# Exercises accompanying 'The Modelling and Analysis of Security Protocols'

## Chapter 3

## Secrecy

**Exercise 3.1** How would you change the system model to enable the distinction between initiator and responder claims of secrecy? △

**Exercise 3.2** Give the Yahalom responder's protocol description with restricted occurrence of $Claim\_secret$. △

**Exercise 3.3** Give an example of a protocol which provides secrecy in the context of the external threat model (where all agents are honest and uncompromised) but not against the internal threat model (where the intruder has access to keys). △

## Authentication

**Exercise 3.4** The Otway-Rees protocol is described as follows:

Message 1. $a \rightarrow b \ : \ m.a.b.\{n_a.m.a.b\}_{ServerKey(a)}$
Message 2. $b \rightarrow s \ : \ m.a.b.\{n_a.m.a.b\}_{ServerKey(a)}.\{n_b.m.a.b\}_{ServerKey(b)}$
Message 3. $s \rightarrow b \ : \ m.\{n_a.k_{ab}\}_{ServerKey(a)}.\{n_b.k_{ab}\}_{ServerKey(b)}$
Message 4. $b \rightarrow a \ : \ m.\{n_a.k_{ab}\}_{ServerKey(a)}$

- Give the message sequence chart for a correct run of this protocol.
- Use your message sequence chart to identify the points at which signals need to be inserted for authenticating the responder to the initiator. What information particular to the run can be included in the signals?
- Insert signals for describing authentication of the initiator to the responder. What information can be included in this case?

△

**Exercise 3.5** Express the authentication properties specified in Exercise 3.4 in the process-oriented style. △

**Exercise 3.6** Express as a trace specification the requirement on duplication of runs captured by $INIT\_AUTH\_SPEC$. △

## Non-repudiation

**Exercise 3.7** Is non-repudiation still present if the label $l$ is omitted from the messages that are sent? Is $NRR$ still present? How about $NRO$ ? △

**Exercise 3.8** How would fairness be specified for a non-repudiation protocol? △

**Exercise 3.9** Specify that $b$ should not have the message $m$ until $a$ has the required evidence that $b$ has received message $m$. △

## Anonymity

**Exercise 3.10** If one of the coins is double-headed, but the cryptographers do not know which, does the system still provide anonymity? How about if one of the coins is double-headed or double tailed, but the cryptographers do not know which? △