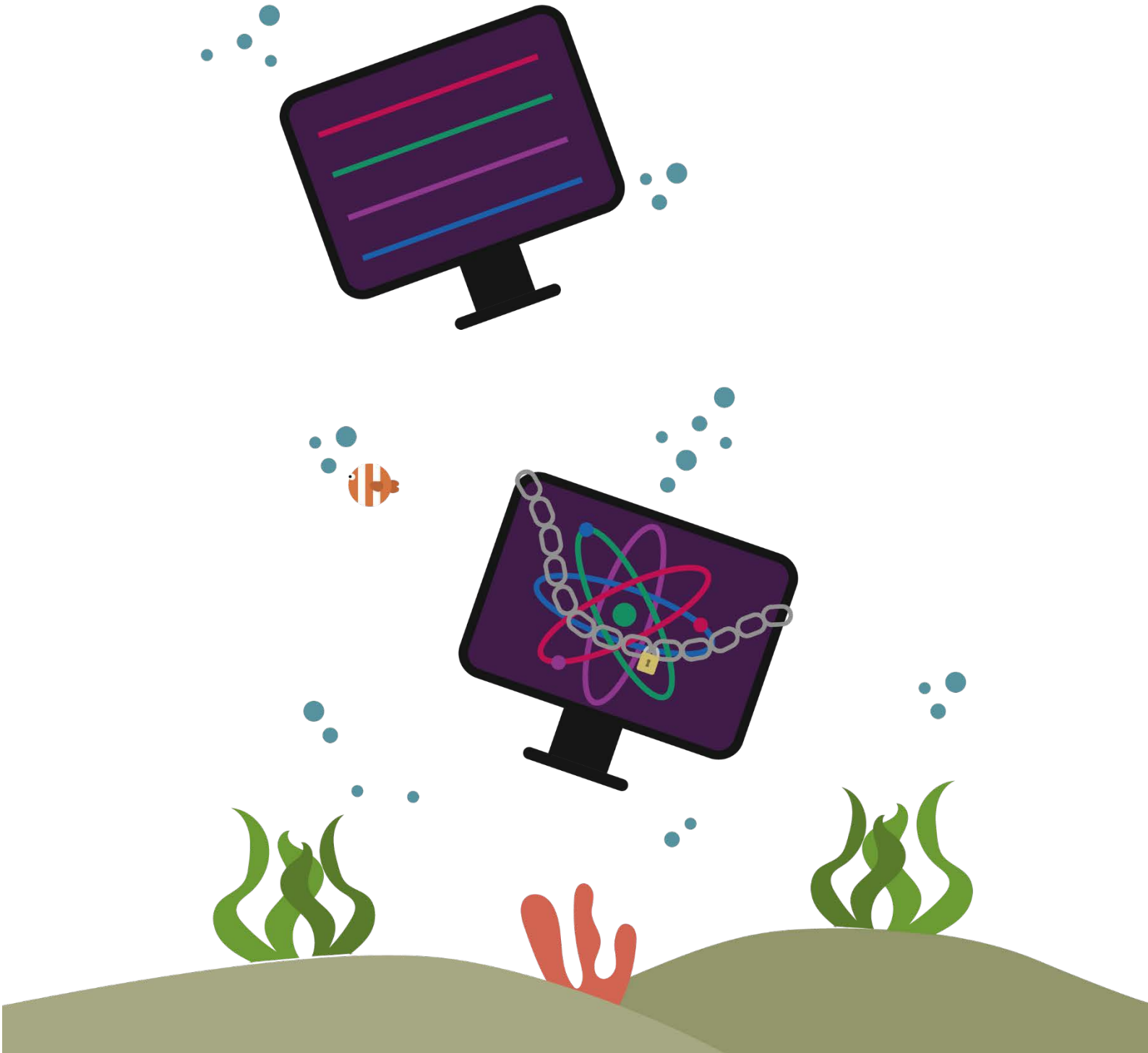
Het hele digitale systeem van de school is kapot! Om het systeem weer aan de praat te krijgen heeft de school een compleet nieuwe digitale infrastructuur nodig. Niemand wil dat dit soort ellende zich nogmaals kan voordoen. Het is absoluut nodig dat jullie data veilig zijn, **ook** voor iemand die het misschien goed bedoelt. Om te voorkomen dat dit soort ellende zich ooit nog kan afspelen en dat heel slecht uitpakt, gaan jullie een computer laten bouwen die tegen hacken is bestand en misschien ook nog wel een positieve bijdrage kan leveren aan het oplossen van energieproblemen in de buurt.

