



## CNER-TU/e

**Un drum ce merita parcurs!**

Andrei Pintilie, Information Security Technology



Leeds  
Manchester

BRITANNIA

Oxford

Southampton

Mânecij

Cambridge

Londra

Brighton

Amsterdam

Haga

Rotterdam

Anvers

Bruxelles

Lille

Belgia

Luxemburg

Olanda

Essen

Köln

Dortmund

Bremen

Hanovra

Braunschweig

Frankfurt  
pe Main

Mannheim

Hamburg

Kiel

Lübeck

Rostock

Berlin

Wolfsburg

Magdeburg

Leipzig

Nürnberg

Dresda

Szczecin

Praha  
R



Wilhelminadorp

Batadorp

A58

A50

A2

A50

WOENSEL-NOORD

Blixembosch

BOKT

Nederwetten

Hool

Gerwen

Alvershool

Eindhoven Airport

A2

STRIJP

WINKELCENTRUM

Aanschot

Technische Universiteit Eindhoven

Boord

Nuenen

N270

A270

Grădină zoologică Dierenrijk

Opwetten

Eeneind

isterveld

re

Meerhoven

A2

STRIJP-S

Eindhoven

N270

TONGELRE

De Spaarpot

Oerle

Heistraat

HURK

Dommel

Boutenslaan

Piuslaan

STRATUM

Geldrop

Coevering

Toterfout

Veldhoven

A2

GESTEL

GENNEP

Hout

Veldhoven

A67

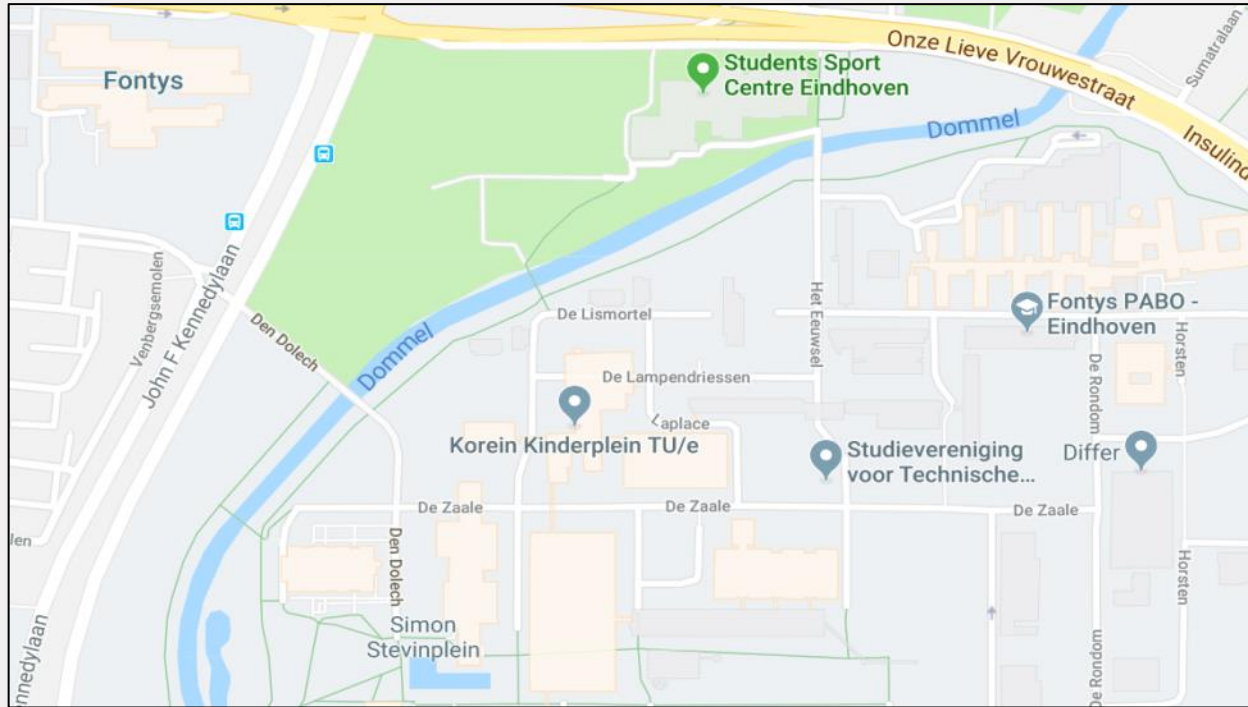
A2

A67

A67

A67

# Alegerea unei facultati bune



## Universitati bune

- TU/e
- Delft
- Twente
- Groningen

# Procesul de selectie

- Aplicare individuala
- Examen de intrare
- Note la bac
- Activitati personale

	Q1	Q2	Q3	Q4
Year 1	Calculus (B) 2WBB0	Applied Physical Sciences (B) 3NAB0 <sup>1</sup>	Intr. to modeling (A) 0LEB0	USE (A) 0SAB0
	Programming (E) 2IP90	Computer Systems (C/E) 2IC30	Data structures (B) 2IL50	Automata & process theory (B) 2IT70 <sup>3</sup>
