File Sharing using Cryptographically Enforced Access Control

Daniel Randall

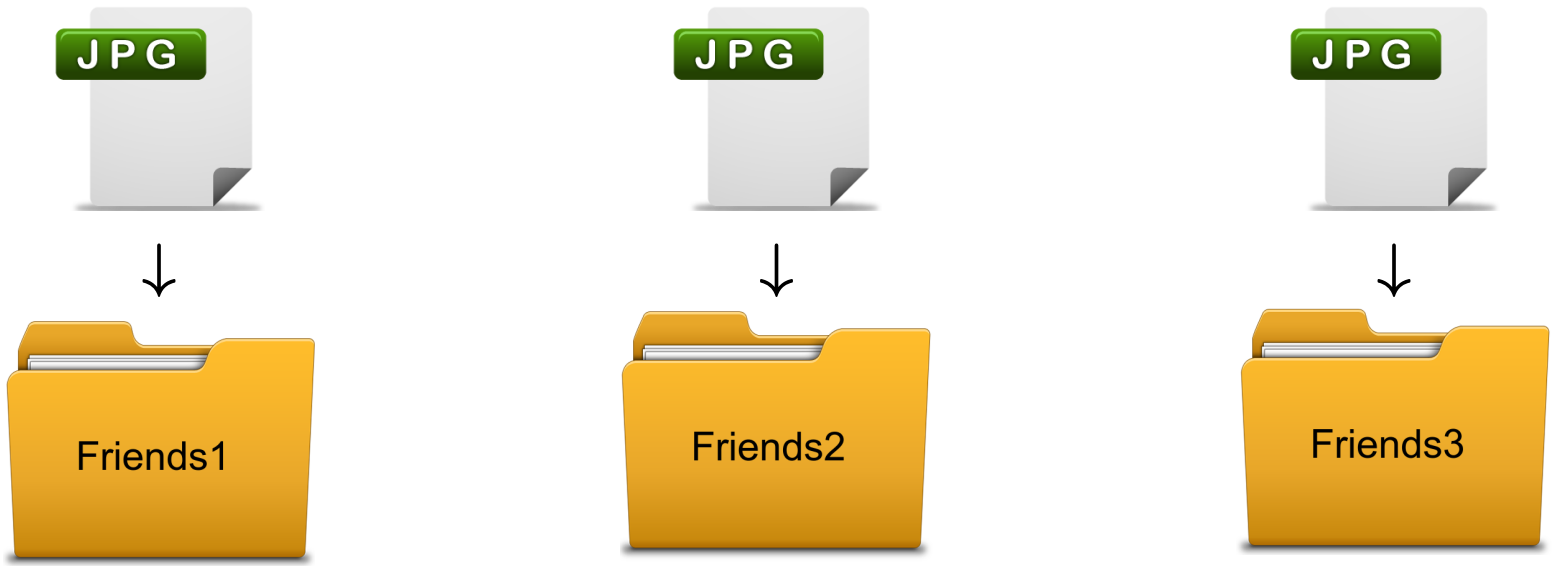
Imperial College London

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

Files flow upwards $\longrightarrow$

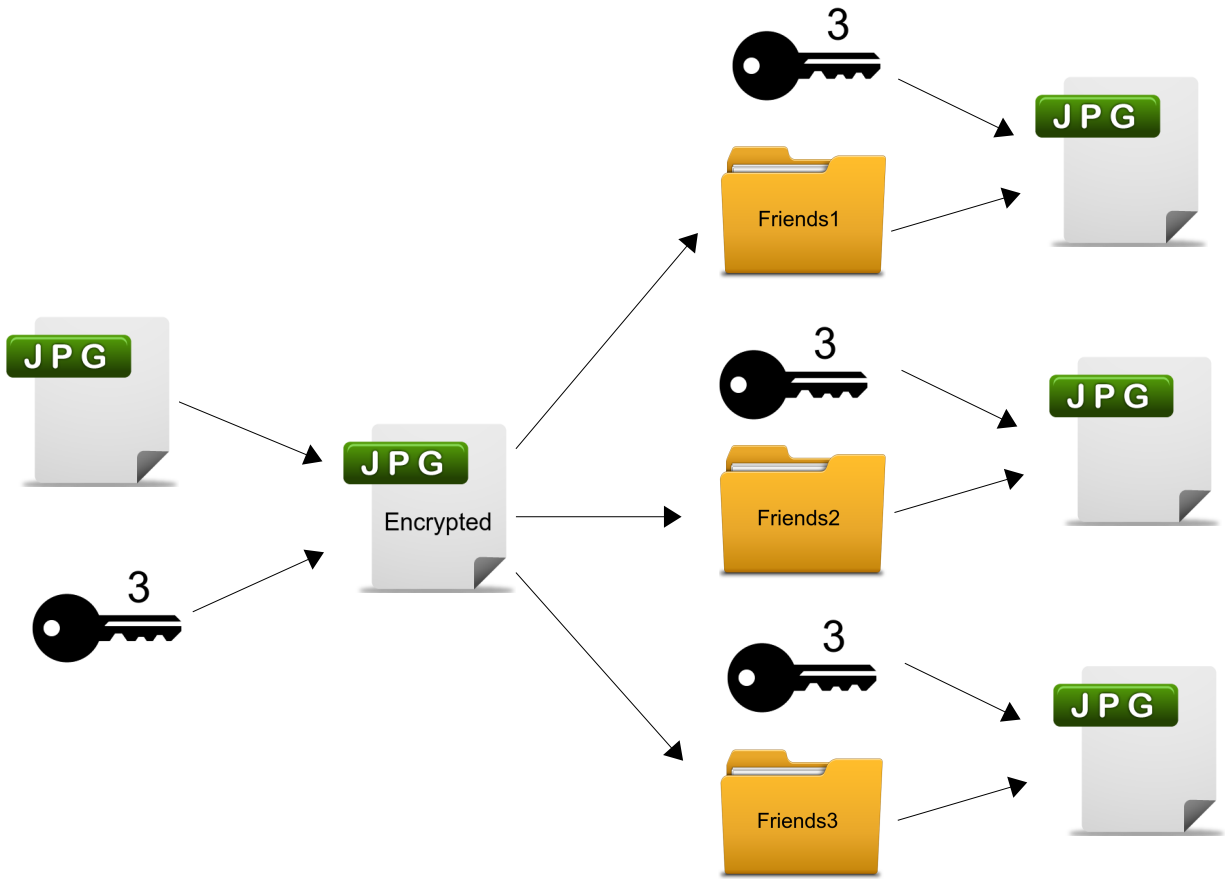
Low 5 4 3 2 1 **High**

Therefore, Group5 $\subseteq$ Group4 $\subseteq$ Group3 ...