Moet het een quantumcomputer zijn met verstrengelde qubits en encryptie die niet te kraken is? Ja of nee, en waarom?

Als het een quantumcomputer moet zijn, wat moet hij dan kunnen?
Maak een lijstje van de mogelijkheden die het nieuwe digitale systeem moet hebben. Maak vervolgens met een groepje de ontwerpopdracht voor de computerbouwer.



De stencils

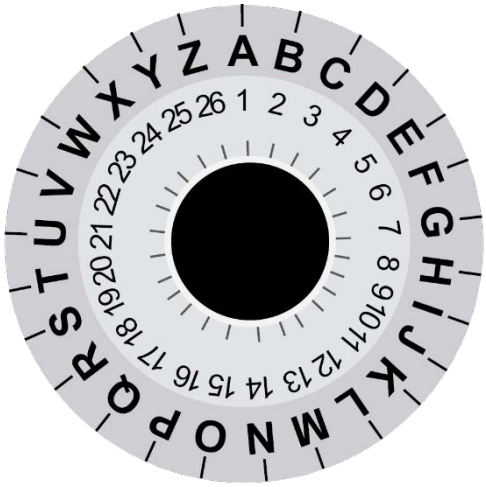


1 - Wat is encryptie?

De data in je telefoon worden beschermd door een code die aan twee kanten beveiligd is. Zo zijn berichten in Whatsapp bijvoorbeeld ‘end-to-end’ versleuteld.

Versleuteling

Om te zorgen dat andere mensen jouw berichten niet zomaar kunnen lezen, kun je jouw berichten ‘versleutelen’. Dat heet **encryptie**. Je maakt dan een geheimtaal en je maakt daar een sleutel bij om die geheimtaal weer te ontcijferen. Zo’n geheimtaal kan bijvoorbeeld zijn: “8.1.12.12.15 4.1.1.18”

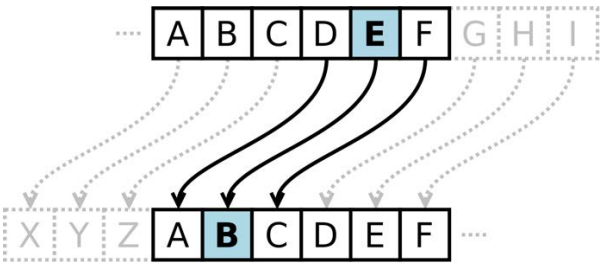


De sleutel: 1 = a, 2 = b, 3 = c, enzovoort voor het hele alfabet.

Kun je lezen wat er staat?

De oudste encryptie

Zelfs Julius Caesar, romeins staatsman (leefde van 100 tot 44 voor Christus) gebruikte al encryptie. Als hij een brief schreef met belangrijke geheime informatie schreef, schoof hij alle letters bijvoorbeeld drie plekken op in het alfabet. Zodra de ontvanger, die dit natuurlijk ook wist, de letters weer terugschoof, stond er weer begrijpelijke tekst. Caesar zou in zijn encryptie ‘Hallo’ schrijven als ‘Exiil’. De sleutel vind je hieronder.



Opdrachten bij stencil 1

1. Maak hieronder je eigen encryptiesleutel. Volg het voorbeeld van Julius Caesar, maar kies zelf hoeveel letters je doorschuift. Let goed op en zorg dat de verbindingslijnen elkaar niet kruisen (als H wordt verbonden met O, verbind je I met P, enzovoort).

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

2. Schrijf op een apart blaadje een geheime boodschap van één zin aan je buur. Pak een stopwatch en laat je buur de boodschap ontcijferen.
    a. Vertel jouw sleutel er *niet* bij. Hoe lang doet je buur erover om jouw boodschap te ontcijferen?
    b. Maak een nieuwe zin. Vertel nu jouw sleutel er *wel* bij en houd bij hoelang het duurt voordat je buur de boodschap heeft ontcijferd.
    c. Wat is het tijdsverschil?

