2004 Paper 7 Question 16

Additional Topics

Guy Fawkes and TESLA are streaming authentication protocols based on hash chains.

(*a*) Describe the problem that Guy Fawkes was designed to solve. [2 marks]

(*b*) Briefly describe how Guy Fawkes works. Draw a diagram of a Guy Fawkes packet (or several) and explain the function and purpose of all the parts. [8 marks]

(*c*) List and explain the practical shortcomings of Guy Fawkes. [4 marks]

(*d*) Draw a diagram of a chain of TESLA packets. For each of the Guy Fawkes shortcomings you found in part (*c*), explain how TESLA fixes it, if it does. [6 marks]