Distributed Systems

Tutorial 3

Lecturer: Vrizlynn Thing
Prepared by Morris Sloman

a Briefly explain the differences between shared secret key (symmetric) cryptography and public key (asymmetric) cryptography.

b In an electronic auction, a client C wants to make an offer by sending message M to the auctioneer A. While the message can remain public, it should be associated with an encrypted digital signature obtained by C from the trusted authentication server S. On receipt of the message, A asks S to decrypt the digital signature and must be able to check that the message is recent and has not been modified in transit. Use shared secret keys with C, A and S (each have their individual secret key) and S knows all the secret keys.

Using the following notation:

\[ X, K_{AB}\{Y\} \] A message contains a field X sent as plain text and a field Y encrypted with a shared secret key known to A and B

i) Show how C can make the offer and how A can satisfy itself that the signature is genuine and that the message has not been tampered with. Indicate the contents of messages and explain how your system works.

ii) Can C claim that the signature was forged?

NB. The notarisation service is NOT the correct protocol.