	Logic and set theory (D) 2IT60	Elective	DBL Emb. Systems (C) 2IO70 <sup>2</sup>	Elective
Year 2	Engineering Design (C) 4WBB0	Data modeling & data bases (E) 2ID50	Programming methods (D) 2IPC0	Probability statistics (C) 2DI90
	Discrete structures (D) 2IT50	DBL Algorithms (D) 2IO90 <sup>4</sup>	Softw. specification (E) 2IX20	Comp. networks & security (E) 2IC60
	Elective / USE <sup>5</sup>	Elective / USE <sup>5</sup>	Elective / USE <sup>5</sup>	Elective / USE <sup>5</sup>
Year 3	Bus. inf. systems (D) 2IIC0 <sup>6</sup>	Algorithms (D) 2ILC0	Elective / USE	SEP/WEP 2IPE0 <sup>7</sup>
	Operating systems (C) 2INC0	Software engineering (C) 2IPD0	Elective / USE	
	Elective / USE <sup>5</sup>	Elective / USE <sup>5</sup>	Elective / USE <sup>5</sup>	Elective / USE <sup>5</sup>

- Self study
- Multa teorie
- 180 credite
- Schimb de cursuri
- Fara internship(la bachelor)



## Ce urmeaza?

- Master in Data Science
- Master in Computer Science
- Master in Information Security Technology (+Radboud)
  
- Phd
- Sute de posibilitati de angajare

	Minim	Maxim
Cazare	350(650)	600(1000+)
Mancare(/luna)	200	400
Cheltuieli scolare(/an)	0	100
Extra cheltuieli(/luna)	50	$\infty$
Asigurare medicala(/luna)	40(105)	>100
Sport(/an)	96	-

+2000

## Oportunitati

- Philips
- ASML
- NXP
- Subventie de la stat pentru:
  - health insurance
  - working grant
  - housing allowance
- Group travelling
- Student discounts(Knaek)

**De ce Olanda?**

O tara de vis!



