1998 Paper 5 Question 5

Introduction to Security

Some banks issue their Automatic Teller Machine (ATM) card customers with a randomly selected personal indentification number (PIN). Others issue their customers with an initial PIN only, and let the customers choose their own PIN the first time they use the card in an ATM. Describe the advantages and disadvantages of these approaches. [5 marks]

Again, some banks compute the customer PIN by encrypting the account number using DES and a key known only to their central systems and ATMs, taking the first four hex digits of the result, replacing the digits A, ..., F with 0, ..., 5 respectively, and finally, if the first digit of the result is 0, replacing it with a 1. What is the probability that a criminal can get the PIN right given three guesses? [5 marks]

Yet other banks have used DES, and a key known only to their central systems and ATMs, to encrypt the PIN (whether randomly generated or customer selected); they then write the result on the magnetic strip on the customer's card, so that the ATM can verify it without reference to the central system. Describe the disadvantages of this arrangement. [5 marks]

In order to prevent attacks based on manipulating magnetic strips, banks in some countries have moved to using smart cards. What effect would you expect such a move to have on the incidence of card-based fraud? [5 marks]