Protocols

Tom Kelliher, CS 400

Write no more than one page per problem.

1. The protocol we designed for securely using a key transmitter to open a car door was:

$$\begin{aligned} C &\longrightarrow T : N \\ T &\longrightarrow C : \{N\}_K \end{aligned}$$

   where K, the encryption key, is only known to C and T. Section 3.3.1 of the textbook suggests:

$$\begin{aligned} C &\longrightarrow T : N \\ T &\longrightarrow C : \{T, N\}_K \end{aligned}$$

   (The third edition of the textbook has $T \longrightarrow C : T, \{T, N\}_K$ for the second line of the protocol. Is this a typo?) Compare and contrast the security of the two approaches.

2. In your own words, describe the problem with the Needham-Schroeder protocol, discussed in Section 3.7.2. Feel free to consult other sources (Wikipedia, etc.).