IN4191 Security and Cryptography

PayPal

MasterCard VISA AMERICAN EXPRESS DISCOVER NETWORK

TU Delft Delft University of Technology

User ID:

Password:

Forgot your password?

TOP SECRET CONFIDENTIAL TOP SECRET

Organization

Zeki Erkin
Head lecturer

Room: HB11.150
Office hours: Fri 10:00 -12:00

Chibuike Ugwuoke
Teaching Assistant

Room: HB11.090
Office hours: Fri 10:00 -12:00

Oguzhan Ersoy
Teaching Assistant

Room: HB11.090
Office hours: Fri 10:00 -12:00

Majid Nateghizad
Teaching Assistant

Room: HB11.090
Office hours: Fri 10:00 -12:00

Topics

1) Introduction to Security and Cryptography Course
2) Classical Systems **(Chapter 7)**
3) Information Theoretic Security **(Chapter 9)**
4) Defining Security **(Chapter 11)**
5) Modern Stream Ciphers **(Chapter 12)**
6) Block Ciphers and Modes of Operation **(Chapter 13)**
7) Block Ciphers and Modes of Operation **(Continued)**
8) Hash Functions, MAC and Key Derivation Functions **(Chapter 14)**
9) Number Theory and Elliptic Curves **(Chapters 1 and 4)**
10) The RSA Algorithm **(Chapter 15)**
11) Public Key Encryption and Signature Algorithms **(Chapter 16)**
12) Public Key Encryption and Signature Algorithms (continued)
13) Certificates, Key Transport and Key Agreement **(Chapter 18)**
14) Advanced Topics **(Chapter 17)***

IN4191-Course Details

- Lectures-recorded, tele-lectured
  - Mondays: 10:45-12:30, Lecture Hall Chip, Delft
  - Wednesdays: 08:45-10:30, Lecture Hall Chip, Delft
- Practice session-**not** recorded, tele-lectured
  - Thursdays: 17:45-18:30, Lecture Hall Chip, Delft

- Grading
  - Written exam: 60%, simple calculators only, closed book
  - Assignments: 40%, 5 mandatory assignments