Cryptology - 01410
Spring 2023

Christian Majenz & Carsten Baum

Assistant Professors, DTU Compute,

Technical University of Denmark

Practicalities

01410 - Organisation

Mondays, 13.00 – 17.00

- Lectures 13:00-15:00, Building 308, Auditorium 13
- then exercises 15:00-17:00. Three groups in Building 308, Databars 001, 009 and 017
- 3 Homework sets. 1 over easter break, two "Homework weeks" with no planned lecture content (but there might be a class we are running behind schedule)

Not Mondays April 03&10 (Easter)

Your teachers

Carsten Baum

Assistant Professor at DTU and Aarhus University

About me

I'm an Assistant Professor in the Cybersecurity Section at DTU Compute in Copenhagen and in the Computer Science Department at Aarhus University, Denmark. My research focus is on (applied) secure computation as well as (lattice-based) zero knowledge protocols. Furthermore, I am interested into security for machine learning and secure protocol design using public ledgers.

Before starting on this position I have been a Postdoc at Aarhus University and Bar Ilan University, Israel. I obtained my PhD in 2016 from Aarhus University.

Christian Majenz

Department of Applied Mathematics and Computer Science, Technical University of Denmark

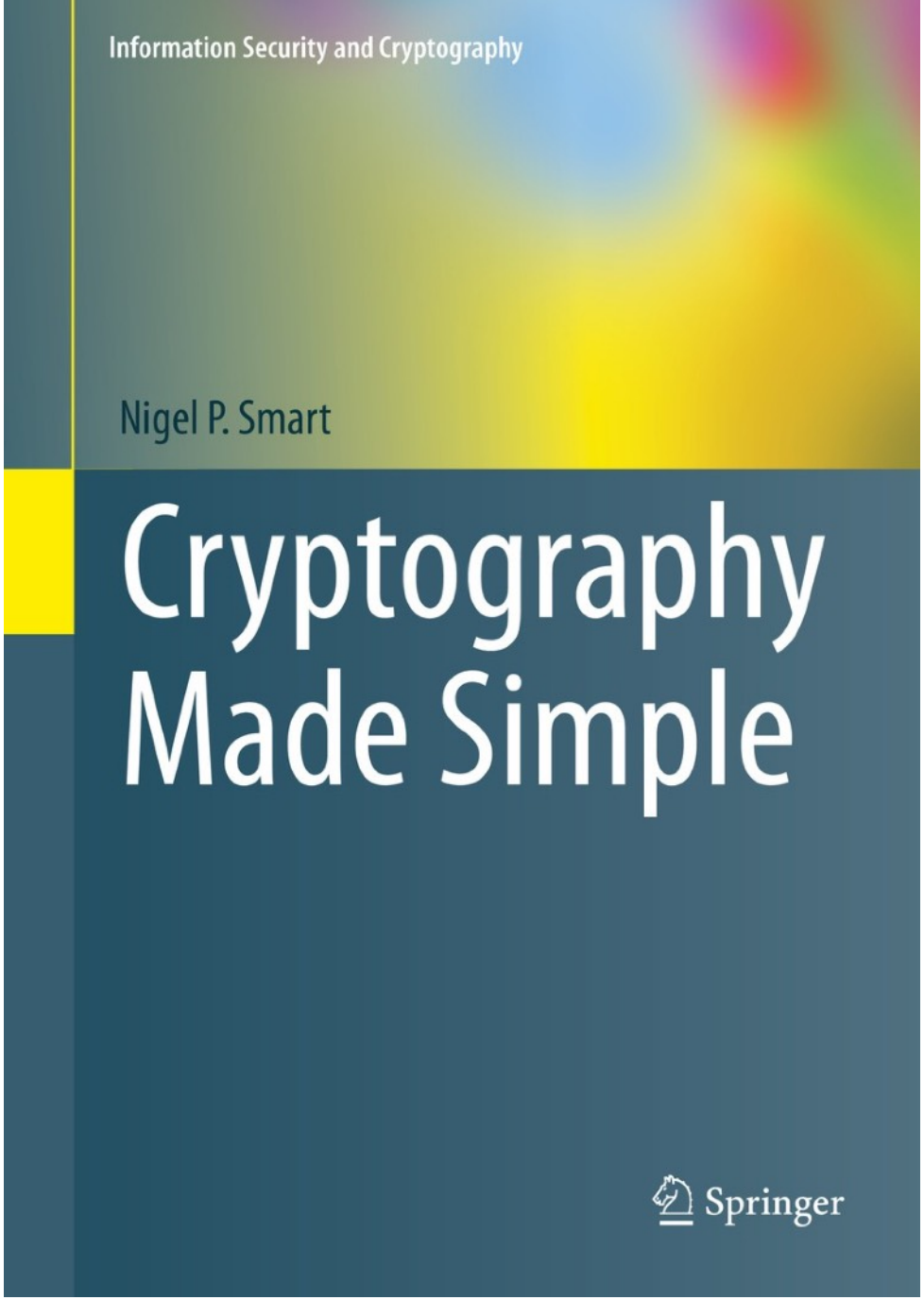
About me | CV | Research | Publications | Presentations | Teaching | Links | Contact

