# Cryptographic Engineering

Clément PERNET

M2 Cybersecurity, UFR-IM<sup>2</sup>AG, Univ. Grenoble-Alpes ENSIMAG, Grenoble INP

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへぐ

# Organization of the course

Week 38 (Sept. 18): Crypto Refresh (C. Pernet & P. Karpman)

- Computational algebra
- Field extensions: implementation and applications
- Discrete probabilities

### Symmetric Crypto (Pierre Karpman)

- Block ciphers and symmetric encryption
- Hash functions
- MACs and authenticated-encryption
- Design and implementation of Block Cipher

◆□▶ ◆□▶ ▲□▶ ▲□▶ ■ ののの

Lab sessions

# Organization of the course

## Asymmetric Crypto (C. Pernet & E. Peyre & J-L Roch)

- Computational security: complexity classes and reductions
- RSA and attacks
- DLP over finite fields; index calculus
- Coding theory applied to post-quantum cryptography
- Elliptic curves (E. Peyre)
- 0-knowledge, homomorphic cryptography, and applications (JLR)

(日) (日) (日) (日) (日) (日) (日)

### Security Models (Cristian Ene)

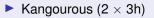
- Properties and proof of correction of crypto primitives
- Protocol verification in the symbolic model

## Lab Sessions

## Symmetric Crypto (Pierre Karpman)

- ► AES(2 × 3h)
- 2nd pre-image on long messages (2 × 3h)

## Asymmetric Crypto: Pierre Karpman



### Security Models: (Cristian Ene)

```
▶ (2 × 3h)
```

・ロト・日本・日本・日本・日本・日本

## References



#### Dan Boneh and Victor Shoup.

A graduate Course in Applied Cryptography. 2020. https://toc.cryptobook.us.

Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. Introduction to algorithms. MIT press, 2009.



Jean-Guillaume Dumas, Jean-Louis Roch, Éric Tannier, and Sebastien Varrette. *Foundations of coding: compression, encryption, error-correction.* Dunod, to appear.



#### Jonathan Katz and Yehuda Lindell.

Introduction to Modern Cryptography.

CRC Press.

http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/ Introduction\_to\_Modern\_Cryptography.pdf.



Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.

#### Handbook of applied cryptography.

CRC Press, 2001.

http://www.cacr.math.uwaterloo.ca/hac/.



Douglas Stinson.

*Cryptography theory and practice.* CRC Press, 2005.