Trusted Third Parties

Mark Lomas
University of Cambridge
Computer Laboratory

What is Trust?

1. a firm belief in the reliability or truth or strength etc. of a person or thing.
2. the state of being relied upon

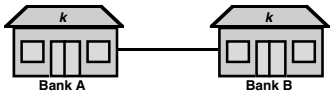
As distinct from "Trustworthy"

- deserving of trust; reliable

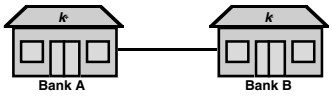
I'll define "Trusted" as

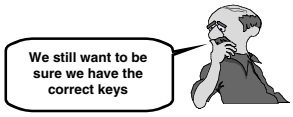
- something that is capable of violating your security policy

Symmetric Keys

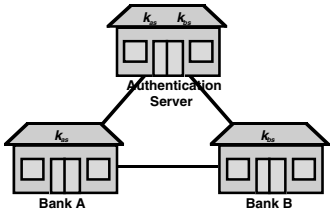


Asymmetric Keys

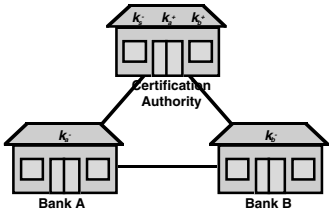




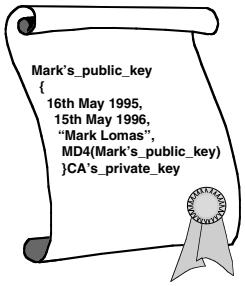
Authentication



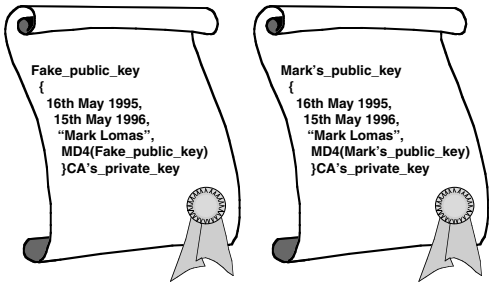
Certification



Certificates



Spotting a Fake



Audit Trails

- **It is important that we log sufficient information to be able to resolve later disputes**
- **This not only protects the user against untrustworthy third parties, it also protects third parties against unwarranted accusations.**

Summary

- **"Trusted" $\neq$ "Trustworthy"**
- **Trusted Third Parties can violate your security policy, so it is important to keep an eye on them**
- **Trusted Third Parties *may* be trustworthy, in which case it is their interest that they be able to prove that they were not responsible for a security breach**