3. Bedenk in tweetallen drie manieren om ervoor te zorgen dat het *moeilijker* wordt om een versleuteling te kraken.

Manier 1: _____

Manier 2: _____

Manier 3: _____

Whatsapp-encryptie (optioneel/vwo)

De encryptie van Julius Caesar is best eenvoudig. Hij versleutelt zijn boodschap met een vertaalsleutel en stuurt hem naar de ontvanger. Maar dan heeft Caesar een probleem: hoe krijgt hij de vertaalsleutel op een veilige manier bij de ontvanger? Als de vijand die sleutel onderschept, zijn al Caesars berichten leesbaar!

Figuur 1 - De publieke sleutel is als een open hangslot: iedereen kan het bericht met dit slot vergrendelen.

Voor dit probleem hebben we tegenwoordig een oplossing: public key-encryptie. Hiermee zijn bijvoorbeeld jouw whatsapp-berichten versleuteld.
Bij public key-encryptie worden **twee** codes aangemaakt: één om de boodschap te versleutelen en een tweede om hem weer te ontcijferen. De eerste code geef je aan iedereen met wie je wilt communiceren, de tweede code is alleen voor jezelf. De eerste code noemen we de publieke sleutel en lijkt op een kluis: je kunt hem wel dichtdoen, maar niet zomaar weer open krijgen. Alleen met de tweede code, de privé-sleutel die jij alleen hebt, kun je de kluis weer openen. Zo kan iedereen jou veilig versleutelde berichten sturen.

Figuur 2 - jouw privésleutel is de enige die het slot weer kan openen.

Priemfactoren
Als jij een whatsappgesprek start met je vriend, maken jullie telefoons automatisch een publieke en een privé-sleutel aan.
Daarvoor gebruikt whatsapp priemgetallen, getallen die alleen door zichzelf en door 1 kunnen worden gedeeld. Priemgetallen zijn bijvoorbeeld: 3, 5, 13 of 1439.
Als je twee priemgetallen met elkaar vermenigvuldigt, heten ze 'priemfactoren'. Bijvoorbeeld: 3 en 5 zijn de priemfactoren van 15. En 15 kan *alleen* door die priemfactoren worden gedeeld. Als je berichten versleutelt met '15' als publieke sleutel, kun je met privé-sleutels '3' en '5' elkaars berichten openen. Nu is dat bij 15 niet zo moeilijk, maar probeer maar eens te bedenken welke priemfactoren het onderstaande getal heeft:
57330641

Het bovenstaande getal heeft priemfactoren van 4 cijfers. Dat valt al niet mee, maar Whatsapp gebruikt priemgetallen van 60 cijfers. Kijk zelf maar eens: open een whatsappgesprek en klik op 'contact weergeven'. Klik daarna op 'versleuteling' en je krijgt het unieke priemgetal te zien waarmee jouw berichten worden versleuteld. Jouw code én die van je gesprekspartner vormen samen de publieke sleutel van 120 cijfers, een veilige 'kluis' voor jullie gesprek.

Oefeningen bij extra stencil 1

1. *Denkvraag:* hoelang zou een computer erover doen om de priemfactoren van een whatsapp-encryptie (120 cijfers) te berekenen?

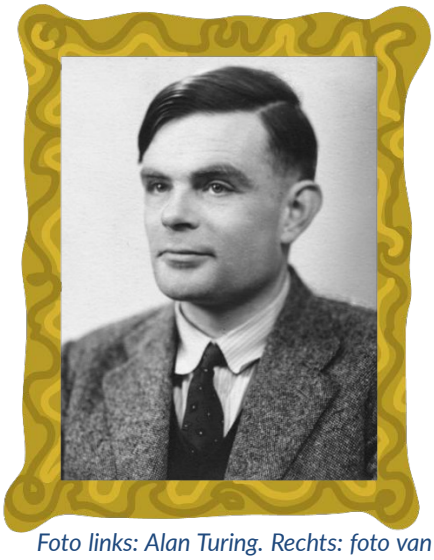
2. *Zoekvraag:* We weten nu dat encryptie voor versleuteling van berichten in Whatsapp wordt gebruikt. Zoek op internet: waarvoor wordt encryptie nog meer gebruikt? Noem ten minste vier dingen.

