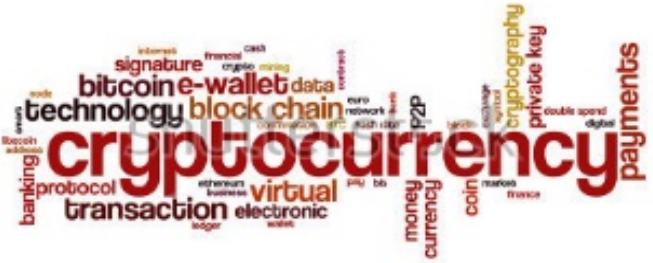
platform wiskunde nederland

Wiskunde in je broekzak: cryptografie in het dagelijks leven.

Vakantiecursus 2018

Eindhoven, 24 en 25 augustus 2018

Amsterdam, 31 augustus en 1 september 2018



Vakantiecursus2018

Voor leraren in de exacte vakken aan havo, vwo, hbo leerlingen en andere belangstellenden organiseert het Platform Wiskunde Nederland (PWN) in 2018 een vakantiecursus met als thema:

"Wiskunde in je broekzak: cryptografie in het dagelijks leven"

Dit jaar betreft het een tweedaagse cursus, **vrijdag 24 augustus** en **zaterdag 25 augustus** aan de TU Eindhoven, Den Dolech 2, 5612 AZ Eindhoven en op **vrijdag 31 augustus** en **zaterdag 1 september** bij het CWI, Science Park 123, 1098 XG Amsterdam (de routebeschrijvingen staan aan het einde van deze brochure).

De cursus is voor wiskundedocenten van elk niveau toegankelijk. De deelnemers ontvangen bij aanvang van de cursus een syllabus met teksten van de voordrachten. Het cursusgeld bedraagt €95. Voor studenten van lerarenopleidingen is het cursusgeld slechts €35. Voor gepensioneerden geldt een speciaal tarief van €50.

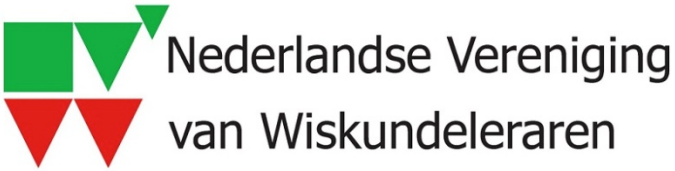
Bij de cursus is inbegrepen een warme maaltijd op vrijdag en een lunch op zaterdag.

De brochure kunt u downloaden door middel van deze link:
http://www.platformwiskunde.nl/vakantiecursus

Aanmelding
Aanmelding voor deelname aan de cursus kan:
- door het aanmeldingsformulier achter in deze brochure in te vullen en vóór 1 augustus 2018 op te sturen aan PWN;
- via de website van Platform Wiskunde Nederland: http://www.platformwiskunde.nl/vakantiecursus waar een online registratieformulier ingevuld en opgestuurd kan worden, eveneens vóór 1 augustus 2018.

Deze cursus geldt als nascholingsactiviteit. Voor geïnteresseerden is een nascholingscertificaat beschikbaar. Degene die daar prijs op stelt, gelieve het betreffende vakje aan te kruisen op het aanmeldingsformulier. Omdat zaken rondom "Register Leraar" momenteel aan verandering onderhevig zijn, is het mogelijk dat er een andere wijze van registratie plaatsvindt.

Sponsoring
Deze cursus wordt mede mogelijk gemaakt door een subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), en een bijdrage van 4TU.AMI, het toegepaste wiskunde instituut van de 3 Nederlandse technische universiteiten alsmede de universiteit van Wageningen. Organisatie vindt plaats in samenwerking met het Centrum voor Wiskunde en Informatica (CWI), de Technische Universiteit Eindhoven (TU/e) en de Nederlandse Vereniging van Wiskundeleraren.



Programma Eindhoven

24 en 25 augustus 2018

vrijdag 24 augustus

Wijzigingen voorbehouden.

