Part 2 Security 2000

(2) The ~~designer~~ 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

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

Explain the symbolism used in this description. (2 marks)

What is wrong with this protocol ? (6 marks)

The protocol is changed to

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

What attacks might there be on the system now? (12 marks)

First - bookwork . K_A : A's public key K_A^{-1} : A's private key. K_{AB} : shared key

Second - bookwork. This is the Denning - Sacco protocol lightly disguised. B can masquerade as A by sending $\{\{T_A, K_{AB}\}_{K_A^{-1}}\}_{K_C}$ to C - this works for the duration of timestamp A.

Third - the same attack still works. To stop it one should have inserted the recipient's name in the key packet, not the sender's.