3. *Denkvraag*: wat zou er gebeuren als die encryptie bij de dingen in vraag 2 werd gekraakt?

2 - Kraken met brute kracht

Hoe kraak je een encryptiesleutel? Je kunt de eigenaar van de privésleutel natuurlijk lief aankijken, of proberen te bedriegen[1], maar dat werkt niet altijd. Je kunt natuurlijk ook één voor één alle codes uitproberen. Dat noemen we de 'brute kracht'-methode. Het voordeel: je krijgt het slot altijd open. Het nadeel: het kost tijd. Een simpel cijferslot, zoals op je reiskoffer, kun je nog wel met de hand kraken, maar bij langere encryptiesleutels duurt dat jaren.

Computers zijn hier gelukkig heel goed in: ze zijn er zelfs voor gemaakt. De wiskundige Alan Turing ontwierp in de Tweede Wereldoorlog een apparaat dat alle mogelijke combinaties van de Duitse geheime code in een paar minuten kon uitproberen: de *bombe*. Sommige wetenschappers beschouwen de bombe als de allereerste computer.
Inmiddels zijn we veel verder. Jouw laptop kan de codes van Julius Caesar makkelijk binnen enkele seconden kraken. Computerbeveiligers gebruiken daarom steeds langere codes voor encryptie.
Om een idee te geven: de encryptiecode van jouw Whatsappberichten is 128 cijfers lang. Het zou een gewone computer ongeveer een miljard jaar kosten om deze code met de 'brute kracht'-methode te kraken. Die sleutel is dus praktisch onbreekbaar en zo blijven je data veilig.



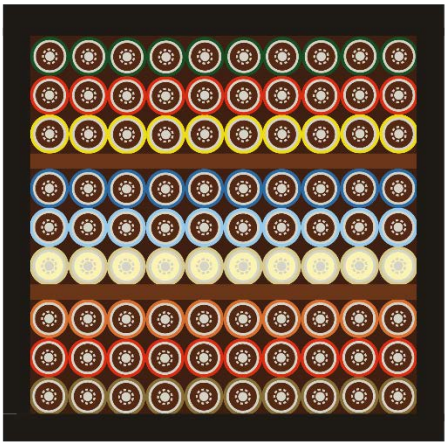


Foto links: Alan Turing. Rechts: foto van de Britse bombe. De echte ontcijfermachine waarmee Turing werkte, is uit elkaar gehaald. In het Bletchley Park museum staat deze replica.

[1] Dit heet ook wel 'social engineering': de zwakste schakel in de beveiliging, namelijk de mens, wordt bedrogen met *phishing mails* of ander bedrog.

Een quantumcomputer werkt anders

Een quantumcomputer met genoeg qubits[2] kan die code, waar een gewone computer misschien wel een miljard jaar over doet, binnen een paar minuten kraken. Dat komt door iets dat we 'superpositie' noemen: een qubit kan op twee plaatsen tegelijk zijn. Dankzij superpositie verschillende mogelijkheden tegelijk uitproberen. Vergelijk codekraken met het oplossen van een doolhofpuzzel: waar een klassieke computer één voor één alle wegen moet afleggen, kan een quantumcomputer zich 'opsplitsen' in superpositie en verschillende wegen tegelijk bekijken. Zo bepaalt hij supersnel welke route het meest waarschijnlijk is.
De docent laat je een filmpje van QuTech zien, waarin het verschil tussen een klassieke computer en quantumcomputer wordt uitgelegd.

Klassieke computer:

poging 1: omlaag, links leidt tot niets (2 stappen)

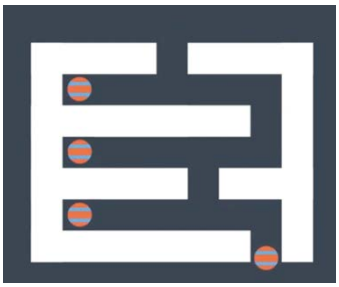
poging 2: een nieuwe bit erin: omlaag, rechts, omlaag, links: ook hier geen uitgang (4 stappen)

poging 3: nog een nieuwe bit: omlaag rechts, omlaag, links, omlaag, links: ook niet (6 stappen). Pas bij de vierde bit kom je eruit, na 7 stappen. In totaal na 2+4+6+7=19 stappen!