15.00-15.30	Ontvangst, koffie
15.30-15.35	Welkomstwoord
15.35-16.20	Algemene inleiding Cryptografie Benne de Weger
16.20-16.45	Pauze
16.45-17:30	Introductie Bitcoin Benne de Weger
17.30-18.30	Diner
18.30-19.15	Praktikum
19.15-19.45	Pauze
19.45-20.30	Bitcoin: een blik onder de motorkap Boris Skoric

zaterdag 25 augustus

09.30-10.00	Ontvangst, koffie
10.00-10.45	Crypto achter de browser Benne de Weger
10.45-11.15	Pauze
11.15-12.00	Authenticeren met privacy én veiligheid Greg Alpar
12.00-13.00	Lunch
13.00-13.45	Praktikum
13.45-14.30	Crypto door de eeuwen heen Een lezing verzorgd door het Cryptomuseum
14.30	Afsluiting

Programma Amsterdam

31 augustus en 1 september 2018

vrijdag 31 augustus

Wijzigingen voorbehouden.

15.00-15.30	Ontvangst, koffie
15.30-15.35	Welkomstwoord
15.35-16.20	Algemene inleiding Cryptografie Benne de Weger
16.20-16.45	Pauze
16.45-17:30	Introductie Bitcoin Benne de Weger
17.30-18.30	Diner
18.30-19.15	Praktikum
19.15-19.45	Pauze
19.45-20.30	Bitcoin: een blik onder de motorkap Boris Skoric

zaterdag 1 september

09.30-10.00	Ontvangst, koffie
10.00-10.45	Crypto achter de browser Benne de Weger
10.45-11.15	Pauze
11.15-12.00	Authenticeren met privacy én veiligheid Greg Alpar
12.00-13.00	Lunch
13.00-13.45	Praktikum
13.45-14.30	Crypto door de eeuwen heen Een lezingverzorgd door het Cryptomuseum
14.30	Afsluiting

Wiskunde in je broekzak: cryptografie in het dagelijks leven.

Ten geleide

Cryptografie is het gebied van de wiskunde waarin het maken van geheimschriften wordt bestudeerd. De cryptografie kent een lange geschiedenis. Net zoals in vroeger tijden de verzegeling van vertrouwelijke berichten, moet een cryptografische techniek helpen de identiteit vast te stellen en een vertrouwensbasis te creëren. De Mesopotamiërs gebruikten zegelrollen om een kleitablet van een 'handtekening' te voorzien; later vormden lakzegels een beveiliging. De Enigma-coderingsmachine werd tot de Tweede Wereldoorlog veel gebruikt om informatie te versleuetlen. De Duitsers vertrouwden er tot het einde van de Tweede Wereldoorlog op dat de berichten, die door deze machine gecodeerd waren, volstrekt veilig verzonden konden worden. Een fout, die hen fataal is geworden. Velen zien het breken van de Enigma-codering door de Britten en Polen als het grote keerpunt in de Tweede Wereldoorlog.
Het belang van het versleutelen van informatie is toegenomen met de komst van internet. Steeds vaker hebben mensen, bewust of onbewust, te maken met cryptografie, doordat mensen het internet gebruiken om gegevens te versturen die ze alleen aan de geadresseerde toevertrouwen. Denk bijvoorbeeld aan e-mailen on online bankieren. Bankbiljetten bevatten moeilijk na te maken afbeeldingen en een watermerk, en een modern betaalpasje bevat een geheime elektronische vingerafdruk. In feite is er niet zo'n groot verschil tussen betalingen met tastbaar geld en moderne, elektronische betaalwijzen. In alle gevallen gaat het om wederzijds vertrouwen.
Veel gebruikte versleutelingstechnieken zijn de Data Encryption Standard, Advanced Encryption Standard en RSA. De laatste is de afkorting van de drie beroemde cryptologen Ron Rivest, Adi Shamir en Leonard Adleman. De kracht van RSA is erop gebaseerd dat het heel moeilijk is om, gegeven het product van twee grote priemgetallen, de twee priemfactoren te vinden. Met de nu bekende technieken vergt dat jarenlang rekenen met een computer. Maar de wetenschap en de techniek staan niet stil. Het is niet ondenkbaar dat RSA en andere codes die gebaseerd zijn op grote priemgetallen, in de toekomst eenvoudig te kraken zijn met behulp van kwantumcomputers. Een van de modernste ontwikkelingen in de cryptografie is kwamtum-encryptie. Kwantum-encryptie is gegarandeerd veilig: elke poging tot afluisteren is meteen zichtbaar voor zender en ontvanger. Zo weten ze zeker dat niemand de sleutel tot de code in handen kan krijgen.
In deze vakantiecursus bespreken we een aantal aspecten van de moderne cryptografie, en gaan we in op de daarachter liggende wiskundige technieken. Er zal veel ruimte zijn voor zelfwerkzaamheid.

