2000 Paper 9 Question 6

Security

The owner of a banking system which previously used manually distributed shared keys to compute MACs on transactions decides to use public key cryptography to distribute MAC keys in future. The proposed protocol is

$$A \to B : \{\, \{T_A, K_{AB}\}_{K_A^{-1}} \,\}_{K_B}$$

Explain the symbolism used in this description. [2 marks]

What is wrong with this protocol? [6 marks]

The protocol is changed to

$$A \to B : \{\, \{A, T_A, K_{AB}\}_{K_A^{-1}} \,\}_{K_B}$$

What attacks might there be on the system now? [12 marks]