Quantumcomputer:

stap 1 – de qubit splitst zich op bij elk keuzepunt op in twee stappen: hier omlaag em dam links+rechts tegelijk!

stap 1 – de rechter qubit gaat omlaag, dan links en splitst op: links+omlaag



stap 3 – de laagste qubit gaat verder omlaag en dan links+rechts en vindt de uitweg. In totaal 7 stapen: omlaag, links+rechts, omlaag, links,_omlaag+links, links+rechts en omlaag,

[2] Qubits zijn de onderdelen van de quantumcomputer waarmee hij berekeningen uitvoert. In stencil 3 lees je meer over wat qubits zijn.

Opdrachten bij stencil 2

Leesvragen

1. Wat is het voordeel van de brute kracht-methode?

   _____

   _____

2. Wat is het nadeel van de brute kracht-methode?

   _____

   _____

3. Leg in eigen woorden uit waarom een quantumcomputer sneller is dan een gewone computer.

   _____

   _____

   _____

   _____

Denkvraag: wat denk je dat er gebeurt wanneer je encryptie gehackt wordt?

_____

_____

_____

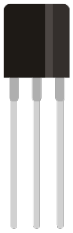
_____

3 – Liever een gewone computer, of een quantumcomputer?

Figuur 1 - Gordon Moore (1929-2023)

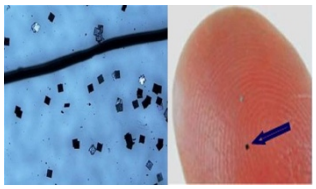
Gordon Moore merkte in 1975 dat de rekenkracht, en dus de snelheid, van computers iedere twee jaar ongeveer verdubbelt. Dit werd bekend als de *Wet van Moore*. Die wet zegt: "het aantal transistors op microchips verdubbelt elke twee jaar."

Transistors zijn kleine elektronische schakelaartjes. Een klassieke computer gebruikt transistors om mee te rekenen. Zoals je misschien weet, bestaat computertaal uit 1-en en 0-en. Elke 1 of 0 staat symbool voor een transistor die in de computer zit: 1 betekent de schakelaar staat op *aan*, 0 betekent de schakelaar staat op *uit*. Je kunt de transistors aan elkaar verbinden met een programma. Het programma zorgt dat de transistors op elkaars standen reageren, en zo kunnen computers dingen berekenen en informatie verwerken. Hoe meer transistors je hebt, hoe sneller je computer werkt.



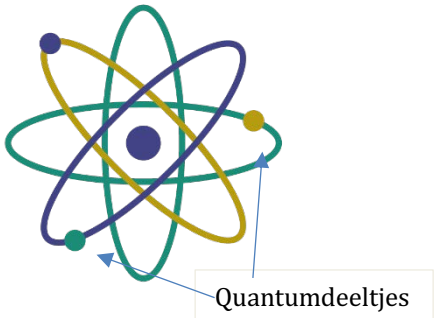
Figuur 2 - transistors in 1980

Uitgegroeid?
De 'Wet van Moore' mag dan een 'wet' heten, maar eigenlijk zegt Moore alleen maar wat hij in het verleden zag gebeuren en hoe het nu lijkt te gaan. Zijn wet voorspelt helemaal niets zekers voor de toekomst. Ook al worden transistors wel steeds kleiner, uiteindelijk is er een fysieke grens: kleiner dan kleinst kan niet. Zodra de allerkleinste transistor op het allerkleinste chipje zit, geldt de Wet van Moore niet meer. Er is dus een grens aan hoe snel klassieke computers kunnen worden.