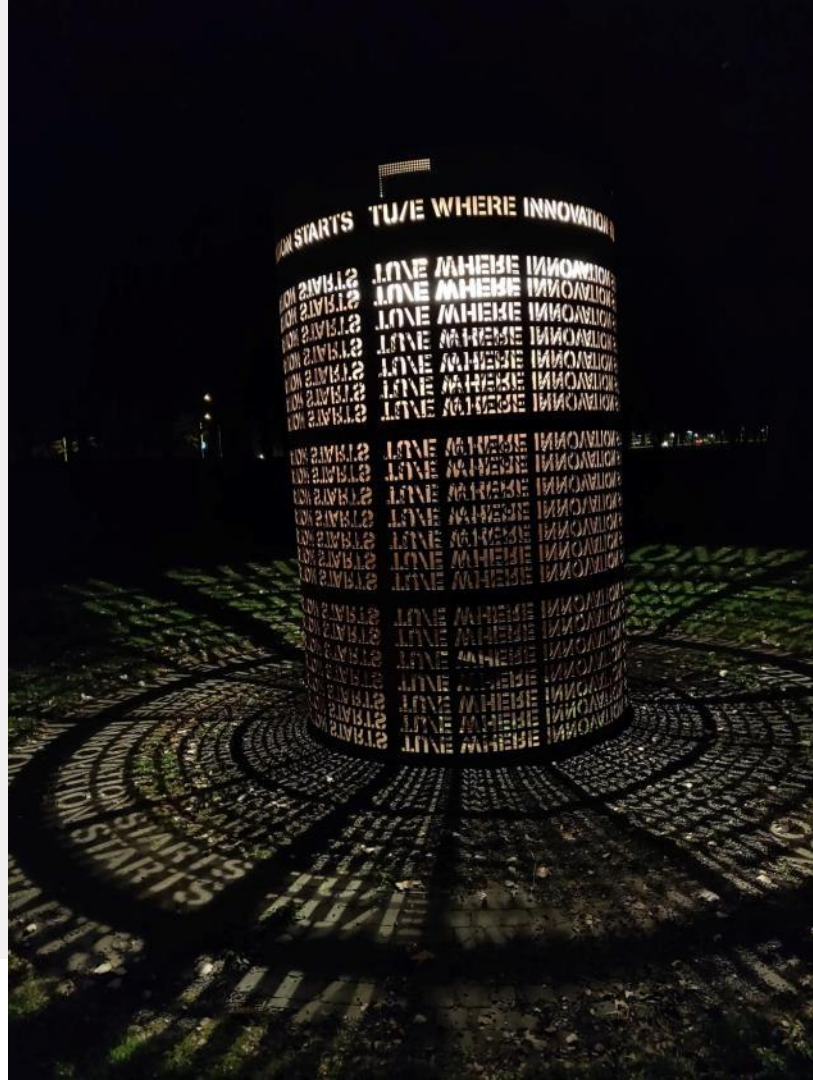






















attacks under  
IND-CPA

$A$

learning

challenge

learning

$E_{PA,C}^{IND-CPA}(\cdot)$

- 1)  $k \leftarrow \text{Gen}(1^n)$
- 2)  $m \leftarrow \mathcal{M} \rightarrow A^{Enc(k)}(m) \rightarrow c$
- 3)  $b \leftarrow \{0,1\}, c' \leftarrow \text{Enc}(m')$
- 4)  $b' \leftarrow A^{Dec(k)}(c')$
- 5) Output 1 if  $b=b'$ , and 0 otherwise

**Def.** A sent key encryption scheme  $\mathcal{E}$  has  $(\epsilon, \delta)$  indistinguishable ciphertexts under chosen plaintext attacks (ICPA) if for all  $(c, c')$  adversaries  $A$  it holds that

$$\Pr[\text{Exp}_{\mathcal{E},C}^{IND-CPA}(A) \leq \frac{1}{2} + \epsilon] \leq \delta$$

**Theorem.** Let  $\mathcal{E}$  be an encryption scheme for which  $\text{Enc}$  is a deterministic algorithm. Then  $\mathcal{E}$  is not IND-CPA secure.

$$\Pr[\text{Exp}_{\mathcal{E},C}^{IND-CPA}(A) \leq \frac{1}{2} + \epsilon] \leq \frac{\Pr[\text{Exp}_{\mathcal{E},C}^{IND-CPA}(A) \leq \frac{1}{2} + \epsilon]}{\Pr[\text{Exp}_{\mathcal{E},C}^{IND-CPA}(A) \leq \frac{1}{2} + \epsilon]}$$

indistinguishable ciphertexts (IND-CPA)

function is a two-input function  $F: \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$

first input is called the key and denoted  $k$

Let  $\mathcal{E} = (\text{Gen}, \text{Enc}, \text{Dec})$  be a sent key encryption scheme. Let the challenge ciphertext be  $c = \text{Enc}(m)$ . Let the adversary  $A$  be given  $c$  and  $m$ . Then  $A$  is said to be successful if  $A$  outputs  $m'$  such that  $m' \neq m$ .

**Theorem.** If  $\mathcal{E}$  is a PRF then  $\text{PRF-ENC}$  is an IND-CPA secure sent key encryption scheme.

**Proof.** Given access to a  $(k, \mathcal{E})$  adversary  $A$  against  $\text{PRF-ENC}$ , we construct a distinguisher  $D$  against  $F$ .

$D$  Given oracle access to a function  $f: \mathcal{X} \rightarrow \mathcal{Y}$  (which is either  $F_k(\cdot)$  for random  $k$ , or random),  $D$  simulates  $\text{Exp}_{\mathcal{E},C}^{IND-CPA}(A)$  using  $f$  instead of  $F_k$ . The  $D$ 's success probability is

$$\epsilon = \left| \Pr[D^{f(\cdot)}(A) = 1] - \Pr[D^{f(\cdot)}(A) = 1] \right|$$

Since  $\text{PRF-ENC}$  is  $\text{PRF-ENC}$  using a random function  $f$  instead of  $F_k$











