Network Security
6CCS3NSE / 7CCSMNSE

Diego Sempreboni
(Kudos L. Vigano)

Department of Informatics
King's College London, UK

Protocols

Revision and possible exam questions: IPsec and TLS

1. What is Perfect Forward Secrecy and how can it be achieved?

2. What are the main objectives of the IKE protocol?

3. Describe the SSL Handshake protocol, illustrating all of its different steps.