

# File Sharing using Cryptographically Enforced Access Control

Daniel Randall

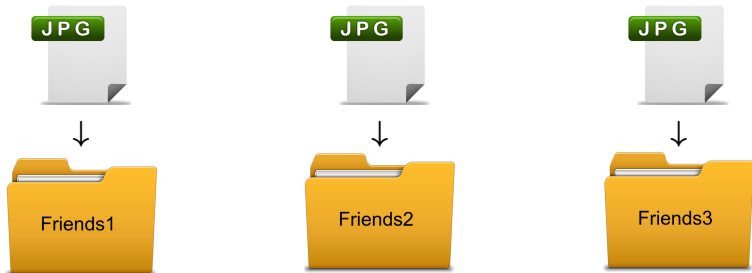
Imperial College London

24th June, 2013

# The problem

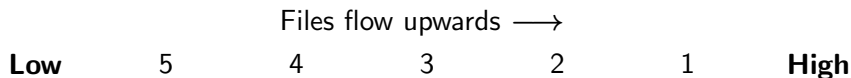
How to share files with multiple groups of people using existing solutions

Share a file with different groups of friends using Dropbox, Wuala, Mega:



## Proposed solution

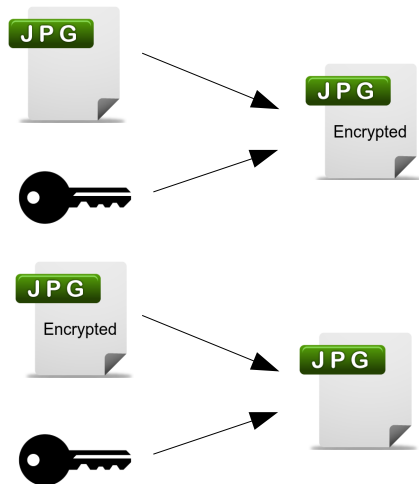
Each file and friend are assigned a rank and the files are automatically transferred to the correct groups



Therefore,  $\text{Group5} \subseteq \text{Group4} \subseteq \text{Group3} \dots$

# How we achieve this

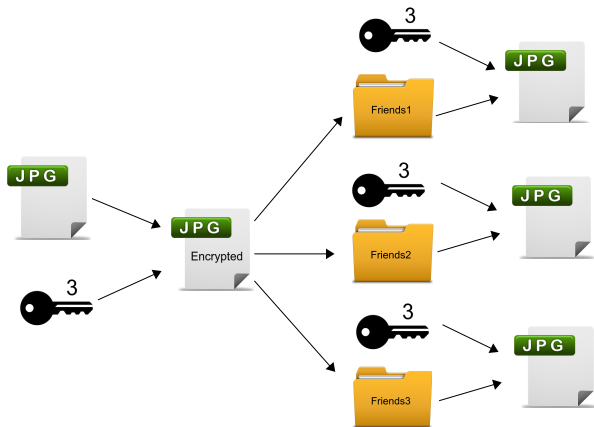
## Asymmetric cryptography



# How we achieve this

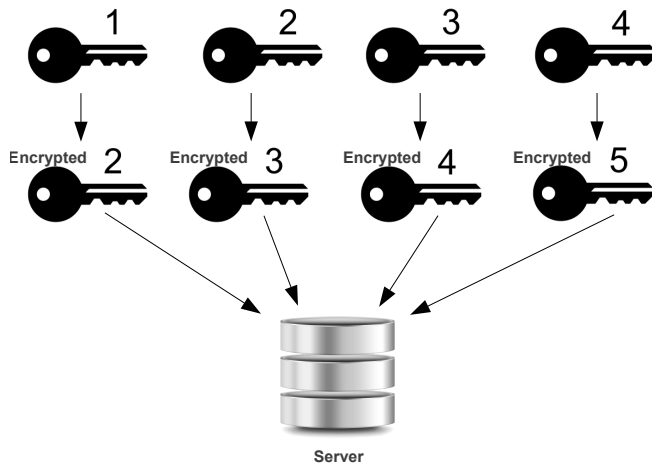
## Cryptography

File labelled with a level  $x$  and the file is encrypted and shared with friends with label  $y$ , where  $y \leq x$ . Example:



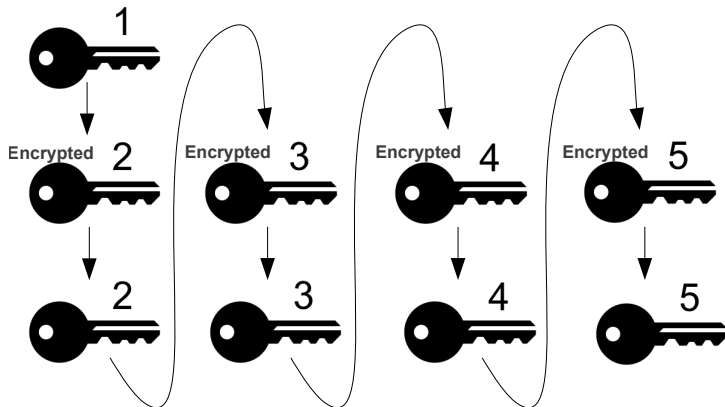
# How we store keys

## Hierarchical cryptography



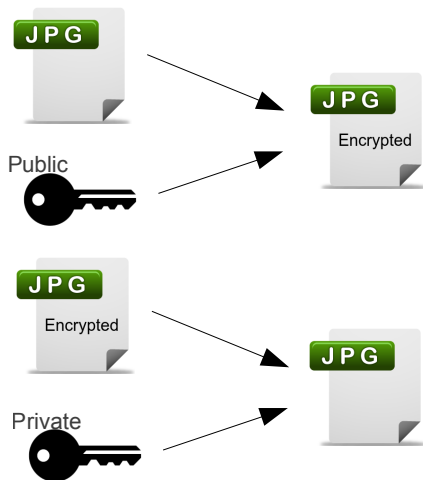
# How we derive keys

## Hierarchical cryptography



# How keys are shared

## Asymmetric cryptography





# How keys are shared

## Asymmetric cryptography

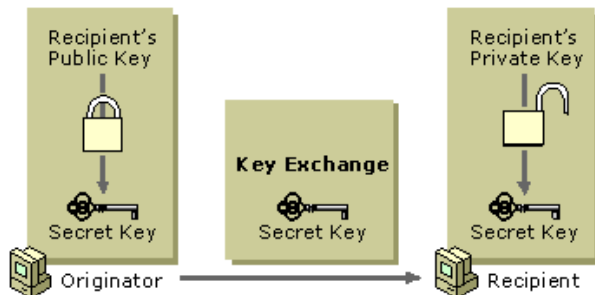


Image source: <http://technet.microsoft.com/en-us/library/cc962035.aspx>

# Updating files

When a friend wishes to modify a file shared with them...

- ▶ Encrypt the new file
- ▶ Share it with all others who have access to it

# Revoking users

When a user no longer wishes to share files with a friend with access level  $x$ ...

- ▶ Replace keys with level  $y$ , where  $y \leq x$
- ▶ Re-encrypt files with level  $y$ , where  $y \leq x$
- ▶ Re-share new keys with friends that still have access

# Applications

Useful in work environments:

- ▶ Project manager
- ▶ Project member
- ▶ Project intern



Level 1

Project manager

Level 2

Project member

Level 3

Project intern

Not so clearly useful in social environments:

- ▶ Mum
- ▶ Friend
- ▶ Uncle

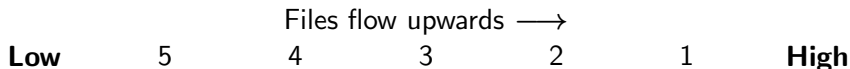


?

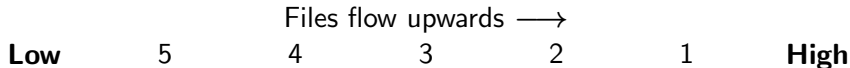
# Future work

## Multiple hierarchies

Group 1:



Group 2:



Where each hierarchy is unrelated

# Future work

## Adjustable lower bounds

Lowest assigned bound does not have to be the lowest available  
(i.e. 5)

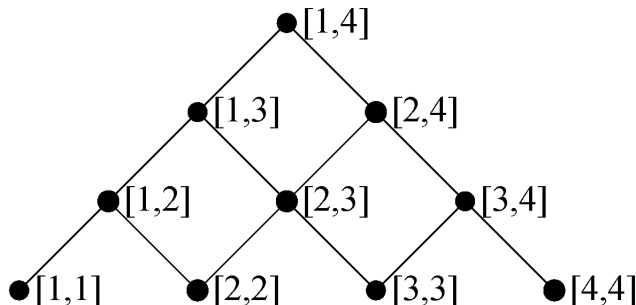


Image source: Jason Crampton, "Practical and Efficient Cryptographic Enforcement of Interval-Based Access Control Policies", 2011.