1994 Paper 8 Question 1

Additional Topics I and II

Cryptosystems can provide *confidentiality* or *integrity*. Consider two messages, one encrypted using a one-time pad and the other, a certificate signed using the private key from a public key system. Which of these two properties do each of these cryptosystems provide? [3 marks]

Explain why five-letter groups are sometimes used for encyphered messages. [4 marks]

Explain how a Vigenère cypher can be attacked. [9 marks]

Is this an asymmetric cypher? [2 marks]

Give a reason why an authentication service might be used instead of individuals sharing keys. [2 marks]