We hopem weer veel wiskundeleraren te mogen verwelkomen op een inspirerende vakantiecursus 2018!

Platform Wiskunde Nederland,
Wil Schilders, voorzitter programma comité VC 2018, en Benne de Weger, hoofdspreker en initiator van deze vakantiecursus.

Wiskunde in je broekzak

Benne de Weger
TU Eindhoven
b.m.m.d.weger@tue.nl

Welke wiskunde zit er in je broekzak? Daar vind je wellicht je portemonnee met pasjes, en je mobiele telefoon: daar zit best wel de nodige wiskunde in.
Maar heb je die echt "in je broekzak"?

Het thema van de PWN Vakantiecursus 2018 is Cryptografie: de wiskunde van het beveiligen van gegevens door middel van versleuteling en authenticatie.
De vakantiecursus zal dit jaar, meer dan de laatste jaren, een echt cursus-karakter hebben, allereerst door een toegespitster thema. Maar ook door de opzet: in een aantal lessen door dezelfde docent zal de basistheorie behandeld worden, waarna enkele wat meer specifieke onderwerpen diepgaander behandeld gaan worden door andere sprekers.

Die basis bestaat uit: symmetrische cryptografie, cryptanalyse (het 'kraken' van cryptografische systemen), asymmetrische cryptografie (met name RSA en crypto gebaseerd op Elliptische Krommen) en de achterliggende getaltheorie, en het gebruik ervan in de praktijk, met name het beveiligen van gegevens op het Internet (TLS / https, certificaten). Ook wordt een inleiding gegeven op hashfuncties. Tijdens de lessen zal er ruimte zijn voor het zelf oefenen met de stof.

Voor de specifiekere onderwerpen zal in ieder geval de wiskunde achter Blockchains (Bitcoin) aan de orde komen, en hoe privacy met behulp van cryptografie op een smartcard gestalte kan krijgen (denk aan: hoe kun je op een volledig controleerbare manier aantonen dat je 18+ bent zonder je geboortedatum, of je naam en adres, te hoeven afgeven).

Andere mogelijke onderwerpen zijn de gevolgen van quantum-computing voor cryptografie, of een meer historisch gerichte voordracht.

Bitcoin: een blik onder de motorkap

Boris Skoric
TU Eindhoven
b.skoric@tue.nl

Bitcoin en andere zogeheten "cryptocurrencies" zijn regelmatig in het nieuws.
In dit college worden de ontwerpprincipes van Bitcoin onder de loep genomen: het gebruik van digitale handtekeningen om betalingen te authenticeren, het gebruik van hash-puzzels om iemand tijdelijk autoriteit te geven, en hoe dat alles cryptografisch aan elkaar geknoopt wordt tot een werkende valuta.
Verder kijken we naar verschillende soorten transacties en wat voor invloed die hebben op privacy.

Authenticeren met privacy én veiligheid

Greg Alpár
Radboud Universiteit en Open Universiteit
g.alpar@cs.ru.nl

Privacy en veiligheid worden vaak omschreven als tegenstrijdige concepten. Ze kunnen echter tegelijkertijd bereikt worden met cryptografie. Cryptografie maakt van wiskunde gebruik om deze magische, intuïtief tegenstrijdige doelen te bereiken.

