Section B

1)

a) Define the terms *stream cipher* and *block cipher* [4]

b) Explain what is meant by a *Feistel cipher* and briefly discuss the rationale behind its design. [8]

c) A naive user decides to encrypt their email messages using a 64-bit block cipher. Their technique involves breaking the message into 64-bit blocks and encrypting each block using the algorithm to produce ciphertext. What are the dangers in doing this and how might they improve their technique? [8]

d) Another naive user decides to produce a stream cipher by using a pseudo-random number generator of the form given below.

$$X_{n+1} = 16807.X_n \mod (2^{31} - 1)$$, where X_0 is the seed

The sender XORs the random number stream with their plaintext stream to obtain ciphertext. The recipient XORs the ciphertext with the same random number stream to obtain the plaintext. They agree the seed to be used in advance.

Briefly explain why this is not a good idea. [5]

2)

a) What is the role of a *security association* in IPsec? [5]

b) I wish to send a packet from machine A to machine B along an IPsec protected tunnel in such a way that it is both authenticated, confidential, and replay protected.

i) Describe the actions that are performed on the packet and the supporting data structures that are used in this process.

ii) How are those data structures initialised?

iii) How does the process ensure authentication, confidentiality and freshness? [20]

[CONTINUED]

3)

a) Briefly state the main *authentication requirements* needed in a distributed computing environment (user workstations connected to servers). [6]

b) Show how functions in the *Kerberos* authentication protocol meets these requirements and indicate any areas which you consider to be weak. [6]

c) A company with about 100 employees hires you to advise on and develop its *security policy*. It has fixed connections to its three main suppliers and uses ISDN and dial-up connections for access to the Web and for e-mail etc. Certain areas of its business are very sensitive, e.g. it cannot afford for its competitors to find out about its new products until their launch.

Discuss your approach to this assignment. You should at least mention the areas your study will address, the likely problems and solutions. (Hint: this is an open-ended question so you are advised to identify the most important areas to address and not spend too much time on it.) [13]

[END OF SECTION B]
[END OF PAPER]