1995 Paper 9 Question 6

Security

The Tatebayashi–Matsuzaki–Newmann protocol may be described as follows:

$$\begin{array}{lcll} A & \rightarrow & S & : \quad {r_A}^3 \pmod N \\ B & \rightarrow & S & : \quad {r_B}^3 \pmod N \\ S & \rightarrow & A & : \quad r_A \oplus r_B \end{array}$$

Explain what is happening here, including the goal and the assumptions. [4 marks]

How can this protocol be attacked? [10 marks]

It has been suggested that the protocol can be strengthened by changing the contents of the last message to $\{r_B\}_{r_A}$ (r_B encrypted by r_A using a secret key algorithm). Does this help? Explain your answer. [6 marks]