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

- $A \rightarrow B : m^{ka} \pmod{p}$
- $B \rightarrow A : m^{ka \cdot kb} \pmod{p}$
- $A \rightarrow B : m^{kb} \pmod{p}$

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

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