COMPUTER SCIENCE TRIPOS Part IA – 2025 – Paper 2

5   Software and Security Engineering (avsm2+arb33+mk428)

You have joined the team developing a new, rapidly growing social media service. The system is decentralised, in the sense that it allows anybody to run their own server and interact with users on other servers, e.g. by seeing posts made by users on other servers.

(a) Explain some possible strategies for testing the server software for this social network.   [6 marks]

(b) Your server currently authenticates users via a password, but your team is discussing whether to introduce public key authentication. Discuss how this might work, and its pros and cons compared to passwords. Consider both how a user logs in to their home server, and also how posts on one server are authenticated by another server.   [14 marks]