DATA PRIVACY AND SECURITY

Prof. Daniele Venturi

Master's Degree in Data Science

Sapienza University of Rome

CIS SAPIENZA

RESEARCH CENTER FOR CYBER INTELLIGENCE AND INFORMATION SECURITY

About Myself

- Full Professor at the **Computer Science** Department
- Research focus: Theoretical and applied **cryptography**
- Personal homepage (contact info, research topics, office hours, etc.):

https://dventuri83.github.io

- Web page for this course:

https://dventuri83.github.io/projects/2_dps/

Logistic

- Lectures both on **Tuesday** and **Thursday**
  - Tuesday: Room A2, 15:00-17:00
  - Thursday: Room A2, 12:00-15:00
- The lectures are offered **exclusively** in person
  - No recodings will be available
  - Active participation is **highly** recommended
- Course material: Slides and bibliograhic references from the course homepage

Exams

- **Oral exam** on the topics covered in class
- Students **presentations**
  - Choose a topic **during the semester** and get assigned either a **research paper** or a **small project**
- Final grade: Oral exam (70%) and student presentation (30%)
- Exams sessions (plenary): January, February, June, July, and September

Syllabus

- Introduction to **cryptography**
  - **Symmetric** and **asymmetric** cryptography, **key exchange** protocols, **post-quantum** crypto
- Differential Privacy
  - **Privacy-preserving statistics** on datasets
- Cryptocurrencies and **distributed ledgers**
  - Bitcoin, Ethereum, altcoins
- Secure **multiparty computation**
  - Secret sharing
  - Distributed key generation
  - Garbled circuits

Bibliography

- J. Katz, Y. Lindell. *“Introduction to Modern Cryptography.”* Chapman & Hall, 3rd Edition
- Y. Lindell (Editor). *“Tutorials on the Foundations of Cryptography.”* Springer
- A. Chiesa, E. Yogev. *“Building Cryptographic Proofs from Hash Functions”* Springer
- A. Narayanan et al. *“Bitcoin and Cryptocurrency Technologies”* Princeton University Press
- C. Hazay, Y. Lindell. *“Efficient Secure Two-party Protocols”*. Springer