Introduction to Modern Cryptography

Michele Ciampi (CO)

Lecture 01, part 1

Administrative Information

Welcome to INFR11131

Introduction to Modern Cryptography (INFR11131)

- Part I: Private-key (symmetric-key) (SK)
- Part II: Public-key (PK)

Lecturer

- Dr. Michele Ciampi

TAs

- Brazitikos Konstantinos

Tutor

- Me

Timetable

- **11** weeks (now is WK01)
- **2 × 50** min lectures per week: **Tue, Fri, 15:10h-16:00h**
- WK01–WK06: SK
- WK07–WK10: PK
- WK11: Additional tutorials or recover lectures

Note

No lectures on the week between WK05 and WK06 (revision week)

Tutorials

- On WK6
- Two groups per week (one tutorial on Wednesday **11:10** and one on Thursday **11:10**)
- Exercises released approximately one week before the tutorial.

Homework / Coursework

- **30**% of grade
- **1** homework on part of the SK topics
- About $\approx$ **4**
- Posted on *Learn* on WK07 Friday Morning
- Due on WK09 at noon on Friday.

Exam

- **70**% of grade
- Similar to homework, but with fewer questions compared to prior 2024 (it will be similar to 2025)
- The problems proposed in the exam could be about any of the topics covered in the course
- Open book
- Allowed: paper copy of lecture slides + your own handwritten notes
- Not allowed: electronic devices of any kind

Textbook and slides

Textbook: SK & PK

- Katz and Lindell, **"Introduction to Modern Cryptography, 2nd edition"** `https://eu01.alma.exlibrisgroup.com/leganto/public/44UOE_INST/lists/49836031260002466?auth=SAML`

Textbook: PK

- **Aggelos Kiayias, Lecture notes**: `http://www.kiayias.com/Aggelos_Kiayias/Introduction_to_Modern_Cryptography_files/Cryptograph_Primitives_and_Protocols.pdf`

Slide content

- SK: adapted from the slides of prof. Jonathan Katz

Recommended Prerequisites

- Computer Security (INFR10067), Algorithms and Data Structures (INFR10052)
- Discrete math
- Probability: random variables, independence, Bayes' theorem, statistical distance, union bound
- Analysis of algorithms, asymptotic notation
- Mathematical maturity and being comfortable with reading and constructing mathematical proofs

Resources: *Opencourse and Learn*

- `https://opencourse.inf.ed.ac.uk/imc/`
  - Slides may be slightly updated right before the lecture
- `https://www.learn.ed.ac.uk/ultra/courses/_127133_1/outline`
  - Recording of the lecture (uploaded within 2 days)
  - Homework assignments
  - Timetable
  - Latest announcements
  - Contacts
  - Almost everything

Resources: *Piazza*

Piazza register link

`https://piazza.com/class/mfcb2xyc18129g/`

- Discussion and questions on lectures and homeworks
- Monitored by lecturers and TAs. You can also ask questions to the tutor.

Warning!

Learn > Piazza

i.e. information on Learn has priority over Piazza in terms of accuracy and timeliness

Lecture and tutorials rooms

Course Timetable Browser

`https://browser.ted.is.ed.ac.uk/`

Course Overview: Symmetric-key 1/2

- Historical ciphers: Shift cipher, Vigenère
- Perfect secrecy
- One-time pad (OTP)
- Computational secrecy
- Pseudorandom generators (PRG)
- Pseudo-OTP
- Security against chosen-plaintext attacks (CPA)
- Pseudorandom functions / permutations (PRF / PRP)

Course Overview: Symmetric-key 2/2

- CPA-secure encryption using PRF/PRP: block ciphers
- Modes of operation: block ciphers, stream ciphers
- Malleability
- Security against chosen-ciphertext attacks (CCA)
- Non-CCA secure schemes: padding-oracle attacks
- Secrecy vs. integrity: message authentication codes (MAC)
- Hash functions

Course Overview: Public-key

- Digital Signatures
  - Trapdoor One-Way functions
  - Random oracles
- Cyclic groups
- The discrete logarithm/Diffie-Hellman assumptions
- Key exchange and the Diffie-Hellman protocol
- Public Key Encryption
- Security against chosen-plaintext attacks
  - ElGamal Encryption
- Zero-Knowledge proofs
  - The Schnorr identification scheme

Questions

How to ask a question

- Ask throughout lecture
- Ask after lecture
- Ask on Piazza
- Office hours: By appointment via email

Contacts

- Michele: `michele.ciampi@ed,ac.uk`, IF-5.26
- TA: Brazitikos Konstantinos `K.Brazitikos@sms.ed.ac.uk`

Course goals

Understand

- The theoretical basis of modern cryptography
- The security guarantees needed/provided by modern encryption schemes
- The key terms and learn how to use cryptography
- Fundamental cryptographic primitives
  - SK and PK schemes, key exchange, digital signatures
- How to formally model security problems and write rigorous security proofs

Course non-goals

The course does not cover

- Advanced cryptanalysis techniques
  - Differential, linear cryptanalysis and derivatives
- Other advanced topics
  - Time-Memory Tradeoffs
  - Memory hardness
  - Proof-of-work
  - Commitments*
  - Blockchain

More importantly

I use the whiteboard a lot

1. Try to attend the lectures (the recording may fail due to unforeseen technical problems or the whiteboard may not be captured in its integrity by the camera)
2. The slides contain more or less everything I write but in a more condensed way
3. Use the book to study, and solve the exercises at the end of each chapter.

Changes compared to previous years (prior to 2024), and student's feedback response

Exam

1. Fewer questions
2. Having the right intuition about how to solve all the exercises is sufficient to pass the exam
3. How correct and detailed the answers are will determine how high the final score will be.

Course

1. More focus on advanced topics like zero-knowledge and secure multi-party computation
2. Less focus on historical aspects of cryptography and removal of some security proofs

End