Cryptography

ISEN Lille – M1 · S1 · 2019

Gabriel Chênevert
gabriel.chenevert@yncrea.fr / C664

Outline

0)	Introduction	9/9
1)	Stream ciphers	9/16
2)	Block ciphers	9/23
3)	Authentication	9/30
4)	RSA encryption	10/7
5)	Discrete logarithms	10/21
6)	Digital signatures	11/4
7)	Loose ends	11/18

References

- Course web page on `https://campus.isen.fr` / `http://gch.ovh/crypto`
- Menezes, van Oorschot & Vanstone, *Handbook of applied cryptography* (2001)
  available online at `http://cacr.uwaterloo.ca/hac`
- B. Schneier, *Applied cryptography* (1996)
  available (French 2nd edition) at the library – might also check out his Crypto-Gram newsletter
- J-P Aumasson, *Serious cryptography* (2017)
- Parr & Pelzl, *Understanding cryptography* (2014)
  some ressources available online at `http://crypto-textbook.com`
- D. Boneh, *Cryptography I* (starts Sept. 30) and *II*
  on Coursera `https://www.coursera.org/learn/crypto` and `crypto2`
- E. Anderson, *Hands-on cryptography* (starts Oct. 6) official site

Evaluation

- Weekly Jupyter (Python 3) labs : 60 %
  Weeks 1 to 7 – don't forget your laptop !
- Final project : 40 %
  Analysis of a cryptographic protocol in a real-world example