Figuur 3 - de allerkleinste transistor in 2016

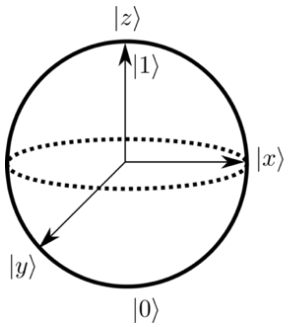
De toekomst: quantumcomputers?
Quantumcomputers gebruiken geen gewone transistors, maar 'qubits'. Qubits bestaan uit de allerkleinste deeltjes die de natuurkunde kent, nog kleiner dan moleculen en atomen. Sommige quantumcomputers werken met *lichtdeeltjes* (*fotonen)* en andere quantumcomputers werken met *elektronen*. Deze deeltjes zijn niet alleen heel erg klein, ze werken ook heel anders dan transistors. In plaats van 'aan' of 'uit' (1 of 0) kan een qubit in miljarden posities *tussen* aan en uit staan. Een qubit is dus een soort driedimensionaal lichtknopje, dat alle kanten tegelijk op kan. In de natuurkunde heet die positie tussen aan en uit 'superpositie'. De qubit blijft in superpositie *totdat* je op enter drukt en de qubit meet. Pas bij het meten verdwijnt de quantumwerking en staat hij gewoon op 1 of 0. Maar *voordat* je op enter drukt, kan de quantumcomputer er al mee rekenen. Op die manier kun je met heel veel mogelijke uitkomsten tegelijk werken.



Figuur 4 – een atoom

De quantumcomputers die nu[3] bestaan, kunnen helaas nog niet zoveel. De grootste quantumcomputer van dit moment heeft 1225 qubits, maar om beter te kunnen rekenen dan een klassieke computer heb je er minstens 100.000 nodig. Grotere quantumcomputers bouwen is erg moeilijk. Daar zijn allerlei redenen voor. Hieronder staan er twee.

Probleem 1: een quantumcomputer kan zijn eigen fouten niet verbeteren
Elke computer maakt weleens fouten. Je weet vast nog wel dat een klassieke computer vol met transistors zit. Die kunnen allemaal weleens verkeerd staan. Je computer controleert daarom altijd of er een fout in de berekening zit. Hij gebruikt daarvoor een kladblaadje, net als jij doet bij een moeilijke rekensom. De computer voert de berekening nog een paar keer uit op 'klad'-transistors en controleert of ze allemaal dezelfde uitkomst hebben. Als de uitkomsten verschillen, kiest hij de uitkomst die het vaakst voorkwam.
Bij een quantumcomputer werkt dat anders: van de qubits in superpositie kán de computer helemaal geen kladblaadje maken. Want qubits in superpositie bevinden zich in allerlei standen tegelijk. Zodra de computer probeert de qubit te controleren, verliest die zijn quantumwerking en springt vanzelf op 1 of 0. Quantumwetenschappers werken daarom hard aan manieren om tóch te kunnen controleren of een qubit een fout maakt.



Figuur 5 - een qubit kan alle kanten op, niet alleen maar naar boven of beneden

Probleem 2: hoe meer qubits, hoe meer en hoe groter de fouten
Je kunt die superkleine qubits niet zomaar met een koperdraadje aan elkaar verbinden, zoals we met transistors doen. Zelfs het kleinste draadje is namelijk veel groter dan de qubits zelf! Qubits kun je alleen aan elkaar verbinden met een ingewikkeld proces dat 'verstrengeling' heet. Zodra twee qubits met elkaar verstrengeld zijn, beïnvloeden ze elkaar. Dat brengt ons op het tweede probleem: hoe meer qubits je in je computer hebt, die verstrengeld en in superpositie zijn, hoe groter de fouten die ze kunnen maken.

Quantumcomputers zijn er al!
In het QuTech laboratorium van de Technische Universiteit Delft staat de Quantum Inspire quantumcomputer. Die heeft een paar qubits, maar hij werkt wel. Hij staat altijd aan.
Iedereen kan de Quantum Inspire via internet gebruiken, gewoon vanaf zijn eigen klassieke computer! Waarschijnlijk gaan we quantumcomputers uiteindelijk op die manier gebruiken.
Een stap verder: als je gevoelige informatie veilig willen versturen, dan heb je straks een kleine quantum-PC nodig en de ontvanger ook. De communicatie loopt dan helemaal over een quantumnetwerk met verstrengelde qubits. Misschien zit daar dan een super-quantumcomputer tussen als knooppunt om de veiligheid van de verbindingen te garanderen.

