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.):

  http://danieleventuri.altervista.org/

- Web page for this course:

http://danieleventuri.altervista.org/dps.shtml

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
- A **small project** (requires coding capabilities)
- Final grade: Oral exam (70%) and presentation of the project (30%)
- Exams sessions (plenary): January, February, June, July, and September

Tentative Topics

- Brush-up on cryptography
- Outsourcing of computation/storage
- Differential privacy
- Cryptocurrencies
- Secure Multi-Party Computation

Bibliography

- J. Katz, Y. Lindell. *"Introduction to Modern Cryptography."* Chapman & Hall, 2nd Edition
- C. Dwork, A. Roth. *"The Algorithmic Foundations of Differential Privacy."* Foundations and Trends in Theoretical Computer Science
- C. Hazay, Y. Lindell. *"Efficient Secure Two-Party Protocols."* Springer
- Research papers and course slides