

## 2001 Paper 3 Question 4

### Introduction to Security

Which mode (or modes) of operation of the Advanced Encryption Standard (AES) block cipher would you use to protect the following? Give a brief justification for your answers.

- (a) Inter-bank funds transfers. [4 marks]
- (b) Email messages. [4 marks]
- (c) A high-frequency radio modem link. [4 marks]
- (d) Passwords stored on a local disk. [4 marks]
- (e) The pulse train from a gearbox sensor to the tachograph in a truck. [4 marks]