De Baas Op Internet

Module 5:

Encryptie

Leerkrachtinstructie

Ontwikkeld door:

waag society

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

NETWERK DEMOCRATIE

Gerealiseerd met bijdragen van:

SIDN fonds

FONDS 21

debaasopinternet.nl

Onderzoek:

OP ELK SLOT PAST EEN SLEUTEL?

Wat is de geheimtaal die computers gebruiken? Hoe zet je iets digitaal op slot? En wat als je de digitale sleutel kwijtraakt, krijg je het dan nog open? Deze module gaat over de computer als versleutelaar van jouw informatie en ontdekken hoe digitale encryptie werkt. Hoe kan het dat bedrijven niet mee kunnen lezen of kijken in de dingen die we via hun diensten versturen? Of kunnen en doen ze dat wel?

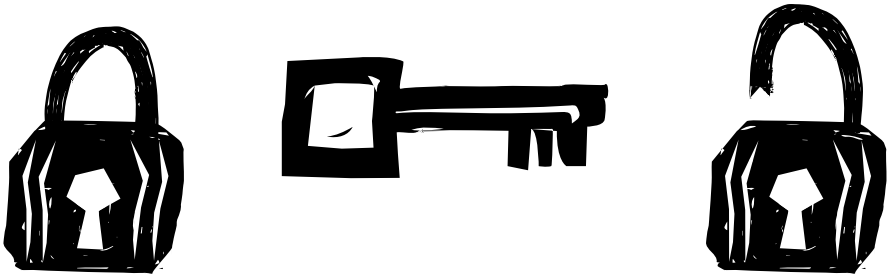
	Thema Door zelf aan de slag te gaan met het principe van zogenaamde ‘public keys’ en ‘private keys’ leren we wanneer digitale berichten veilig verzonden worden, zonder dat er meegelezen kan worden. We komen erachter dat we digitale encryptie ook zelf kunnen gebruiken, of dat misschien al doen.		**Doelgroep** PO groep 7 en 8 VO 1e en 2e klas **Lesduur** 1,5 uur (of 2x 45 minuten)
	Lesdoel Inzicht in de onderliggende principes en relevantie van digitale versleuteling op internet.		**Benodigdheden** Werkbladenset (1 per leerling) Stiften (gekleurd) Grote vellen papier (1 vel per groepje) Kistje Snoepjes 2 Hangsloten met sleutel
	Voorbereiding Lesmateriaal downloaden Lesmateriaal doornemen Werkbladen printen Materialen verzamelen		**Vakgebieden** Deze module draagt bij aan de PO kerndoelen: Nederlands: 2, 3, 4 Rekenen/wiskunde: 23 Oriëntatie op jezelf en de wereld, Natuur en techniek: 44,45 Deze module draagt bij aan de VO kerndoelen: Nederlands: 1, 6 Mens en natuur: 29, 31, 33 Mens en maatschappij: 36, 38, 39 De module kan gegeven worden binnen de vakken informatica, techniek, maatschappijleer en de mentorles.

Stap 1	**Sloten en sleutels** In tweetallen kijken we naar de basis van iets beveiligen: Wat zijn dingen die we afsluiten? Dit kan alles zijn, van dakraam tot garagebox tot smartphone. En hoe maken we ze open?
Stap 2	**Hacken** In dezelfde tweetallen denk je na over hoe je de eerder genoemde dingen open kunt maken of breken zonder de sleutel/toegangscode. Hoe gaat een deur open zonder sleutel? Hoe gaat een fietsslot open zonder code? In de computerwereld wordt het openen van dingen zonder originele sleutel ‘hacken’ genoemd.
Stap 3	**Digitale versleuteling (Encryptie)** Ook op internet heeft ieder slot een sleutel. Die sleutel kan je namaken of stelen, maar gelukkig kunnen we het door digitale encryptie wel heel moeilijk maken voor ongewenste meelezers om die sleutel te bemachtigen. Met een kistje, hangsloten, sleutels en snoepjes verkennen we hoe ‘public key’ encryptie werkt.
Stap 4	**Veilig chatten** De ‘public key’ encryptie is onder andere heel geschikt voor het beveiligen van e-mail, maar met de apps op je smartphone gebruik je het internet voor veel meer vormen van communicatie. Hoe kunnen we onze informatie daar beveiligen? We verkennen wat je belangrijk vindt aan een chatapp en hoe je je online privacy kunt vergroten.

Extra stap	**Onkraakbare codes en priemgetallen** Wanneer je van een wiskundige uitdaging houdt doe dan deze extra stap: Rekenen met codes en priemgetallen. Ontdek hoe public keys en private keys uniek kunnen zijn en alleen bij elkaar horen (en niet bij een andere code).

