Section B

4) You have been commissioned to act as a technical consultant to a company producing cryptography software for PCs owned by the general public. You find that, whilst the code they have written follows standards in the main, it uses the Unix inbuilt function random() to generate random numbers, seeded by the time of day.

a) What effect does this have on the usefulness of their software and why? [5]

b) Suggest alternatives for random number generation and seed selection, outlining how they work and why and where you think them better. [15]

c) If the software were instead intended for use on the line between a command-and-control centre and a nuclear missile silo, how would your answer change? [5]

5)

a) Define the terms *mutual authentication* and *authentication server*. [4]

b) The following is an authentication protocol in which principals A and B are trying to achieve mutual authentication.

$A \rightarrow B \qquad A, B, \{I_a, A, B\}_{K_A}$

$B \rightarrow AS \qquad A, B, \{I_a, A, B\}_{K_A}, \{I_b, A, B\}_{K_B}$

$AS \rightarrow B \qquad \{I_a, K_S\}_{K_A}, \{I_b, K_S\}_{K_B}$

$B \rightarrow A \qquad \{I_a, K_S\}_{K_A}$

$A \rightarrow B \qquad \{Data\}_{K_S}$

Key:

- I_a, I_b are nonces
- K_A is the key shared between A and the authentication server
- K_B is the key shared between B and the authentication server
- K_S is the session key

Explain what is happening and discuss whether it achieves the goal of mutual authentication as you have defined above. [11]

c) In IPSec, a variant of the Diffie-Hellman algorithm is used to agree a session key. Explain why it was considered unwise to use the original version of Diffie-Hellman for authentication and key exchange. [6]

[TURN OVER]

6)

a) Define the terms discretionary access control policy, mandatory access control policy and conflict of interest in the context of information security [6]

b) Define a suitable policy for avoiding conflicts of interest in businesses with a variety of clients. Use an example to illustrate how the policy would work. [5]

c) Define the main properties of a Public Key Certificate and indicate the important fields that it contains. [5]

d) A university wishes to use public key certificates for authentication of its students and staff (30,000 students; 10,000 staff). Discuss the issues that they should be considering before they implement it and suggest a procedure for managing the certificates. [9]

[END OF SECTION B]

[END OF PAPER]