4TU.

IN4191 Security and Cryptography

Jan van der Lubbe and Zeki Erkin –TU Delft
Andreas Peter-Twente

TU Delft Delft University of Technology

TU/e Technische Universiteit Eindhoven University of Technology

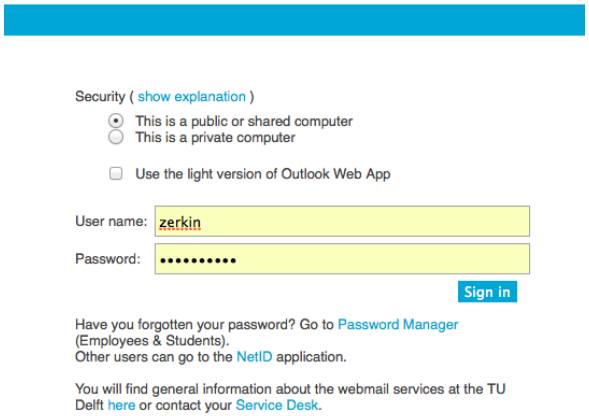
UNIVERSITY OF TWENTE.

WAGENINGEN UR For quality of life

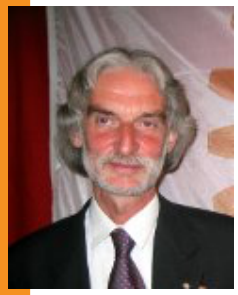
4TU.

Security and Cryptography

It’s everywhere!



Organization



Responsible Lecturer
Dr.ir. Jan van der Lubbe
Office: HB11.150

Dr. Zeki Erkin (Lecturer)
Office: HB11.150

Teaching Assistant
Gamze Tillem
Office: HB11.090

Teaching Assistant
Majid Nateghizad
Office: HB11.090

Teaching Assistant
Chibuike Ugwuoke
Office: HB11.090

Course Details

Lectures

- Mondays 10:45-12:30
- Wednesdays 8:45-10:30

Requirements

- Lectures: 7 weeks, 14 sessions. Attendance suggested (videos will be available)
- Self study
- Mandatory assignments: 20%
  - September 19: individual assignment
  - September 28: individual assignment
  - October 24-26: group assignment+presentation
- Written exam: 80% closed book

Course details

Course Material

- Tekst book: J.C.A van der Lubbe, Basics methods of cryptography
- Supporting books:
  - Nigel Smart (blackboard)
- Hand-outs (blackboard)

Attention!

Possibility of surprise Pop-up quizzes for feedback (not graded)

4TU.

Course Content

No	Date	Topic	Lecturer
1	Sep 12	Introduction to Classical Cryptosystems and Information Theoretic Security	Zekeriya Erkin
2	Sep 14	DES – Modes of Operations	Jan van der Lubbe
3	Sep 19	AES	Jan van der Lubbe
4	Sep 21	Public Cryptosystems	Zekeriya Erkin
5	Sep 26	Public Cryptosystems	Zekeriya Erkin
6	Sep 28	Random Number Generation	Zekeriya Erkin
7	Oct 3	Hash Functions	Jan van der Lubbe
8	Oct 5	Digital Signatures	Zekeriya Erkin
9	Oct 10	Digital Signatures	Zekeriya Erkin
10	Oct 12	Key management	Jan van der Lubbe
11	Oct 17	Key management and Lightweight cryptography	Jan van der Lubbe
12	Oct 19	Secret Sharing	Jan van der Lubbe
13	Oct 24	Case Study	Jan van der Lubbe Zekeriya Erkin
14	Oct 26	Case Study-Presentations	Jan van der Lubbe Zekeriya Erkin

4TU.

Background

- Probability and statistics
- Integer arithmetic
- Discrete mathematics

4TU.

Aims of the Course

- Understanding the notion of security
- Familiar with basic cryptographic concepts, algorithms and protocols for security and privacy
- Readiness in use of cryptographic tools in practice; in future applications and challenges.
- (Im)possibilities of cryptography