Introduction to cryptology

Presentation

Bruno Grenet

M1 INFO, MOSIG & AM

Université Grenoble Alpes – IM²AG

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

Historic cryptography *versus* Modern cryptography

Definitions

- "*The art of writing or solving codes.*"

  C. Soanes, A. Stevenson. Concise Oxford English Dictionary. 2004.

- Techniques for secure communication in the presence of adversarial behavior

  "Cryptography." Wikipedia, The Free Encyclopedia

Goals and scope

- Confidentiality
- Communications between militaries, governments, banks

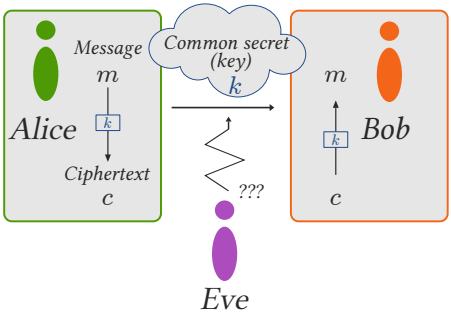
- Confidentiality, integrity, authentication, non-repudiation, …
- Passwords, credit cards, wifi, hard drives, signed software updates, cryptocurrencies, electronic voting, …

From art to science

- Heuristic design
- Haphazard analysis
- Based on intuitions

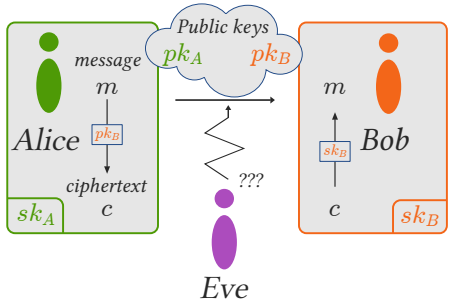
- Definitions: adversary, secure, …
- Theorems, proofs of security, …
- Based on TCS foundations

Main course content



Symmetric cryptography

- Symmetric encryption
- Message authentication codes
- Hash functions



Public-key cryptography

- Key exchange
- Public-key encryption
- Digital signatures

Additional content

Cross-cutting concept: provable security

- Models of security — what does *secure* mean?
- Proofs of security — what guarantees are there?
- Some attacks — what can *go wrong*?

Maths as a foreign language

- (Basic) discrete probability theory
- (Basic) algebra and number theory

Putting it all together: TLS

- Transport Layer Security: communications security
  - secure browsing — `https`
  - other uses: email, VoIP, VPN, …
- Uses symmetric and public-key encryption, key exchange, hash functions, digital signatures, …

Course goals and non-goals

Goals

- Understand the *theoretical basis* of *real world cryptography*
  - Key vocabulary
  - Security guarantees
  - Avoid *misuse* of cryptography
  - Have an idea of what's *under the hood*
- Possibly prepare for the Cybersecurity Master or for other Crypto/Security courses

Non-Goals

- Design your own cryptographic systems (hard!)
- Implement cryptographic systems for practical use (hard!)
- Study the whole field of cybersecurity: steganography, network security, software security, hardware security, social engineering, …
- Become a specialist in the mathematics of cryptography

Organization

Weekly schedule

- Lecture: theoretical concepts
- Tutorials: exercises
- Twice in the semester: programming labs

Additional course: Algebraic Algorithms for Cryptology

- For more details on the underlying algorithms

Exams

- *Contrôle continu*: programming lab *or* in-class exam (to be fixed) 30%
- Final exam (+ retake exam) 70%

References

- J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021.
- D. Boneh, V. Shoup. A Graduate Course in Applied Cryptography, version 0.6, Jan. 2023. *Online: http://cryptobook.us*