Cryptography
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

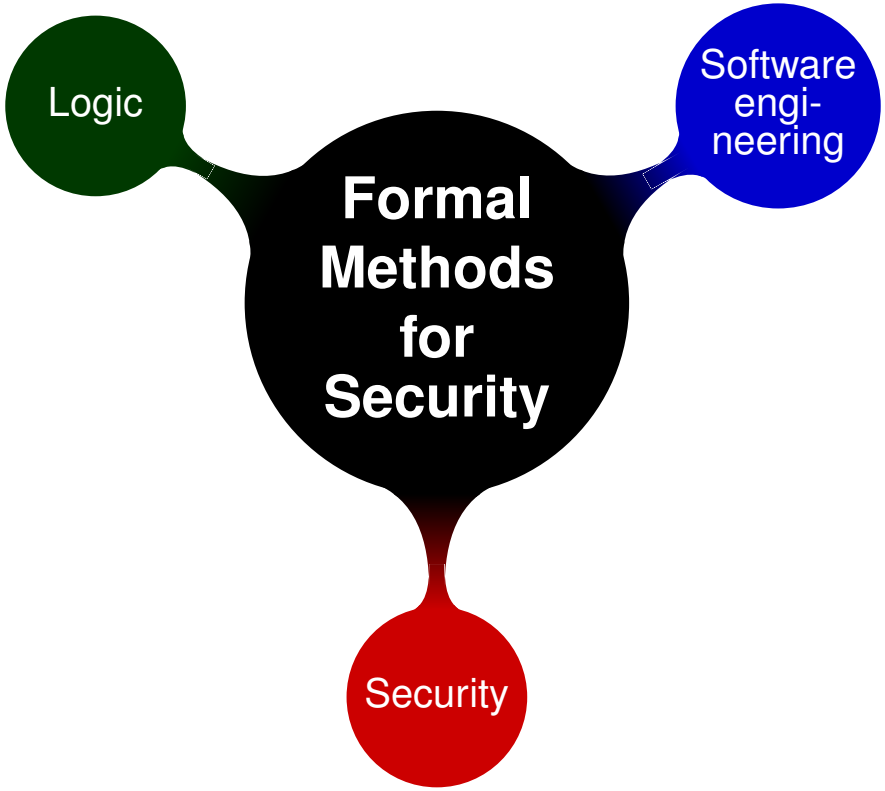
First term 2020/21

Lecture 1.1: Introduction to the module

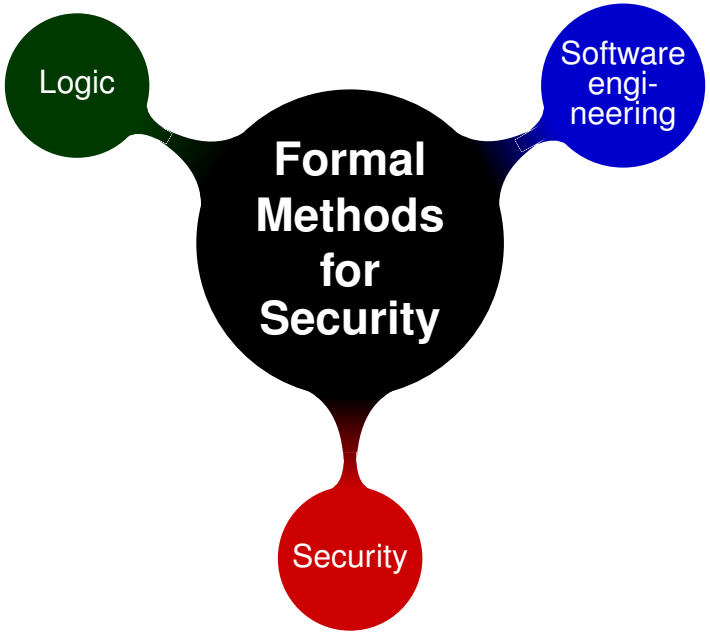
Pleased to meet you

About myself

About myself: Research (and teaching)



About myself: Research (and teaching)