[3] In 2024

Opdrachten bij stencil 3

kijk eerst het filmpje in de klas en beantwoord daarna de vragen

Leesvragen

1. Wat is de Wet van Moore?

   _____
   _____

2. Noem twee verschillen tussen een klassieke computer en een quantumcomputer

   _____
   _____
   _____
   _____

3. Hoe zou jij een quantumdeeltje in superpositie tekenen?

4. Wanneer zijn twee qubits verstrengeld?

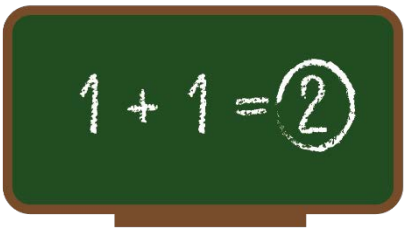
   _____
   _____

Denkvraag: hoelang denk jij dat het duurt voor de eerste grote, werkende quantumcomputer er is?

4 – Wie is verantwoordelijk?

Als je wilt beoordelen of je iets goed hebt gedaan, helpt het vaak om er vanuit verschillende kanten naar te kijken. In de filosofie zijn er grofweg drie manieren om dat te doen:

1. **Je kijkt naar de uitkomst.**



'Streef naar het grootste geluk voor het grootste aantal', zei Jeremy Bentham. Je kunt heel makkelijk bepalen wat het goede is om te doen. Je kijkt naar wat jouw keuze voor gevolgen zal hebben. Hoeveel mensen/dieren worden er gelukkig als je dit doet? En hoeveel mensen/dieren worden er ongelukkig van? Worden ze érg gelukkig/ongelukkig of maar een beetje, en duurt hun geluksgevoel lang of kort?
Dan kies je de beste balans: zo véél mogelijk geluk en zo min mogelijk pijn, voor zoveel mogelijk mensen én dieren. Volgens Bentham kun je deze balans gewoon uitrekenen: tel al het geluk bij elkaar op, trek daar alle pijn vanaf, en streef naar het hoogste totaal.

Bijvoorbeeld: er is nog één snoepje over. Jij wilt hem, maar ik ook. Wie wordt er het gelukkigst van? Die moet hem volgens Bentham krijgen.

2. **Je kijkt naar de bedoelingen**

Iedereen maakt ongelukken: je hebt vast wel eens iets laten vallen, gemorst of iemand verdrietig gemaakt zonder dat dat je bedoeling was. Heb jij dan evenveel schuld als iemand die al die dingen expres doet?

Immanuel Kant vond van niet. Of iets goed of slecht is, kan volgens hem niet afhangen van het toeval. Het enige dat volgens Kant *altijd* goed is, is de 'goede wil'. Maar wanneer is jouw wil goed? Volgens Kant kun je dat met je eigen verstand bepalen: stel jezelf de vraag of de *regel* die jij volgt met je keuze voor *iedereen* kan gelden.

Bijvoorbeeld:
Keuze: ik loop door rood.
Regel: "Je mag door rood lopen als je haast hebt"
Kun je nog op tijd komen als iedereen door rood zou lopen?

