COMPUTER SCIENCE TRIPOS Part II – 2015 – Paper 7

12 Security II (FMS)

(*a*) Clearly explain the Clark-Wilson security policy model and what it tries to achieve, defining technical terms such as CDI, UDI, CW triples, IVP, TP and auditing. [6 marks]

(*b*) (*i*) What is a master key system? What is its purpose? How can we turn a normal pin-tumbler lock into one supporting a master key? [5 marks]

(*ii*) Describe in detail the Blaze Privilege Escalation attack on master key systems. What resources does an attacker need and what can be achieved? Compare the effort required to that of a brute-force attack. [5 marks]

(*c*) Discuss the security, privacy and economic aspects of the iPhone's "App Store" model, as opposed to the traditional desktop software model. [4 marks]