2007 Paper 10 Question 9

Introduction to Security

(*a*) You have received a shipment of hardware random-number generators, each of which can output one 128-bit random number every 10 milliseconds. You suspect that one of these modules has been tampered with and that it actually produces only 30-bit random numbers internally, which are then converted via a pseudo-random function into the 128-bit values that it outputs.

   (*i*)   How does this form of tampering reduce the security of a system that uses a generated 128-bit random number as the secret key of a block cipher used to generate message authentication codes?   [2 marks]

   (*ii*) Suggest a test that has a more than 0.5 success probability of identifying within half an hour that a module has been tampered with in this way.
                                                                           [6 marks]

(*b*) Explain briefly

   (*i*)   the encryption and decryption steps of Cipher Feedback Mode;   [3 marks]

   (*ii*)   why some operating systems ask the user to press a special key combination (e.g., Alt-Ctrl-Del) before each password login;   [3 marks]

   (*iii*) how a secure hash function can be used to implement a one-time signature scheme;   [3 marks]

   (*iv*)   what happens if the same private key of the scheme from (*iii*) is used *multiple times*, to sign different messages.   [3 marks]