Belangrijke ideeën:

- Een goed wachtwoord gebruiken is de eerste drempel om mensen ervan te weerhouden mee te lezen. Een goed wachtwoord is moeilijk te raden en bevat kleine letters, hoofdletters, cijfers en leestekens. Maar het moet simpel genoeg zijn om uit je hoofd te leren.
- Een sterk wachtwoord zorgt er nog niet voor dat bedrijven niet mee kunnen lezen. Daarvoor heb je encryptie nodig.
- In deze module gaan we in op public keys en private keys, de digitale oplossing voor het ‘sleutelprobleem’.



Onleesbaar

Een pinpas en de bijbehorende pincode worden nooit in dezelfde envelop naar je toegestuurd. Ook zie je aan de buitenkant van de envelop met pincode niet dat deze van je bank afkomstig is. De envelop is zo neutraal mogelijk vormgegeven en de pincode wordt alleen zichtbaar wanneer je een speciale sticker van het papier haalt. Hierdoor kan je de pincode niet achterhalen door de envelop tegen het licht te houden. Dit is een soort papieren vorm van encryptie. De boodschap wordt ‘onleesbaar’ gemaakt voor ongewilde meelezers.

Sleutelprobleem

Het ‘sleutelprobleem’ (ook besproken in de module Geheimtaal) houdt in dat een versleuteld bericht en de sleutel altijd beide verzonden moeten worden naar de ontvanger. Net als een nieuwe pinpas en pincode. Wanneer iemand beide onderschept kan diegene de boodschap ontcijferen. Wanneer een versleutelde e-mail onderweg onderschept wordt, en ook de digitale sleutel wordt onderschept, kan de e-mail alsnog gelezen worden. Daar merk je als gebruiker niets van, want de e-mail komt ook gewoon bij jou aan!

Een aantal wiskundigen heeft daarom een publieke sleutel en een privé sleutel ontworpen. In deze module ontdekken we hoe dit werkt.

Publiek en privé

Een public key en een private key horen bij elkaar. Het zijn een slot en een sleutel, of eigenlijk: een som en het antwoord.

De public key deel je online met iedereen. Het is een soort open hangslotje waarvan alleen jij de sleutel hebt. Als iemand jou een versleuteld bericht wil sturen dan gebruikt hij jouw public key: een code waarmee het bericht versleuteld wordt. Ze hoeven het hangslotje als het ware alleen maar dicht te klikken en dan zit het op slot. Net als een deur die achter je in het slot valt. Alleen de ontvanger beschikt over de private key: de som waarmee het antwoord van de public key te achterhalen is. Die som bestaat altijd uit priemgetallen, zodat er niet meer dan één goede oplossing is.

Goede wachtwoorden

Encryptie zoals met een public key en private key werkt vooral goed bij e-mailverkeer. Ook voor je andere internetgedrag moet je je beschermen tegen inbrekers. In de stappen in deze module ontdek je hoe je dat kunt doen.

Belangrijke begrippen:

- **Encryptie**
  Het versleutelen van informatie zodat niet iedereen kan meelezen of kijken.

- **Public key**
  De lange code die je online deelt met iedereen. Mensen die je een versleutelde e-mail willen sturen kunnen je public key gebruiken als een soort hangslot. Ze sluiten het bericht ermee af voor ongewenste meelezers.

- **Private key**
  Je private key is de sleutel op het hangslot van de public key. Beiden horen bij elkaar. Je private key deel je met niemand.

- **Priemgetallen**
  Een getal dat alleen te delen is door zichzelf en elkaar. Bijvoorbeeld 7, 13 en 7823. Gek genoeg is het cijfer 1 geen officieel priemgetal. Dit fimpje legt het uit:

  “Wat zijn priemgetallen?” - Clipphanger, NTR
  https://www.youtube.com/watch?v=5udOCr72ZT0

Verdieping:

- **“Hoe werkt encryptie op internet?” - De Correspondent**

  Dit artikel van Emiel Lijbrink legt uitgebreid uit hoe encryptie werkt en waar het online toegepast wordt.

  https://decorrespondent.nl/691/hoe-werkt-encryptie-op-internet/52838769555-c6c0f16c

- **“Hoe beschermen priemgetallen mijn data?” - De Correspondent**

  Dit artikel van Emiel Lijbrink gaat in op hoe grote priemgetallen onze informatie versleutelen.

  https://decorrespondent.nl/698/hoe-beschermen-priemgetallen-mijn-data/53374039290-48ecfeae

