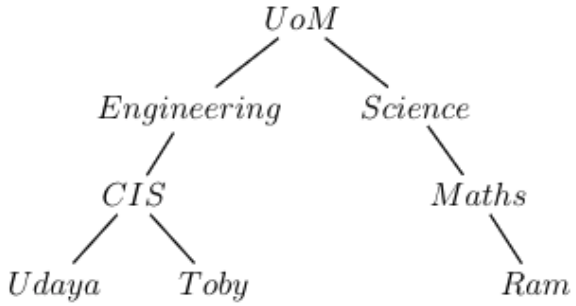
**COMP90043 Cryptography and Security**
**Semester 2, 2020, Workshop Week 9**

## Key Management and Distribution

1. Discuss four methods which are used in distributing public keys.
2. What are the essential ingredients of a public-key directory?
3. What is a chain of certificates? What are forward and reverse certificates?
4. Consider the following:

For the following hierarchy, what is the chain of certificates that user "Udaya" needs to obtain in order to establish a certificate path to "Ram"? You can use X.509 conventions for the certificate chain, for example the certificate for "Udaya" by CA "CIS" is represented as CIS«Udaya».




## ElGamal

- Say a message $M$ is broken up into two blocks $M_1, M_2$ and encrypted using ElGamal encryption. Show how knowledge of the first block $M_1$ allows the use to computer the block $M_2$ if it is know that the same random integer $k$ was used for both blocks.
- Show how to recover the long-term signing key for ElGamal signature if the signer re-uses a secret value $k$.

Notice that reusing the key $k$ for encryption is problematic as blocks of messages can be reproduced, but for ElGamal signature it is a disaster as the private key can be found.