2003 Paper 10 Question 11

Introduction to Security

(a) Explain the difference between mandatory and discretionary access control. [4 marks]

(b) (i) Explain the purpose and operation of cipher-block chaining (CBC). [4 marks]

(ii) Explain how to decrypt a message in CBC. [4 marks]

(c) To protect her interview partners, a journalist needs to ensure that what she records with her digital camera cannot be viewed by anyone before she returns to her home country. You were asked to design for her a camera that encrypts recordings immediately before they are stored on tape. The question arises, how to handle the encryption key. If it is stored in the camera, it could be extracted if the hardware were confiscated and analysed. A key memorised by the user might be obtained using coercion, so this is not a suitable solution either.

Suggest *two* alternative convenient ways of arranging the encryption inside the camera such that decryption of the tape is possible only on the journalist's home computer. [8 marks]