2005 Paper 3 Question 9

Introduction to Security

(*a*) A and B play a simple game. A chooses a number $R_A \in \mathbb{Z}_3$ and B chooses a number $R_B \in \mathbb{Z}_3$. Then A and B communicate their respective choice to each other *simultaneously*, meaning that the players cannot change their choice after having seen that of the opponent. These rules decide who wins the game:

$$\begin{aligned} R_A &\equiv R_B + 1 \pmod 3 \quad \Rightarrow \quad A \text{ wins} \\ R_B &\equiv R_A + 1 \pmod 3 \quad \Rightarrow \quad B \text{ wins} \end{aligned}$$

In any other case, the result of the game is a draw.

(*i*) What complication arises when this game is played at a distance, for example via e-mail? [2 marks]

(*ii*) Suggest a cryptographic protocol that prevents cheating when this game is played via e-mail. Your solution should not rely on a trusted third party. [6 marks]

(*iii*) What assumptions do you make about the cryptographic functions used in your solution of part (*ii*)? [3 marks]

(*iv*) What assumptions do you make about the amount of computing power available to the opponent in your solution of part (*ii*)? [3 marks]

(*b*) Outline briefly the purpose of an organisation's security policy and what steps should be considered in its development. [6 marks]