- Faculté des sciences
- www.unine.ch/sciences

Cryptographic Algorithms (3IN2085)

Filières concernées	Nombre d'heures	Validation	Crédits ECTS
Master en informatique	**Cours: 2 ph** **Exercice: 2 ph**	**Voir ci-dessous**	5
Master en mathématiques	**Cours: 2 ph** **Exercice: 2 ph**	**Voir ci-dessous**	6

ph=période hebdomadaire, pg=période globale, j=jour, dj=demi-jour, h=heure, min=minute

Période d'enseignement:

- Semestre Automne

Equipe enseignante

Dr Gabriel Dill

Contenu

Cryptography is the study of techniques for securing and authenticating communication and data, especially in the presence of potential adversaries. We use it every day: when we pay with a credit card or access a website. Public-key cryptography in particular allows secure communication even over an insecure channel, where anyone might be listening, and without having agreed on a common secret key beforehand.

After reviewing basic cryptographic notions (with a focus on public-key methods), we will study two families of public-key cryptographic algorithms:

Elliptic-curve cryptography is based on the mathematics of elliptic curves. These curves have a lot of additional structure, which is used in cryptographic schemes to define hard mathematical problems. Elliptic curves are used for instance in TLS 1.3 — and therefore in HTTPS.

Lattice-based cryptography relies on the geometry of lattices — grids of points in a high-dimensional space. The security comes from the difficulty of certain problems such as finding the shortest non-zero vector in a lattice. Lattice-based cryptography underlies two of the three post-quantum cryptographic algorithms standardized by NIST in 2024.

We will cover both theoretical foundations as well as practical applications and possible attacks on these systems. We will also see how to work with the associated mathematical objects, using a computer algebra system such as Sage. All required mathematical notions beyond a basic course in discrete mathematics will be introduced and explained in the course.

Time permitting, we will cover also other cryptographic algorithms such as isogeny-based or pairing-based cryptography.

Forme de l'évaluation

Oral exam (30 minutes)

If you receive 5 ECTS for this course, the exam will cover the contents of the course and of the standard exercises.

If you receive 6 ECTS for this course, the exam will cover the contents of the course, of the standard exercises, and of the extra exercises.

Modalités de rattrapage

Oral exam (30 minutes)

If you receive 5 ECTS for this course, the exam will cover the contents of the course and of the standard exercises.

If you receive 6 ECTS for this course, the exam will cover the contents of the course, of the standard exercises, and of the extra exercises.

Pré-requis

A basic course in mathematics (such as "Discrete Mathematics and Applications").

Having already followed the "Cryptography" course at Uni Bern will be useful, but is not mandatory.

Cryptographic Algorithms (3IN2085)

Forme de l'enseignement

Ex cathedra + exercises