TIJD:	OEFENING:	WERKVORM:	MATERIAAL:
10 min.	**Introductie** ➔ **Stel een paar prikkelende vragen:** - Wat is voor iedereen vrij in te zien op internet? - En wat niet? - Hoe veilig is het internet? - Hoe privé zijn privé berichten? Hoe zorg je ervoor dat niet iedereen op internet overal bij kan? Deze module gaat over de computer als versleutelaar van jouw informatie. ➔ **Kom kort terug op de module over Geheimtaal:** - Wat weten jullie nog over geheimtaal en cryptografie? Gebruik ook de inzichten uit de modules Privacy en Internet om terug te blikken op het feit dat informatie via veel verschillende partijen bij de ontvanger komt. - Wanneer mogen deze partijen wat jou betreft meelezen? En wanneer liever niet? Wat is de geheimtaal die computers gebruiken? Hoe zet je iets digitaal op slot? En wat als je de digitale sleutel kwijtraakt, krijg je het dan nog open? Dat gaan we deze module ontdekken.	***Klassikaal***	***Schoolbord***
20 min.	**Stap 1 - Sloten en sleutels** We beginnen met herkenbare voorbeelden van dingen die op slot kunnen. Door daarover na te denken, begrijpen we straks beter hoe men op internet informatie zoals e-mails en Whatsapp berichten kan beveiligen. ➔ **Loop rond en spoor leerlingen aan om na te denken over welke sloten ze het meest belangrijk vinden.** Is het belangrijker dat je brievenbus op slot kan? Of dat je fiets op slot kan? ➔ **Vraag leerlingen waarom ze het belangrijk vinden om iets te beschermen.** Zit er een code op hun smartphone? Hebben ze dingen op hun computer staan die ze willen beschermen? Wie mag wel meekijken? Wie niet? (Mogen je ouders alles zien? Mag je leraar alles zien?) **Afronding**: Benadruk het belang van versleuteling en privacy. Iedereen heeft het recht om bepaalde dingen privé te willen houden.	***Tweetallen***	***Werkbladen*** ***Pennen***

TIJD:	OEFENING:	WERKVORM:	MATERIAAL:
10 min.	**Stap 2 - Hacken** De leerlingen vullen Stap 2 op hun werkblad in. Hoe krijg je bovenstaande sloten open zonder de 'sleutel'? Oftewel: Hoe zijn ze te 'hacken'? **Extra**: Computer hackers breken niet altijd in om slechte redenen. Er zijn ook goede redenen om te hacken en dus ook andere soorten hackers. Kijk bijvoorbeeld deze filmpjes met de klas: "Lucas duikt in de wereld van het hacken" - Zapp Weekjournaal: https://www.youtube.com/watch?v=UBrH5-Kdkd8 "Hacken - Wat is dat precies?" - Bastanieuws, AT5: https://www.youtube.com/watch?v=KFQGr5HguQU **Afronding**: Gelukkig kun je huizen, auto's en fietsen goed beveiligen tegen inbrekers. Computers kun je ook beveiligen, in de volgende stap leren we hoe.	***Tweetallen***	***Werkbladen*** ***Pennen***
25 min.	**Stap 3 - Digitale versleuteling (encryptie)** Ieder slot heeft een sleutel... ook online... en sleutels kun je stelen of namaken. Hierdoor is alles (uiteindelijk) te hacken. Maar door gebruik van encryptie kun je het ongewenste meelezers wel heel moeilijk maken. Hoe werkt deze computergeheimtaal? Digitale versleuteling werkt vaak met meerdere sloten en sleutels. We gaan demonstreren hoe de zogenaamde 'public key' encryptie werkt. Met behulp van snoepjes. **➔ Volg de stappen:** a. Zet twee leerlingen neer in het klaslokaal. Hoe verder ze van elkaar verwijderd staan, hoe leuker het is. b. Introduceer het kistje met snoepjes dat straks via het internet van de ene leerling (verzender) naar de andere leerling (ontvanger) wordt verzonden. c. Zet meerdere leerlingen tussen de verzender en de ontvanger. Deze leerlingen symboliseren samen het internet.	***Klassikaal & Tweetallen***	***Kistje Snoepjes*** ***2 hangslotjes*** ***Werkblad 'Sleutelprobleem' (2 stuks per duo)***

TIJD: **OEFENING:** **WERKVORM:** **MATERIAAL:**

Verdieping: Geef eventueel de leerlingen die het internet vormen een specifieke rol:

- internet provider
- datacenter
- overheid
- adverteerder
- openbare wifi provider
- hacker

d. Het kistje wordt doorgegeven via een ketting van leerlingen naar de ontvanger.

e. De kans is groot dat de partijen die de boodschap hebben overgedragen, de boodschap hebben bekeken, of wellicht zelfs opgegeten (laat dit gebeuren, zorg dat je vooraf een paar snoepjes overhoudt voor de volgende stappen).

f. Herhaal de voorgaande oefening, maar nu doet de verzender het kistje op slot met een hangslotje. De sleutel stuur je achter het gesloten kistje aan. Oplettende leerlingen zorgen dat het kistje en de sleutel tegelijk bij hen komen, om zo alsnog een snoepje te kunnen pakken.

g. Laat de leerlingen in tweetallen de oplossing voor dit sleutelprobleem bedenken. Daarbij gebruiken ze het werkblad ‘Sleutelprobleem’. (Geef zo nodig als tip dat het kistje misschien meerdere keren heen en weer moet reizen.)

h. Laat weten wat de oplossing kan zijn: Leerling B doet na ontvangst van het gesloten kistje, zijn slot er bij op en stuurt het terug naar A.

