Summary
The goal of the course is to introduce basic notions from public key cryptography (PKC) as well as basic number-theoretic methods and algorithms for cryptanalysis of protocols and schemes based on PKC.

Content
Basic notions and algorithms from public key cryptography such as RSA, ElGamal, key exchange protocols, zero knowledge proofs. Main topics may include, but are not limited to
- modular and finite field arithmetic
- primality testing
- polynomial and integer factorization algorithms
- index calculus and discrete logarithm-based schemes
- elliptic curve arithmetic and cryptography
- basic notions from lattice-based cryptography: lattice-basis reduction algorithms, learning-with-errors, applications to homomorphic encryption

Keywords
public key cryptography, key exchange, digital signatures, zero knowledge proofs, RSA, ElGamal, integer factorization, index calculus, elliptic curve cryptography, lattice-based cryptography

Learning Prerequisites
Recommended courses
Some knowledge of abstract algebra (groups, rings and fields) is desirable, but not mandatory. Knowledge of basic algorithms is a plus.

Assessment methods
Homework assignments: Weekly problem sets focusing on number-theoretic and complexity-theoretic aspects. These will be complemented by programming exercises in SAGE which is a Python-based computer algebra system. No prior experience with SAGE or Python is required. A subset of the homework will be handed in and graded, counting for 40% of the final grade.
The written final exam counts for 60% of the final grade. There will be a mock midterm exam not to be part of the final grade. The final exam will test theoretical understanding as well as understanding of the algorithms and protocols. The exam will include no SAGE programming exercises. If needed, algorithms could be presented with pseudo-code. The exact final exam format will be adapted to the epidemiological situation and resulting guidelines.

Resources
Moodle Link

• https://go.epfl.ch/MATH-489