

## Informatiebeveiliging (E019400)

Wegens Covid19 kan mogelijk afgeweken worden van de onderwijs- en evaluatievormen. Dergelijke afwijkingen zullen via Ufora worden gecommuniceerd.

**Cursusomvang** *(nominale waarden; effectieve waarden kunnen verschillen per opleiding)*

**Studiepunten 6.0**                      **Studietijd 180 u**                      **Contacturen**                      60.0 u

### Aanbodsessies en werkvormen in academiejaar 2020-2021

A (semester 2)	Nederlands	Gent	practicum	11.25 u
			begeleide zelfstudie	30.0 u
			werkcollege: geleide oefeningen	10.0 u
			project	1.25 u
B (semester 2)	Engels		werkcollege: geleide oefeningen	10.0 u
			project	1.25 u
			practicum	11.25 u
			hoorcollege	30.0 u

### Lesgevers in academiejaar 2020-2021

Laermans, Eric	TW05	Verantwoordelijk lesgever
Deschrijver, Dirk	TW05	Medelesgever

### Aangeboden in onderstaande opleidingen in 2020-2021

	stptn	aanbodssessie
<a href="#">Bachelor of Science in de informatica</a>	6	B
<a href="#">Educatieve Master of Science in de wetenschappen en technologie (afstudeerrichting informatica)</a>	6	B
<a href="#">Brugprogramma Master of Science in Bioinformatics (afstudeerrichting Engineering)</a>	6	B
<a href="#">Brugprogramma Master of Science in de ingenieurswetenschappen: computerwetenschappen</a>	6	A
<a href="#">Brugprogramma Master of Science in Computer Science Engineering</a>	6	B
<a href="#">Master of Science in Bioinformatics (afstudeerrichting Engineering)</a>	6	B
<a href="#">Master of Science in de ingenieurswetenschappen: computerwetenschappen</a>	6	A
<a href="#">Master of Science in Computer Science Engineering</a>	6	B

### Onderwijstalen

Nederlands, Engels

### Trefwoorden

beveiliging, encryptie

### Situering

Kennis bijbrengen van basisbegrippen over informatiebeveiliging (wiskundige basis, toepassingen en legale aspecten)  
Leren toepassen van beveiligingstechnieken

### Inhoud

- Inleiding: vormen doelstellingen van beveiliging, mogelijke aanvalstechnieken
- Beveiligingstechnieken: wiskundige basis voor encryptie, cryptografische algoritmen en protocols
- Toepassingen: ingebouwde beveiliging in netwerken, opslag private sleutels/certificaten, bescherming tegen intrusie, biometrische systemen, beveiligingsproject
- Beveiligingsnormen: normen

- Juridische aspecten: informaticacriminaliteit, privacy en bescherming van persoonsgegevens, elektronische documenten

### **Begincompetenties**

Discrete wiskunde, communicatienetwerken

### **Eindcompetenties**

- 1 Beveiligingsfuncties (vertrouwelijkheid, authenticatie,...) begrijpen.
- 2 De werking van beveiligingsmechanismen (encryptie, firewall, biometrie,...) begrijpen.
- 3 De nodige middelen inschatten om cryptografische beveiligingsmechanismen te kraken.
- 4 Beveiligingsmechanismen aanwenden om beveiligingsfuncties te realiseren.
- 5 De complexiteit van een degelijke beveiliging inzien.
- 6 De maatschappelijke en legale aspecten van informatiebeveiliging inzien.

### **Creditcontractvoorwaarde**

Toelating tot dit opleidingsonderdeel via creditcontract is mogelijk mits gunstige beoordeling van de competenties

### **Examencontractvoorwaarde**

Dit opleidingsonderdeel kan niet via examencontract gevolgd worden

### **Didactische werkvormen**

Begeleide zelfstudie, hoorcollege, practicum, project, werkcollege: geleide oefeningen

### **Leermateriaal**

Stallings, William, Cryptography and network security : principles and practice. (Intl ed., 7de uitgave), Englewood Cliffs : Prentice Hall, 2016. ISBN-13: 978-1292158587 (Engelstalig; verkrijgbaar via VTK-cursusdienst; kost (2017-2018) 67€ voor niet-VTK-leden; 60€ voor VTK-leden; oudere edities zijn ook nog bruikbaar)  
Slides (Engelstalig; beschikbaar via het elektronisch leerplatform)

### **Referenties**

- Tel, Gerard, Cryptografie : beveiliging van de digitale maatschappij., Amsterdam : Addison-Wesley, 2002. ISBN: 9043005002
- Bishop, Matt, Computer security: art and science, Boston (Mass.) : Addison-Wesley, 2003. ISBN: 0201440997
- Menezes, Alfred J. and van Oorschot, Paul C. and Vanstone, Scott A., Handbook of applied cryptography, Boca Raton (Fla.) : CRC, 2001. ISBN: 0849385237 (pdf gratis online beschikbaar)

### **Vakinhoudelijke studiebegeleiding**

#### **Evaluatiemomenten**

periodegebonden en niet-periodegebonden evaluatie

#### **Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode**

Openboekexamen, mondeling examen

#### **Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode**

Openboekexamen, mondeling examen

#### **Evaluatievormen bij niet-periodegebonden evaluatie**

Verslag

#### **Tweede examenkans in geval van niet-periodegebonden evaluatie**

Examen in de tweede examenperiode is enkel mogelijk in gewijzigde vorm

#### **Toelichtingen bij de evaluatievormen**

Periodegebonden evaluatie: mondeling examen met open boek.

Niet-periodegebonden evaluatie (geldt voor 25% van de punten): beoordeling van projectverslagen + presentatie van demonstratiesoftware; tweede examenkans: mogelijk in gewijzigde vorm; frequentie: 1 project (in groepen van ongeveer 6 studenten) met deadline op het einde van de lessenperiode.

#### **Eindscoreberekening**

De evaluatie van het project (verslag + deel mondeling examen over project) telt voor

25% van de eindscore.

Om te kunnen slagen voor het opleidingsonderdeel moet een student minstens 8/20 behalen zowel voor de periodegebonden als voor de niet-periodegebonden evaluatie. Is aan deze voorwaarde niet voldaan, dan kan een student niet meer dan 9/20 halen voor dit vak.