3. **Je kijkt naar degene die de keuze maakt**

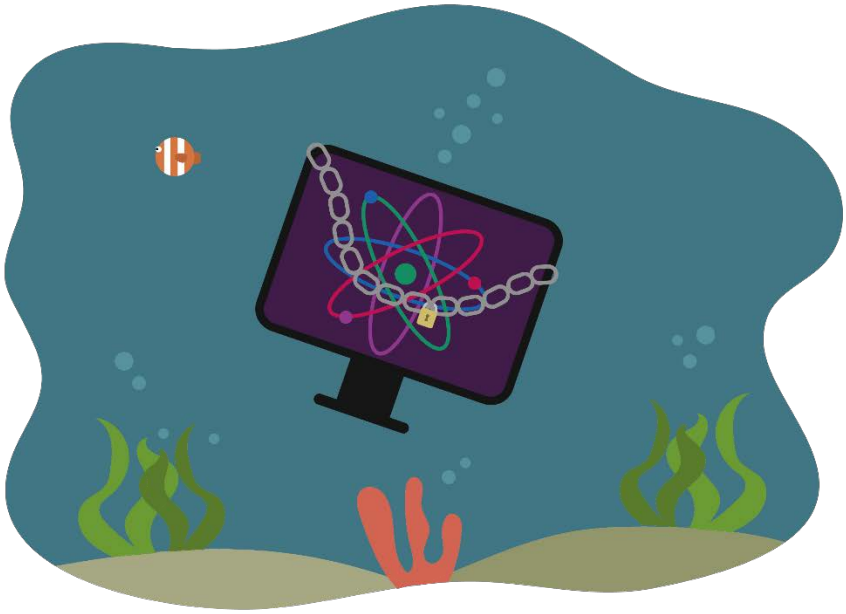
Regels over de gevolgen of de bedoelingen van je keuzes zijn natuurlijk belangrijk, maar elke situatie is anders. Past één regel echt op alle duizenden verschillende situaties in een mensenleven? Daar komt nog bij dat je niet alleen moet wéten wat de juiste keuze is, je moet het ook nog echt *doen*. Volgens Aristoteles heb je daarom *inzicht* en een *goed karakter* nodig om goede keuzes te maken. Inzicht om te weten welke regels er bij de situatie passen en een goed karakter dat jou motiveert. Wanneer je inzicht en een goed karakter hebt, ben je - volgens Aristoteles- een wijs en volmaakt mens. Zo'n mens zal altijd het goede kiezen. Hij geeft zelfs een manier om zo'n mens te worden: je begint met veel oefenen en het helpt ook om een voorbeeld te nemen aan een wijs mens dat jij kent.

Bijvoorbeeld:
Je bent vanavond vrij dus kun je kiezen uit: je huiswerk maken of nog even gamen op je telefoon.
Vraag jezelf: wat zou een wijs mens in dit geval doen?

Stencil 5: Red het systeem

Het hele netwerk in de school ligt plat. Er moet een nieuw systeem komen. De vraag is: moet het een klassieke computer of een quantumcomputer worden? Je hebt de afgelopen weken gezien hoeveel chaos er kan ontstaan wanneer een computer verkeerd gebruikt wordt. Jullie uitdaging is om tezorgen dat er een nieuw systeem komt en bovendien dat jullie (quantum) computer niet in slechte handen komt. Hoe bepaal je trouwens wie de goede handen heeft?

Opdracht: Bedenk samen met één of twee klasgenoten een plan voor een nieuw systeem. Jullie hoeven het niet zelf te bouwen, maar wees wel nauwkeurig, want de systeembouwer doet precies wat jullie hem opdragen. Bedenk welke dingen het systeem moet kunnen en wat volgens jullie de beste beveiliging voor het systeem is. Beantwoord daarvoor eerst de onderstaande vragen. Beschrijf of teken daarna hoe jullie systeem eruit moet zien.



- Welk soort computer kiezen jullie? Een quantumcomputer of een klassieke computer?
    - Schrijf op waarom jullie voor dit type computer kiezen.

- Maak een lijst met eigenschappen waaraan het systeem moet voldoen.
    - Hoe zorg je dat de computer niet verkeerd gebruikt kan worden?
    - Hoe zorg je dat de computer blijft werken in de toekomst?
    - Hoe zorg je dat de computer in goede handen blijft? En hoe bepaal je wat die goede handen dan zijn?

- Schrijf op voor welke dingen het systeem gebruikt mag worden.

- Moet iedereen in het systeem kunnen? Waarom wel/niet?

- Teken hoe het systeem eruit moet zien. Teken jullie ontwerp zó, dat de belangrijkste dingen uitvergroot zijn en benoem de onderdelen van je tekening. Je mag pijltjes gebruiken.

Verdieping

- Kunnen jullie met jullie systeem een oplossing bedenken voor de schaalvergroting zoals beschreven in stencil 3?
- Is er een medicijn dat je als eerste wilt ontwikkelen? Welk medicijn is dat? Waarom dat medicijn?