Attribuutgebaseerde credentials bieden een nieuwe cryptografische wijze van authenticeren door het selectief tonen van persoonlijke attributen, zonder daarbij noodzakelijkerwijs de gebruiker te identificeren. Bijvoorbeeld, je kunt Netflix kijken met het bewijzen dat je een betalende klant bent, zonder verdere login gegevens of privé informatie te hoeven delen. Op deze manier authenticeren is niet alleen gemakkelijker dan het authenticeren met wachtwoorden, maar het is ook veiliger en privacy-vriendelijker. (Attribuutgebaseerde credentials worden ook in het steeds beroemdere Nederlandse IRMA project gebruikt.)

In dit college wordt enkele elegante, wiskundige aspecten van deze technologie uitgelegd. Onder andere komen de volgende cryptografische technieken aan bod: zero-knowledge bewijs, randomisatie om credentials ontraceerbaar te maken en selectief tonen van attributen.

Cursusgeld

Het cursusgeld bedraagt €95, waarbij de syllabus en de maaltijden zijn inbegrepen. Voor studenten aan lerarenopleidingen bedraagt het cursusgeld €35, terwijl voor gepensioneerden een gereduceerd tarief geldt van €50.

Aanmelding

Via de website: http://www.platformwiskunde.nl/vakantiecursus of per post door het aanmeldingsformulier achterin de brochure in te vullen en op te sturen naar:

Platform Wiskunde Nederland
o.v.v. Vakantiecursus 2018
Science Park 123
1098 XG Amsterdam

Tegelijkertijd dient men het cursusgeld over te maken op bankrekening **NL95INGB0005864482** van de Stichting Platform Wiskunde Nederland onder vermelding van uw naam en VC2018.

Onze buitenlandse gasten kunnen voor betaling gebruik maken van onderstaande gegevens.

BANK	ING BANK N.V.
BIC	INGBNL2A
IBAN	NL95INGB0005864482

NB. Deze cursus geldt als nascholingsactiviteit
Voor geïnteresseerden is een nascholingscertificaat beschikbaar. Degene die daarop prijs stelt, gelieve dit bij aanmelding te laten weten door aankruising van het betreffende vakje op het aanmeldingsformulier.

Plaats(en)

Eindhoven: TU Eindhoven, Auditorium, zaal 2, Den Dolech 2 Amsterdam: CWI,

Science Park 123, Turingzaal.

Syllabus

De syllabus zal worden uitgereikt bij aankomst op de cursus.

Informatie

Voor nadere informatie over de Vakantiecursus kunt u zich wenden tot het bureau van het Platform Wiskunde Nederland, tel. 020-592 4006 dan wel 06-51892525, e-mail: vakantiecursus@platformwiskunde.nl

Contactinformatie

Bureau PWN, 020 – 592 4006; e-mail: vakantiecursus@platformwiskunde.nl;

Platform Wiskunde Nederland, Science Park 123, 1098 XG Amsterdam

Docenten

Dr. B.M.M. de Weger, TU Eindhoven, Postbus 513, 5600 MB Eindhoven

Dr. B. Skoric, TU Eindhoven, Postbus 513, 5600 MB Eindhoven

Dr. G. Alpár, Radboud University, Mercator I, Tournooiveld 212, 6525 EC Nijmegen

Routebeschrijvingen

TU Eindhoven

Met openbaar vervoer:

NS-station Eindhoven, perron af, rechtsaf en via de uitgang aan de noordzijde naar het busstation. Loop 25 meter schuin naar rechts en u ziet de universiteitsgebouwen liggen op enkele minuten loopafstand. Steek bij de verkeerslichten over en volg het golvend voetpad naar de TU/e-campus.
Voorbij Grand Café De Zwarte Doos (rechterkant), is het Auditorium het eerste, wat lagere gebouw aan de linkerkant
Het pad aan de rechterzijde van de campus, de Prof. Dr. Dorgelolaan, is geschikt voor rolstoelgebruikers.