I currently hold a personal Veni grant from NWO, which I have taken with me to Denmark via the "Money Follows Researcher" scheme, and I am part of the MSCA doctoral training network "Quantum-Safe Internet". In addition I have been awarded a Sapere Aude grant from the Independent Research Fund Denmark, which will start September 2023.

About me

I am an assistant professor of cryptography at DTU Compute, the Department of Applied Mathematics and Computer Science at the Technical University of Denmark. My research areas are post-quantum and quantum cryptography, and quantum information theory. I find the interplay of the algebraic structure of quantum mechanics and the computational framework of modern cryptography, as well as representation-theoretic and combinatorial techniques, particularly interesting.

I hold a PhD degree in mathematics, which I obtained from the Department of Mathematical Sciences at University of Copenhagen under the supervision of Matthias Christandl. Before that, I studied physics at University of Freiburg where my M.Sc. thesis was supervised by David Gross.


Information Security and Cryptography
Nigel P. Smart
Cryptography Made Simple
Springer

Exercises and Tutoring Classes

One Exercise sheet per week. Work on it during tutoring classes and in between classes!

Three tutoring class groups — three teaching assistants: Freja Elbro, Polly Nielsen Boutet-Livoff and Fabrizio Sisinni.

The exercise problems are *very* important for actually learning something in this course, please (try to) solve them!!!

Exam

3 homeworks in course: 30% of the grade

Written examination: 70% of the grade

The practice problems and homework problems are indicative of how exam problems will look like (except the ones that obviously take too much time)

Homework

3 Homework sheets. Each counts 10 percent of your grade.

You can submit in groups of up to 3 — please team up!

- TA time is valuable! Fairness demands that it is equally divided between you
- $\Longrightarrow$TAs have more time to give constructive written feedback on team submissions (but of course all submissions are graded according to the same standards)


UNDER
CONSTRUCTION

Changes compared to last year

Old:

Læringsmål

En studerende, der fuldt ud har opfyldt kursets mål, vil kunne:

- Foretage beregninger ved modulær aritmetik, herunder Euklids algoritmer og den kinesiske restklassesætning.
- Diskutere forskellene mellem klassisk (symmetrisk) kryptologi og public-key (asymmetrisk) kryptologi.
- Definere det diskrete logaritme problem modulo et primtal og demonstrere anvendelserne i kryptologi.
- Redegøre for hvordan man vælger store primtal til brug i public-key kryptologi.
- Definere egenskaberne ved en digital signatur og forklare detaljerne i El Gamal's signatursystem.
- Skitsere anvendelserne af kryptografiske hashfunktioner i kryptologi, og beskrive de ønskelige egenskaber med funktionerne i den pågældende anvendel
- Redegøre for hvordan de symmetriske krypteringssystemer, DES og AES, anvendes til kryptering og autentificering.
- Præsentere RSA public-key kryptosystemet i alle detaljer, samt forklare hvordan systemet kan bruges til kryptering og til at konstruere digitale signaturer.
- Forklare hvad "secret-sharing" bruges til og hvordan en hemmelighed deles.
- Demonstrere hvordan man udveksler en nøgle til symmetrisk kryptering på en sikker måde.

