# COMP522
# Privacy and Security
# revision notes

www.csc.liv.ac.uk/~alexei/COMP522

Alexei Lisitsa

Dept of computer science

University of Liverpool

alexei@csc.liv.ac.uk

# Topics to revise (different order)

- **Part 1: Identification and authentication**
  - Passwords v.tokens v. biometrics;
  - Data aggregation and anonymity;
- **Part 2: Monitoring** & IDS
  - Audit, and intrusion detection;
  - Techniques (statistics, pattern recognition, etc); and

# Topics to revise

- **Part 3: Protocols & Algorithms**
  - Protocol design;
  - Cryptography for secrecy, for signing, etc;
  - Symmetric key and asymmetric key protocols;
  - 3DEA and RSA protocols;
  - Logical representation of protocols;
  - Formal properties of protocols; and
  - Applications, e.g encryption, key distribution, identification, authentication
  - Information hiding: steganography

# Topics to revise

- **Part 4: Advanced Crypto**
  - Homomorphic encryption and computing over encrypted data
  - Zero-knowledge proofs & Secure MPC
- **Part 5: Legal and Social Issues**
  - Reasons for legal regulations of cryptography
  - Different aspects: patents, trade secrets, digital rights, etc
  - OECD guidelines on privacy

# How to revise

**Possible way:**

- Go through the list of topics (**titles of lectures** + **titles of individual slides** of all lectures) and check if you can say something **precise** (a few sentences) in response to the questions related to the topic/slide title:

  What? How? Why?

- Have a look and inspect the links to additional information provided at the web-page of the course. Ask the same questions above

# Appendix. Learning outcomes

- Understand the main problems in security, confidentiality and privacy in computers and in networks, and the reasons for their importance
- Understand the main approaches adopted for their solution and/or mitigation, together with the strengths and weaknesses of each of these approaches.
- Understand the main encryption algorithms and protocols.
- Appreciate the application of encryption algorithms to secure messaging, key distribution and exchange, authentication
- Understand the use of epistemic logics for formal modelling of security and privacy protocols.
- Understand the legal and ethical issues related to security, confidentiality and privacy