**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 cryptography
- basic notions from lattice-based cryptography

**Keywords**

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

**Teaching methods**

lectures, exercises, additional references

**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 30% of the final grade.

**One mid-term exam** (20% of the final grade) and **one final exam** (50% of the final grade). Both exams will test theoretical understanding as well as understanding of the algorithms and protocols. The exams will include no SAGE programming exercises. If needed, algorithms could be presented with pseudo-code.

Dans le cas de l’art. 3 al. 5 du Règlement de section, l’enseignant décide de la forme de l’examen qu’il communiquera aux étudiants concernés.