New:

Learning objectives

A student who has met the objectives of the course will be able to:

- Do calculations in modular arithmetic, including Euclid's algorithms and the Chinese Remainder Theorem.
- Discuss the differences between classical (symmetric) cryptology and public-key (asymmetrical) cryptologi.
- Explain the functionality and security properties required of symmetric-key and public-key encryption schemes, message authentication codes and digita signature schemes.
- Describe the design principle of AES.
- Explain how block ciphers are used for encryption and authentication, and analyze the security of modes of operation.
- Define the discrete logarithm problem modulo a prime number and demonstrate the applications in cryptology.
- Explain how to find big prime numbers for use in public-key cryptology.
- Outline the applications of cryptographic hash functions in cryptology, and describe the desired properties of the functions in the particular application.
- Present the RSA public-key cryptosystem in all details, and explain how the system is used for encryption and to construct digital signatures.
- Demonstrate how to exchange a key for symmetric encryption securely using Diffie-Hellman key exchange.
- Discuss the quantum threat to cryptography.
- Explain the Learning With Errors problem and Regev's encryption scheme.

I'm also learning...

Parts of this year's course will be the "Capstone Project" for a the DTU teacher training program I am enrolled in

$\Longrightarrow$I will ask for feedback a lot, please help me out and respond!

Cryptography

What is cryptography?

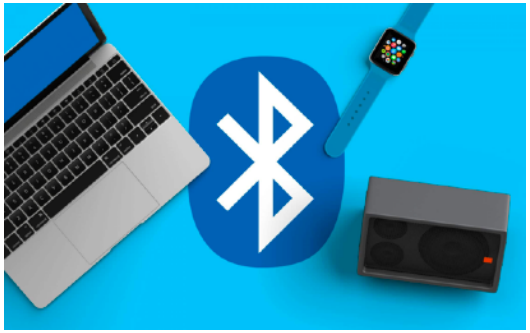
Cryptography

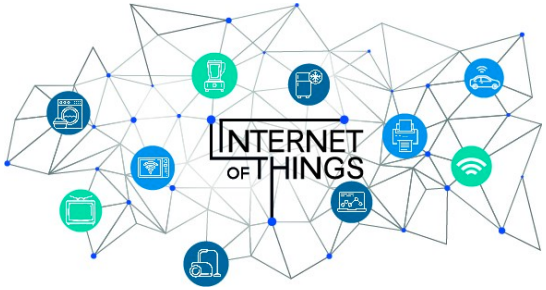
cryptography(=cryptology): the science (and art) of constructing and analyzing cryptographic schemes

Examples:

- encryption schemes
- authentication schemes
- digital signatures
- hash functions
- zero-knowledge proofs, secure multiparty computation, program obfuscation, block chain, fully homomorphic/functional/identity-based/attribute-based/threshold encryption…

Where is cryptography used?

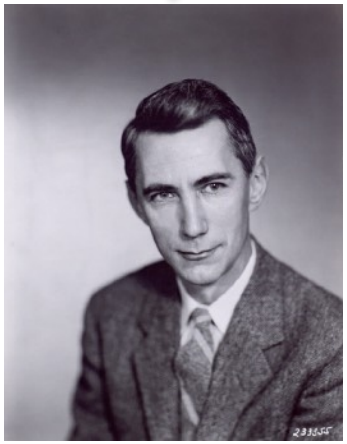




History of cryptography - seen from Mars

1900BC

1945



now

Ciphers/Encryption schemes

Definition, historical ciphers

($\Longrightarrow$blackboard)