

# Cryptographic Engineering

---

Clément PERNET

M2 Cybersecurity,

UFR-IM<sup>2</sup>AG, Univ. Grenoble-Alpes

ENSIMAG, Grenoble INP

# Organization of the course

## Week 38 (Sept. 15): Crypto Refresh (C. Pernet)

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

## Asymmetric Crypto (C. Pernet, V. Vitse, J-L. Roch)

- Computational security: complexity classes and reductions
- Provable security: hardness assumptions and reductions
- Attacking the hard problems : Pollard Rho, index calculus, etc
- Coding theory applied to post-quantum cryptography
- Elliptic curves (V. Vitse)
- 0-knowledge, homomorphic cryptography, and applications (JLR)

## Symmetric Crypto (Léo Colisson)

- Block ciphers and symmetric encryption
- Hash functions
- MACs and authenticated-encryption
- Design and implementation of Block Cipher
- Lab sessions (T. Briand)

## Security Models (Cristian Ene)

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

## Symmetric Crypto (Tom Briand)

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

## Asymmetric Crypto: Tom Briand

- Kangourous (2 × 3h)

## Security Models: (Cristian Ene)

- (2 × 3h)

## References

-  Dan Boneh and Victor Shoup.  
***A graduate Course in Applied Cryptography.***  
<https://toc.cryptobook.us>.
-  Jean-Guillaume Dumas, Jean-Louis Roch, Éric Tannier, and Sebastien Varrette.  
***Foundations of coding: compression, encryption, error-correction.***
-  Jonathan Katz and Yehuda Lindell.  
***Introduction to Modern Cryptography.***
-  Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.  
***Handbook of applied cryptography.***
-  Mike Rosulek.  
***The Joy of Cryptography.***  
<https://joyofcryptography.com/>.
-  Douglas Stinson.  
***Cryptography theory and practice.***