2005 Paper 8 Question 6

Security

A mobile telephone company has 5 million prepay customers who buy scratchcards to pay for air time. Each card has a code of 9 decimal digits, and at any time there are about 20 million cards active (issued to the supply chain and not yet used).

(a) Discuss the relative advantages and disadvantages of implementing the code system with a database of random numbers *versus* an encrypted counter. [4 marks]

(b) If you were using an encrypted-counter system, how would you go about selecting, adapting or designing a suitable cipher? [4 marks]

(c) Some of the customers have got clever. As they are allowed two invalid code attempts, they try two random codes before entering a correct one. The telephone company is now getting 2000 complaints a month from people who bought a scratchcard and found, when they tried to use it, that someone else had already guessed the number. How would you modify the system to reduce the level of complaints? [8 marks]

(d) You are now approached by a telephone company in China which wants to use your system to manage 100 million prepay customers. What further modifications would you consider? [4 marks]