2001 Paper 8 Question 6

Security

In the Wired Equivalent Privacy protocol used in IEEE 802.11 networks, data are protected at the link level during transmission on a wireless LAN. Each frame has a 32-bit CRC appended to it; it is then encrypted using the RC4 stream cipher, initialised with a shared key and a 24-bit initial value; and finally, the initial value is sent with the encrypted frame.

(a) Why is the initial value used? [4 marks]

(b) Is the CRC an appropriate mechanism, and, if not, what should be used instead? [4 marks]

(c) Describe *one* passive attack on this system. [4 marks]

(d) Describe *one* active attack on this system. [4 marks]

(e) What would be the effect of upgrading from RC4 to a stronger cipher, such as AES used in output feedback mode? [4 marks]