2002 Paper 8 Question 6

Security

(*a*) Explain the concept of a *Trusted Computing Base* and outline its meaning in the context of the access control provided by a typical Unix workstation. [5 marks]

(*b*) An automatic teller machine (ATM) communicates with a central bank computer for PIN verification. A 32-bit CRC code is added to each packet to detect transmission errors and then the link is encrypted using a block cipher in counter mode. Describe an attack that is possible in this setup. [5 marks]

(*c*) (*i*) Describe a cryptographic protocol for a prepaid telephone chip card that uses a secure 64-bit hash function H implemented in the card. In this scheme, the public telephone needs to verify not only that the card is one of the genuine cards issued by the phone company, but also that its value counter V has been decremented by the cost C of the phone call. Assume both the card and the phone know in advance a shared secret K. [5 marks]

(*ii*) Explain the disadvantage of using the same secret key K in all issued phone cards and suggest a way around this. [5 marks]