COMPUTER SCIENCE TRIPOS Part II – 2018 – Paper 7

14 Security II (DRT)

(*a*) Compare and contrast the usability and security of messaging using encrypted email (either GPG or PGP) and end-to-end encrypted messaging (WhatsApp, Signal, or iMessage). [5 marks]

(*b*) Let's Encrypt provides free TLS certificates and has a secure protocol for issuing them automatically. This means that software can automatically provision itself with a valid TLS certificate when it is installed without manual intervention. How does this change the security ecosystem for TLS provision? Justify your answer with reference to security economics, network security, and usability. [5 marks]

(*c*) You are responsible for designing, implementing and maintaining a user-authentication service for a new e-commerce website. The website will include a marketplace for third party vendors, multiple methods of processing payments and is optimised for mobile and desktop computers. Describe and justify your design in detail. [10 marks]