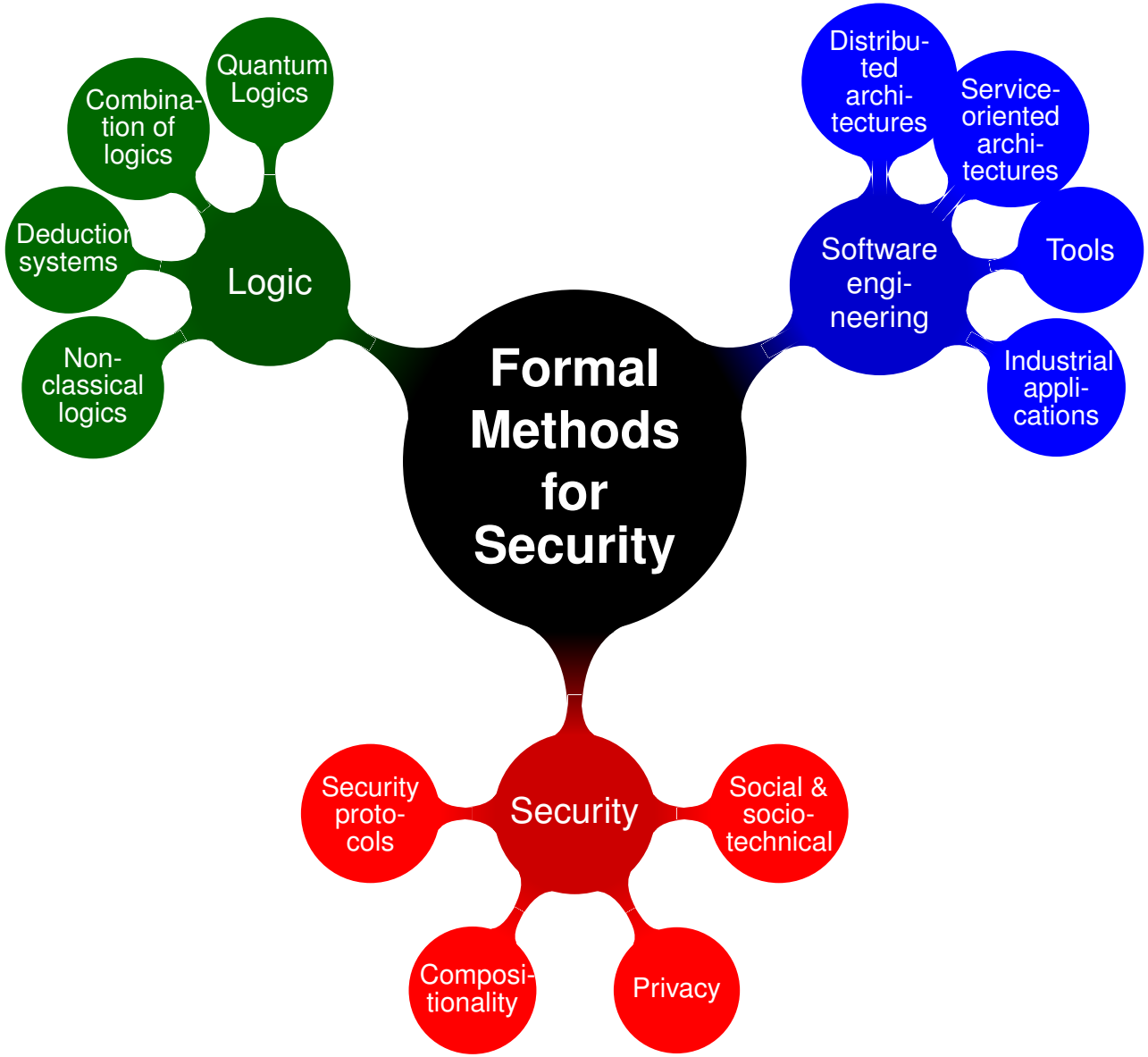
Theoretical research

Formal Methods: Techniques and tools based on mathematics and logic that support the specification, construction, analysis and testing of hardware and software systems.

