2004 Paper 3 Question 9

Introduction to Security

(*a*) Explain briefly mechanisms that software on a desktop computer can use to securely generate secret keys for use in cryptographic protocols. [5 marks]

(*b*) Give *two* different ways of implementing residual information protection in an operating system and explain the threat addressed by each. [5 marks]

(*c*) Consider the standard POSIX file-system access control mechanism:

(*i*) Under which conditions can files and subdirectories be removed from a parent directory? [2 marks]

(*ii*) Many Unix variants implement an extension known as the "sticky bit". What is its function? [2 marks]

(*iii*) On a POSIX system that lacks support for the "sticky bit", how could you achieve an equivalent effect? [2 marks]

(*d*) VerySafe Ltd offer two vaults with electronic locks. They open only after the correct decimal code has been entered. The VS100 – a low-cost civilian model – expects a 6-digit code. After all six digits have been entered, it will either open or will signal that the code was wrong and ask for another try. The VS110 – a far more expensive government version – expects a 40-digit code. Users of a beta-test version of the VS110 complained about the difficulty of entering such a long code correctly. The manufacturer therefore made a last-minute modification. After every five digits, the VS110 now either confirms that the code has been entered correctly so far, or it asks for the previous five digits again. Compare the security of the VS100 and VS110. [4 marks]