Course plan:

30.1.22

- Practicalities
- Introduction to cryptography:
    - Where is cryptography used
    - the security mindset/"professional paranoia"
    - definition of a symmetric-key encryption scheme
    - historical ciphers
    - Kerkhoffs' principle

6.2.22

- Lightning-fast reminder: probability
- Perfect secrecy
- One-time pad, proof of security
- Examples of real-world chosen-plaintext and chosen-ciphertext attacks

13.2.22

- Block ciphers
    - Iterated block ciphers
    - SPN design
    - AES
    - The IND game, chosen-plaintext and chosen-ciphertext security
    - Modes of operation

20.2.22

Homework week. Lecture only if we didn't get through the material from previous weeks

27.2.22

- Message authentication codes
- UF-CMA
- CBC-MAC
- Hash functions:
    - Where are they used
    - Collision-resistance
    - Preimage resistance, second preimage resistance
    - Merkle-Damgård
    - Application: H-MAC

6.3.22

- Lightning-fast reminder: Modular arithmetic
    - Extended Euclid's algorothm
    - Chinese Remainder Theorem
    - Euler's totient function and euler's theorem
- Define public-key encryption
- Plain RSA encryption

13.3.22
Homework week. Lecture only if we didn't get through the material from previous weeks

20.3.22
- Recap insecurity plain RSA encryption
- How to construct secure RSA encryption
- Define Digital signatures and note that UF-CMA is security notion
- RSA signatures
- hash-then-sign.

27.3.22
- Prove UF-CMA security of RSA signature
- Primality tests

Homework over the Easter break

17.4.22
- (Possibly primality tests ctd.)
- The discrete logarithm assumption
- Diffie-Hellman key exchange
- Public-key encryption from key exchange (ElGamal)

24.4.22
- Quantum computing
- Bird's-eye view of Shor's algorithm
- Where are quantum broken schemes used?

1.5.22
- The Learning With Errors (LWE) problem
- Regev's encryption scheme.

8.5.22
Buffer/bonus lecture

Homework hand-in dates
1. 27.2.22, 13:00
2. 20.3.22, 13:00
3. 17.4.22, 13:00

Book
"Cryptography made simple" by Nigel Smart

Exam
Date: 15.05.2023
"All help" is allowed, which means all help except internet
The exercise and homework problems give you an indication of how the exam problems could look.