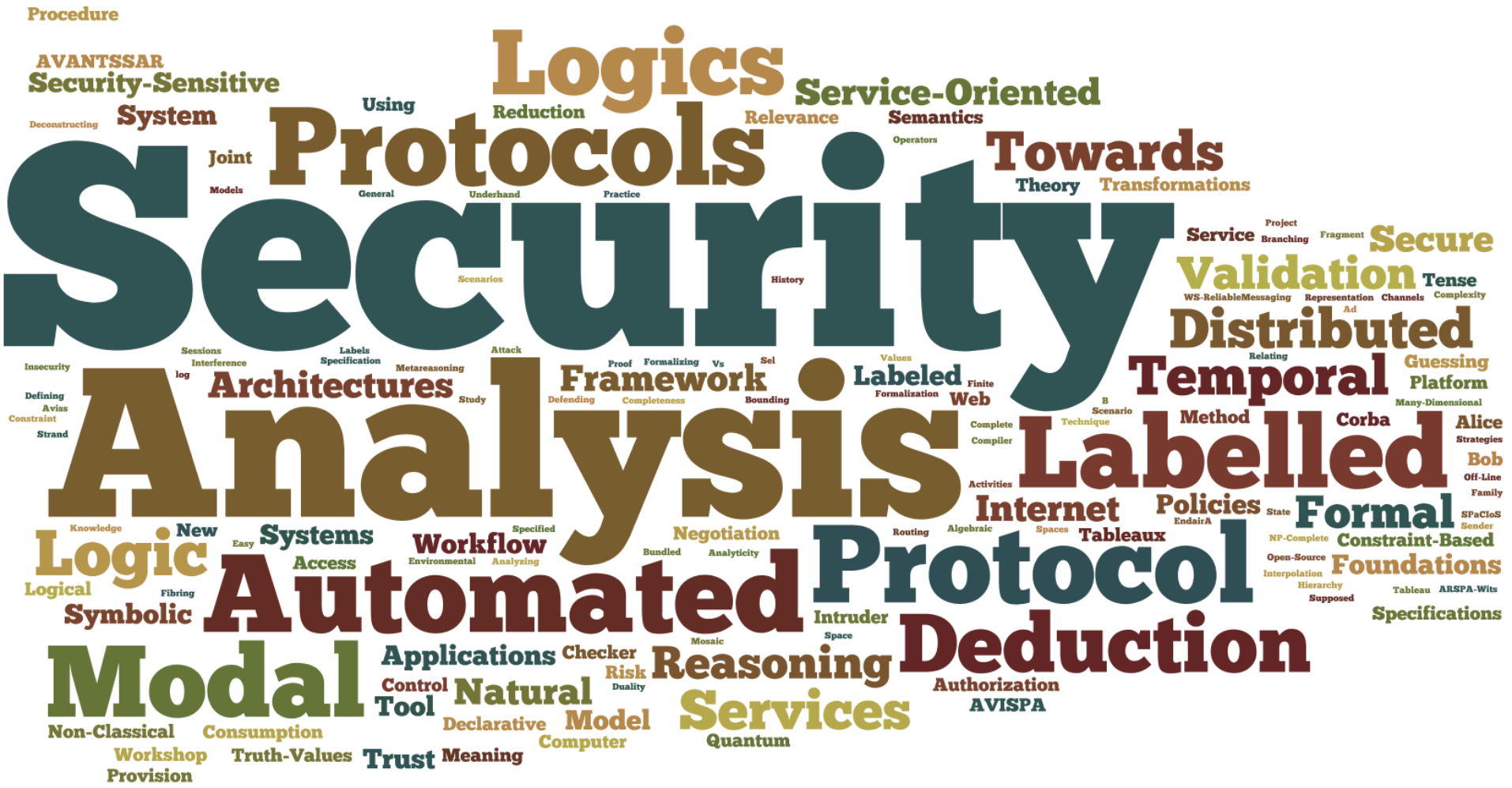
and its application to practical problems

in the small, e.g. security protocols and web applications, privacy, attribution
in the large, e.g. distributed security architectures, cyber-physical systems.

About myself: Research (and teaching)



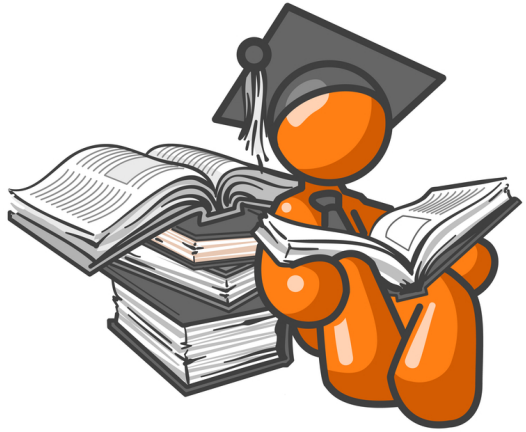
About myself: wordle of my research papers



And you are?

Programmes: BSc, MSci, MSc

- BSc Computer Science, Year 3
- BSc Computer Science with Management, Year 3
- BSc Computer Science with Management and a Year Abroad, Year 4
- BSc Computer Science with Management and a Year in Industry, Year 4
- BSc Computer Science with a Year Abroad, Year 4
- MSci in Computer Science, Year 3
- BSc Computer Science with a Year in Industry, Year 4
- Mathematics and Computer Science, Year 3
- MSc in Advanced Computing
- MSc in Computing & Internet Systems
- MSc in Computing, IT Law & Management
- MSc in Cybersecurity
- MSc in Data Science
- MSc in Web Intelligence
- MSci Computer Science
- ...



