

Distributed Systems

COMP90015 2021 Semester 1
Tutorial 09

Today's Agenda

- Assignment 2 Q & A
- Questions on Security (continued)
- Demo - Client Server Encryption

Assignment 2 Q & A

1. How can Alice authenticate and communicate secretly with Bob assuming there is an authentication server that knows Alice's and Bob's secret keys?

2. Assuming that Bob has a public/private key pair, how can Alice and Bob establish a shared key to communicate secretly using a Key Distribution Service?

3. Explain how digital signatures work.

4. What is a digital certificate and why do we need it?

5. What is the process to obtain a digital certificate?

Code Demo

- Client Server Encryption with AES (Shared Secret Key)