How we achieve this

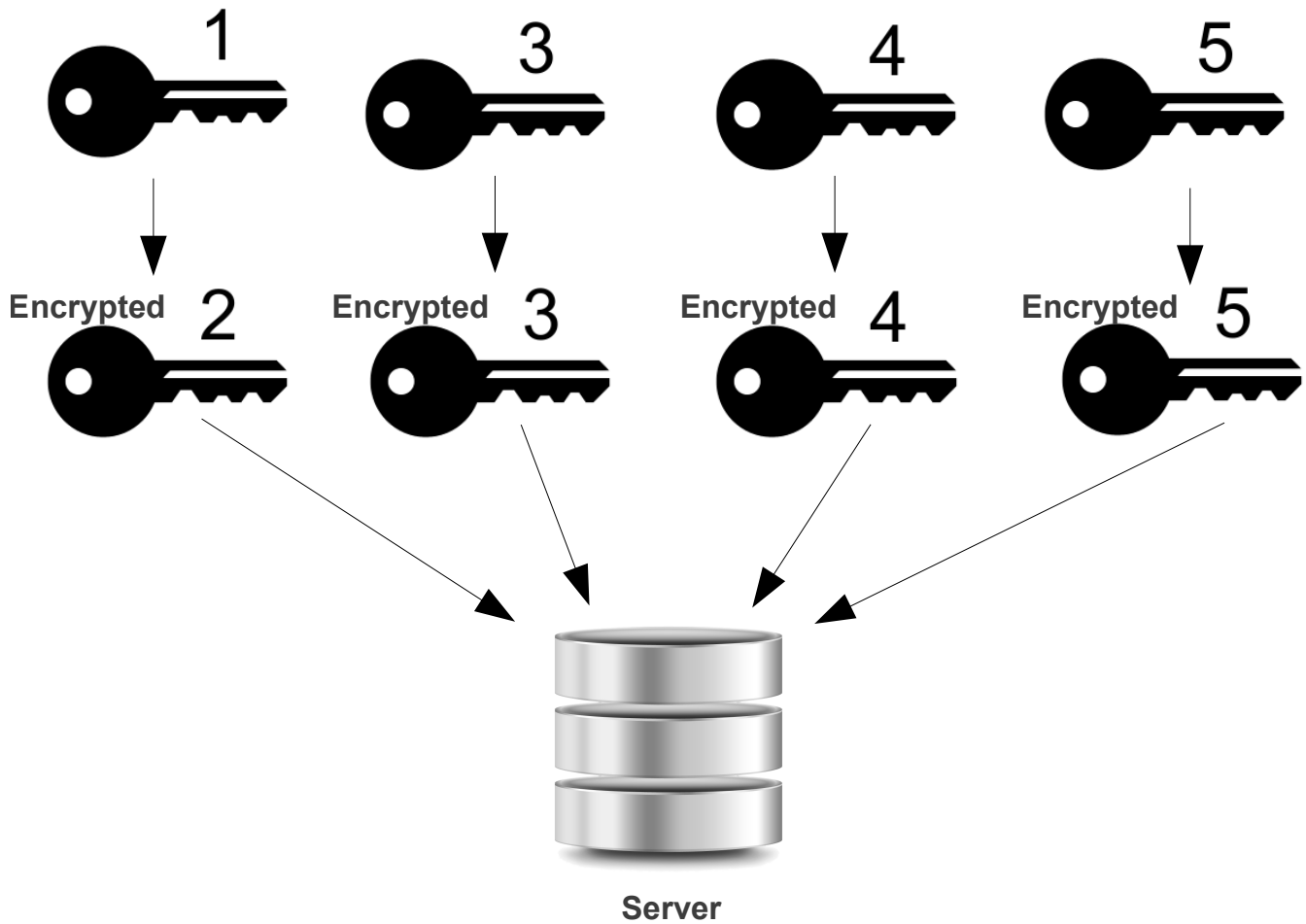
Cryptography

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