   A haalt vervolgens zijn eigen slot eraf en stuurt het terug. B kan nu het eigen slot weer openen en de inhoud van het bericht bekijken.

i. Boodschap: Inefficiënte encryptie, snoepjes maken de reis drie keer. Dat kan beter!

j. Maak met het werkblad ‘Sleutelprobleem’ weer een oplossing, maar dan een die de reis maar 1 keer aflegt.

Afronding: Dit idee van een publiek slotje dat iedereen mag gebruiken (de public key) en een privé sleutel (private key) die maar door een iemand te gebruiken is, is hoe internet encryptie werkt. Je kunt dit bijvoorbeeld voor je e-mail installeren.

TIJD:	OEFENING:	WERKVORM:	MATERIAAL:
20 min.	**Stap 4 - Veilig chatten** Niet alle internetdiensten kun je beveiligen via private keys en public keys. Soms moet je andere beveiligingsmanieren gebruiken. Met de klas nemen we chat-apps onder de loep. Op het werkblad brengen leerlingen in kaart wat zij belangrijk vinden in het gebruik en de veiligheid van een chat-app. Ook kijken ze welke apps daaraan voldoen. **Afronding**: Bespreek na het invullen van het werkblad welke apps het meest geschikt zijn volgens de leerlingen. Wat zijn de voor- en nadelen van Whatsapp? Is het een idee om met z'n allen over te stappen naar een nieuwe chat-app? Waarom wel of niet? De meest actuele versie van het overzicht op het werkblad is hier te vinden: https://toolbox.bof.nl/playlist/mobiel/4/ Hierin staat ook uitgelegd wat de verschillende kolommen betekenen.	***Individueel & Klassikaal***	***Werkblad***
5 min.	**Afronding** **➔ Sluit af met de vraag:** - Wie is volgens jullie de baas van de gegevens op internet? Is dat de ontvanger? En blijft dat de ontvanger ook als de boodschap onversleuteld wordt verstuurd? - En als je gehackt wordt? Wie is dan de baas?	***Klassikaal***	
20 min.	**Extra stap: Onkraakbare codes en priemgetallen** We gaan nu gezamenlijk kijken wat de computerlogica is waarmee bestanden versleuteld worden. Omdat de computer met cijfers werkt, lijkt dit een beetje op wiskunde. Maar eigenlijk is het heel simpel. **➔ Schrijf de volgende som op het bord:** ? x ? = 12 Een public key (slot) en private key (sleutel) worden altijd tegelijk gemaakt. Ze horen bij elkaar, net als een som en het antwoord. Stel we gaan een bericht versleutelen met de public key van leerling B en deze public key is het getal 12. Vraag de leerlingen wat de mogelijke sommen zijn waar 12 het antwoord op is.	***Klassikaal***	***Schoolbord / Digibord***

De mogelijke oplossingen zijn 3 sommen:

1 x 12 = 12
2 x 6 = 12
3 x 4 = 12

Dat is niet handig, je hebt dus 3 mogelijke sleutels.
Je zoekt een slot dat maar 1 oplossing heeft.
Vraag: Wat zijn priemgetallen? Leg dit uit als het niet bekend is. Of kijk samen dit filmpje:

https://www.youtube.com/watch?v=5udOCr72ZT0

Schrijf op het bord en maak gezamenlijk de som:

Stel je public key is 21.

? x ? = 21

7 x 3 = 21

Dus:
Je public key is 21.
Dan bestaat je private key uit de priemgetallen 3 en 7.

Nu andersom. Je public key is 143. Welke priemgetallen zitten erachter?

Antwoord: 11 en 13 vormen samen je private key.

In werkelijkheid gebeurt dit met veel langere cijfer- en letterreeksen, die veel lastiger te kraken zijn.

➔ **Kijk eventueel tot slot het laatste deel van deze video van CANVAS, die legt het encryptie principe met een public key en private key nogmaals uit.**

“Priemgetallen en encryptie” - CANVAS

https://youtu.be/SM28-2GQCWI?t=3m38s

Antwoorden:

Niet van toepassing in deze module. De goede antwoorden zijn meegenomen in de klassikale toelichting door de leerkracht.