1996 Paper 9 Question 9

Security

Shamir's three-pass protocol enables Alice to send a message m to Bob in the following way:

$$\begin{array}{ll} A \to B : m^{ka} & (\text{mod } p) \\ B \to A : m^{ka\,kb} & (\text{mod } p) \\ A \to B : m^{kb} & (\text{mod } p) \end{array}$$

Explain this protocol, stating the constraint on m and the principal vulnerability. [10 marks]

It is suggested that the encryption operation $m \to m^{kx}$ be replaced with a provably secure encryption operation, namely a one-time pad. How would this affect the protocol's security? [10 marks]