2008 Paper 3 Question 8

Introduction to Security

(*a*) A source of secure, unpredictable random numbers is needed to choose cryptographic keys and nonces.

(*i*) Name *six* sources of entropy that can be found in typical desktop-computer hardware to seed secure random-number generators. [4 marks]

(*ii*) What sources of entropy can a smartcard chip, like the one in your University Card, access for this purpose? [4 marks]

(*b*) As Her Majesty's prime hacker "001", on a mission deep inside an enemy installation, you have gained brief temporary access to a secret chip, which contains a hardware implementation of the DES encryption algorithm, along with a single secret key. You connect the chip to your bullet-proof laptop and quickly manage to encrypt a few thousand 64-bit plaintext blocks of your choice, and record the resulting 64-bit ciphertext blocks. You are unable to directly read out the DES key K used in the chip to perform these encryptions and you will not be able to leave the site without knowing K. But you know that all S-boxes in the last DES round are supplied in this chip via a *separate* power-supply pin. When you create a short-circuit on that pin, the encryption progresses as normal, except that the output of all S-boxes in the last round changes to zero.

(*i*) Explain briefly the role of an S-box and the structure of a single round in DES. [4 marks]

(*ii*) How can you find K, considering that your available time and computing power will not permit you to search through more than 10^9 possible keys? [8 marks]