Exercise 3: Consider the man-in-the-middle attacks in the following cases.

(a) Identify two consequences when some entries of a data base have been modified.

① Redirection

↳ MITM can intercept the request to add a backup email/number to an account and set it to one of their own so when they request a password reset, the verification link is sent to the attackers email/number ⟹ attacker can hijack account now

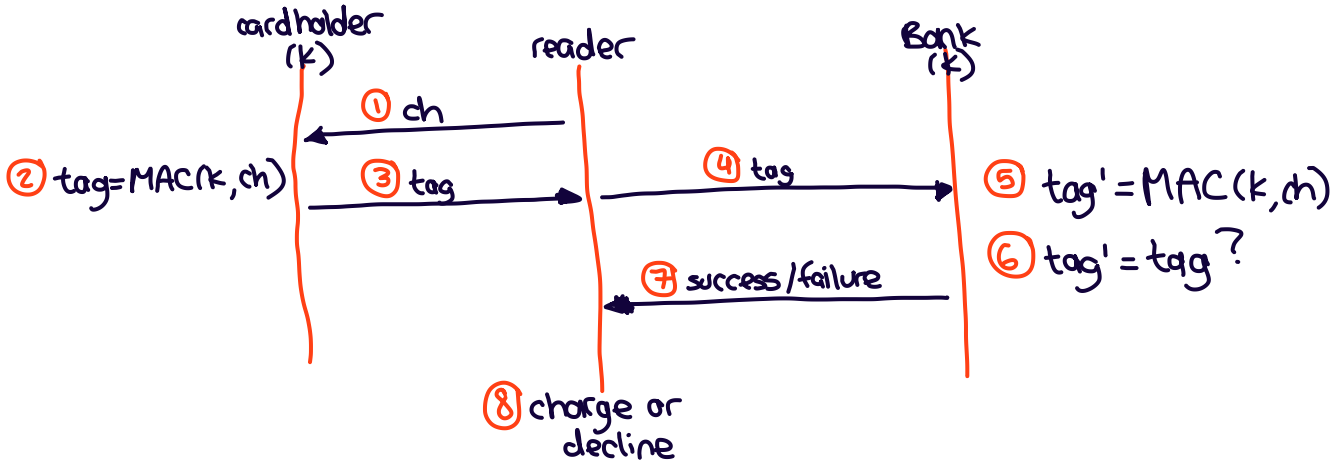
② Modify privileges

↳ attacker can intercept request to create an account and modify the role of the client to expand their CRUD options within an application (i.e. grant system admin privileges to a less-privileged role).

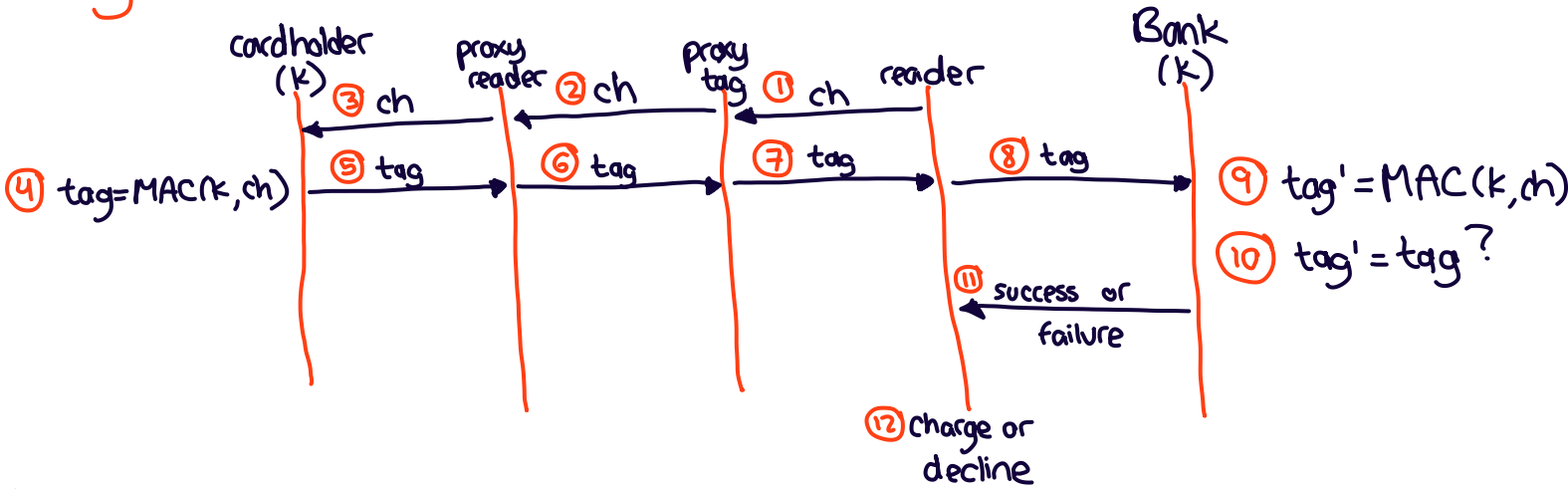
(b) Detail the entity authentication in the RFID system for contactless transaction, shown in the relay attack described in Lecture 3 (page 19).

Standard:

The reader authenticates the chipcard holder using the entity auth protocol (i.e. challenge response)



Relay attack:



in the relay attack case, the proxy tag can't compute the tag because it does not have the cardholder's key so it forwards the challenge from the reader to the proxy reader, which subsequently relays the challenge to the cardholder

(c) For (b), provide three countermeasures for the relay attack.

① RFID Blockers
↳ insulate card technology with metal (aluminum) sheets

② Timing analysis (tamper detection)
↳ measure latency of response times and monitor for discrepancies

③ Distance bounding protocols
↳ cardholder must convince reader that it is within range