

Introduction to cryptography

Welcome

Gilles VAN ASSCHE
Christophe PETIT

INFO-F-405
Université Libre de Bruxelles
2024-2025


© Olivier Markowitch and Gilles Van Assche, all rights reserved

Compiled on September 9, 2024

Introducing myself

Gilles Van Assche

`gilles.van.assche@ulb.be`

- Cryptographer at **STMicroelectronics** in Diegem 
 - User of cryptography for secure chips (e.g., smartcards)
 - Active in research in symmetric cryptography
- Professor of **Cryptanalysis** (Erasmus Mundus Cyberus)

Lectures – Outline

- 1 Historical ciphers and general principles
- 2 Secret-key techniques (symmetric cryptography)
 - Primitives: keystream generator, block cipher, permutation
 - Modes of operation
 - Encryption, authentication, authenticated encryption
- 3 Hashing
- 4 Public-key techniques (asymmetric cryptography)
 - Key establishment, encryption, signature
 - Factorization, discrete logarithm, elliptic curves

Exercises

Abel Laval

`abel.laval@ulb.be`

The exercises follow the same chapters as the lectures.

Plus two additional sessions:

- The finite field $\text{GF}(2^8)$
- Modular arithmetic

Starts this week already

Friday September 20 in Forum D

References

- The lecture slides
- The **outline** on the Université Virtuelle (UV)
 - Key points to remember
 - Pointers for more information
- **Paar and Pelzl, *Understanding Cryptography*, Springer 2011**
(ISBN 978-3642041006)
 - Note: there is a second edition available, but not yet evaluated
- Katz and Lindell, *Introduction to Modern Cryptography*
(third edition), CRC Press, 2021 (ISBN 978-0815354369)
- Menezes, van Oorschot and Vanstone, *Handbook of applied cryptography*, freely available on
<http://www.cacr.math.uwaterloo.ca/hac/>