Coordinates

- **Credit level:** 6 / 7
- **Credit value:** 15
- **Assessment:** through quizzes on Keats; details to be provided

- **KEATS:** slides, exercises and general material, news and discussion forum
  - Recordings and slides available before lectures
  - Watch for corrections (new versions with errata lists)
  - Student questions and discussion forum

- **Office hours:** Tuesday 10-12 (online) or email
- ~~**Office:** BH(N)7.18~~
- **Email:** luca.vigano@kcl.ac.uk

Objectives: for you

Objectives: for me

Format

- A mix of asynchronous (pre-recorded) and synchronous (live) teaching.
  - Weekly recordings, readings, quizzes (asynchronous)
  - Tue 09:00-10:00: synchronous online tutorial with me
  - Tue 17:00-18:00: synchronous online tutorial with TA (if needed)
  - Weekly small group tutorials (online and/or face-to-face) with TAs

- Meet the team:
  - Professor Luca Viganò
  - Teaching Assistants:
    - Andrew Cook
    - Lara Dal Molin
    - Jide Edu
    - Francesca Mosca
    - Xiao Zhan
    - (Xuehui Hu)

Learning aims & outcomes

- To introduce both **theoretical** and **practical** (and **technological**) aspects of cryptography and information security.
- On successful completion of this module, students should be able to
  - understand the relevant mathematical techniques associated with cryptography;
  - understand the principles of cryptographic techniques and perform implementations of selected algorithms in this area; and
  - appreciate the application of security techniques in solving real-life security problems in practical systems.

Please note that this module contains several advanced mathematical techniques. This should not be a problem for students with a reasonable mathematical background. Explanations are given during the lectures/tutorials and examples are studied in detail.
Nevertheless, an in-depth understanding of these techniques is required for the examination and personal work should be anticipated.

Complementary (and introductory) to other modules in security.

Syllabus and general information

- Basic terminology and concepts:
  - Goals of cryptography, terminology and notation, players
  - Basic cryptographic functions
- Number theory:
  - Congruent modulo n, equivalent class modulo n
  - Integer modulo n (Zn)
  - Multiplicative inverse
  - Relatively prime
  - Euler's theorem
  - Fermat's little theorem
  - EEA (Extended Euclidean Algorithm)
  - CRT (Chinese Remainder Theorem)
- Ciphers:
  - Block ciphers (substitution, transposition, product)
  - Stream ciphers
  - Modes of operation (ECB, CBC, CFB, OFB)
- Cryptosystems:
  - Block cipher: DES (Data Encryption Standard), AES (Advanced Encryption Standard)
  - Public-key: RSA (Rivest-Shamir-Adleman), El Gamal
  - One-way hash function: SHA and MD5 (Message Digest 5)
  - Password hashing and salting

Syllabus and general information

- Key-establishment protocols:
  - Symmetric and asymmetric techniques (Diffie-Hellman, Needham-Schroeder, Otway-Rees)
  - Public-key encryption
  - Basic and advanced Kerberos protocols
- Authentication and identification:
  - Concepts
  - Fiat-Shamir and Feige-Fiat-Shamir protocols
  - Zero-knowledge identification protocol
- Digital signatures:
  - Classification
  - Digital signature schemes: RSA; EI-Gamal; DSA (Digital Signature Algorithm) and DSS (Digital Signature Standard)
- Information Security:
  - Password systems: number of acceptable passwords for a given password policy, exhaustive search password ageing
  - Introduction to viruses, secure communication, social engineering (phishing), firewall, buffer overflow, denial of services

Recommended reading

- Recordings and slides will cover all the topics.

- Recommended bibliography:
  - William Stallings. *Cryptography and Network Security. Principles and Practice*, 7th ed., Prentice Hall, 2016.
  - Alfred Menezes, Paul van Oorschot, Scott Vanstone, A.J. Menezes. *Handbook of Applied Cryptography*, CRC Press, 1996 and 2018). Available online: http://cacr.uwaterloo.ca/hac/.
  - Wenbo Mao. *Modern Cryptography: Theory & Practice*, Prentice Hall, 2003.
  - Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.
  - Bruce Schneier. *Applied Cryptography*, John Wiley & Sons, 1996 (and 20th anniversary edition in 2016).
  - Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering*, John Wiley & Sons, 2010.

  These books are recommended only (not required to buy them).