Met de auto:

Vanaf alle autosnelwegen naar en rond Eindhoven (A2, A50, A58, A67 en A270) kunt u de richting Centrum op de ANWB-wegwijzers blijven volgen, tot Universiteit staat aangegeven.

Parkeren: Op de campus kunt u tegen betaling parkeren. Er zijn helaas geen uitrijkaarten beschikbaar, men kan betalen bij de automaten op het terrein.

CWI Amsterdam

Met openbaar vervoer:

- Vanaf station Amsterdam Amstel en station Amsterdam Muiderpoort: bus 40. Zie www.gvb.nl voor meer informatie.
- Vanaf Amsterdam Centraal Station, of Weesp, stopt er vier keer per uur een trein op Science Park Amsterdam. Zie www.ns.nl voor meer informatie.
- Vanaf Amsterdam Centraal met tram 14 naar Soembawastraat en vandaar lopend naar het Science Park (ongeveer 15 minuten).

Met de auto:

- Wanneer u uit de richting Amersfoort komt, neemt u de ring richting Utrecht/Den Haag.
- Wanneer u uit de richting Utrecht/Den Haag/Schiphol/Haarlem of Zaandam komt, neemt u de ring richting Amersfoort. Op de ring neemt u de afslag Watergraafsmeer/S113 (ring Oost). Aan het eind van de afrit volgt u de richting Science Park/Watergraafsmeer. U rijdt dan op de Middenweg.
- Volg vanaf de Middenweg de borden naar Science Park Amsterdam, u komt dan vanzelf op de Carolina Mac Gillavrylaan. Via de rondweg van het Science Park zijn alle bedrijven en instituten te bereiken.
- Aan cursisten die gebruik maken van een navigatiesysteem. De nieuwe straatnaam 'Science Park' kan in enkele systemen nog niet zijn doorgevoerd. U kunt dan intoetsen: Kruislaan 413.

Parkeren: Op het terrein van het CWI is betaald parkeren van kracht. Bij het oprijden moet u een parkeerkaart trekken. Gelieve deze inrijkaart te bewaren,
U ontvangt van de contactpersoon een uitrijkaart. Bij het uitrijden steekt u eerst de inrijkaart in, deze komt terug, en daarna steekt u de uitrijkaart in.

AANMELDINGSFORMULIER VAKANTIECURSUS 2018

Wiskunde in je broekzak: cryptografie in het dagelijks leven

Ondergetekende,

Naam:

Adres:

Postcode:

Woonplaats:

Geboortedatum:

Telefoon:

E-mail:

wenst deel te nemen aan de Vakantiecursus 2018 op de lokatie

Eindhoven op vr. 24 en za. 25 augustus 2018 [ ]

Amsterdam op vr. 31 augustus en za. 1 september 2018 [ ]

en heeft het verschuldigde bedrag van €95,- (dan wel €35,- of €50) overgemaakt (voor rekeningnummer zie pagina 15).

Mijn voorkeur gaat uit naar vegetarisch eten [ ]

Nascholingscertificaat [ ]

Indien van toepassing, hier het adres van de onderwijsinstelling vermelden:

.....

Gelieve dit formulier vóór 1 augustus 2018 te sturen naar:

Platform Wiskunde Nederland
o.v.v. Vakantiecursus 2018
Science Park 123
1098 XG Amsterdam

Voor wie is PWN interessant?

Beroepswiskundigen

Wiskundeleraren

Bedrijven

Leerlingen en studenten

Breed publiek

Platform Wiskunde Nederland is hét landelijke loket voor alles wat met wiskunde te maken heeft.

PWN behartigt de belangen van, en fungeert als spreekbuis voor, de gehele Nederlandse wiskunde.

Platform Wiskunde Nederland | Science Park 123 | kamer L013 | 1098 XG Amsterdam | 020 592 40 06

Ga voor meer informatie naar:
www.platformwiskunde.nl

platform wiskunde nederland