1997 Paper 7 Question 9

Security

Describe the following modes of operation of a block cipher: electronic codebook, cipher block chaining, output feedback, cipher feedback, message authentication code and hash function. [12 marks]

With which of these modes would it usually be unwise to use the Data Encryption Standard algorithm? [3 marks]

How would you choose a mode of operation to protect the confidentiality of data traffic on a radio link with known rates of (a) bit errors and (b) burst errors causing loss of synchronisation? [5 marks]