

IS53012B/A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2018-19 (since 2007)

Homework

- 1 Study the Diffie-Hellman Key Exchange Protocol. Demonstrate how the Diffie-Hellman protocol can suffer from the Man-in-the-Middle Attack.
- 2 Let L be the *power set* of (a, b, c) . The system low is \emptyset and the system high is (a, b, c) . Draw the lattice for (L, \subset) .

Part I

Homework