2011 Paper 7 Question 12

Security II

(*a*) Write out the Needham–Schroder protocol, explaining the notation you use. [5 marks]

(*b*) Describe the "bug" in the protocol, stating why some people consider it to be a bug and other people consider it not to be. [5 marks]

(*c*) Provide an amended protocol that does not have the "bug" but which (unlike Kerberos) uses random nonces rather than timestamps. [10 marks]