Topics to revise (different order)

• Part 1: Identification and authentication
  – Passwords v. tokens v. biometrics;
  – Data aggregation, anonymity and pseudoanonymity;
  – Information hiding: steganography (different order)
• Part 2: Monitoring
  – Audit, and intrusion detection;
  – Techniques (statistics, pattern recognition, etc); and
  – Issues such as accountability v. privacy;

• 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, electronic cash, voting

• Part 4: Attacks and defences
  – Malware: viruses, worms, etc
  – Anti-virus and anti-worm methods;
• Part 5: Legal and Social Issues
  – Reasons for legal regulations of cryptography
  – Different aspects: patents, trade secrets, digital rights, etc
  – OECD guidelines on privacy
Topics to revise

- **Part 7: Future directions**
  - Quantum protocols and cryptography
  - Computations over encrypted data

How to revise

Possible way:

Go through the list of topics (+ 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?

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 and electronic payment systems.
- 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.