Technische Universiteit
Eindhoven
University of Technology

Bezoekadres
Den Dolech 2
5612 AZ Eindhoven

Postadres
Postbus 513
5600 MB Eindhoven

www.tue.nl/masterclasses/wi

Voor meer informatie kunt u terecht op de website of contact opnemen met

Sander Kerstens
E-mail: slkerstens@gmail.com

Aanmelden kan tot en met een week voor de betreffende masterclass via het bovenstaande emailadres.

Technische Universiteit
Eindhoven
University of Technology

Uitnodiging

23 maart en 11 mei 2012

Security Masterclass

Where innovation starts

Masterclass

Cryptologie is de wetenschap van het versleutelen van data (cryptografie) en van het breken van zulke versleutelingen (cryptanalyse).

Crypto speelt tegenwoordig een niet meer weg te denken rol in onze maatschappij. Vroeger was het gebruik van sterke crypto alleen weggelegd voor regeringen, banken, criminele organisaties en andere grote spelers. Nu heeft iedereen computers en is de cryptografie zo ver gevorderd dat zelfs veiligheidsdiensten machteloos staan tegenover versleuteling door de gemiddelde burger.

Je hebt dagelijks te maken met crypto zonder er bij stil te staan: Allerhande elektronische betalingen worden versleuteld. DVD's, Blu-ray discs en Ipods zijn voorzien van gehate kopieerbeveiligingssystemen en "Digital Rights Management". Browsers gebruiken geavanceerde crypto om na te gaan of een website wel betrouwbaar is, etc.

Programma

Tijdstip	Onderdeel
9:30 uur	Zaal open
10:00 uur	Eerste deel college door dr. Boris Skoric
10:45 uur	Korte pauze met fris en een versnapering
11:00 uur	Practicum
11:45 uur	Lunch bij studievereniging GEWIS
12:30 uur	Tweede deel college door dr. Boris Skoric
14:00 uur	Korte pauze
14:15 uur	Practicum
16:00 uur	Einde

Masterclass

(door dr. Boris Skoric en dr. Benne de Weger)

In deze masterclass krijg je een mini-college over crypto en ga je zelf aan de slag met het maken en breken van versleutelingen.
We geven je een indruk hoe het mogelijk is om met simpele middelen een ongelooflijke puinhoop te maken van je bestanden, maar ze vervolgens toch nog terug te toveren.
Twee onderwerpen komen aan bod: De "symmetrische" crypto, waarbij zender en ontvanger allebei dezelfde sleutel gebruiken (hiermee is perfecte geheimhouding te realiseren).
Maar ook de wonderen van de "asymmetrische" crypto, waarbij een andere sleutel gebruikt wordt voor versleutelen dan voor ontsleutelen.
De bijna magische trucs die hiermee mogelijk zijn bestaan pas sinds 1978.

Omdat er afgelopen jaar enorm veel belangstelling was voor de masterclass van Technische Informatica, hebben we dit jaar gekozen om deze masterclass twee keer aan te bieden. Als je wilt komen, kun je dus kiezen welke dag je komt!

Wanneer? Vrijdag 23 maart of vrijdag 11 mei 2012
Waar? Technische Universiteit Eindhoven (verdere details volgen na opgave)
Voor wie? Leerlingen van klas 5 en 6 van het VWO
Kosten? Geen!

De masterclass is ook een interessante start voor je profielwerkstuk, een praktische opdracht of invulling van je keuzeruimte. Overleg hierover met je docent.
Wil je deelnemen, meld je dan een week voor de betreffende masterclass aan via mail: slkerstens@gmail.com