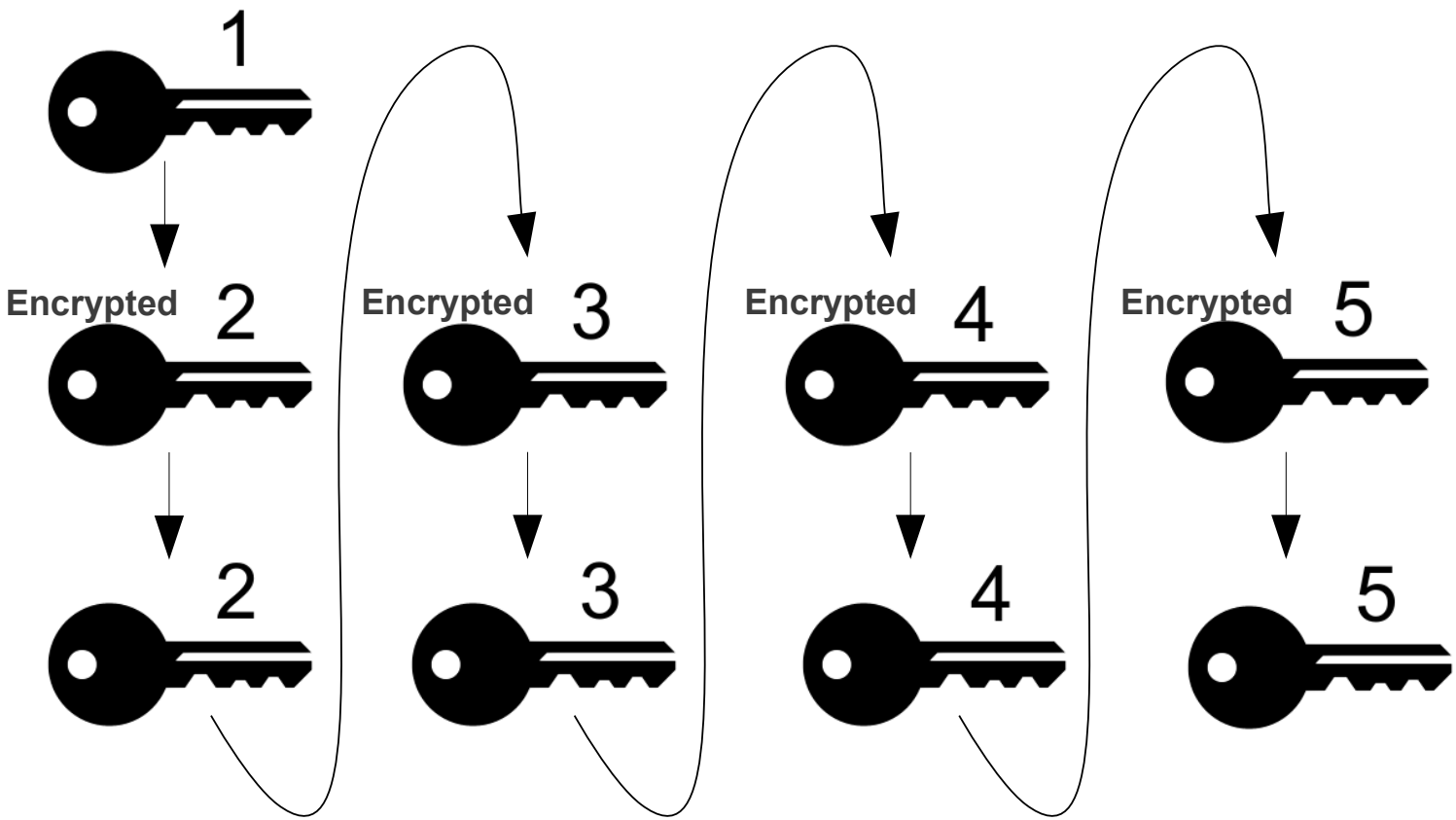
How we store keys

Hierarchical cryptography



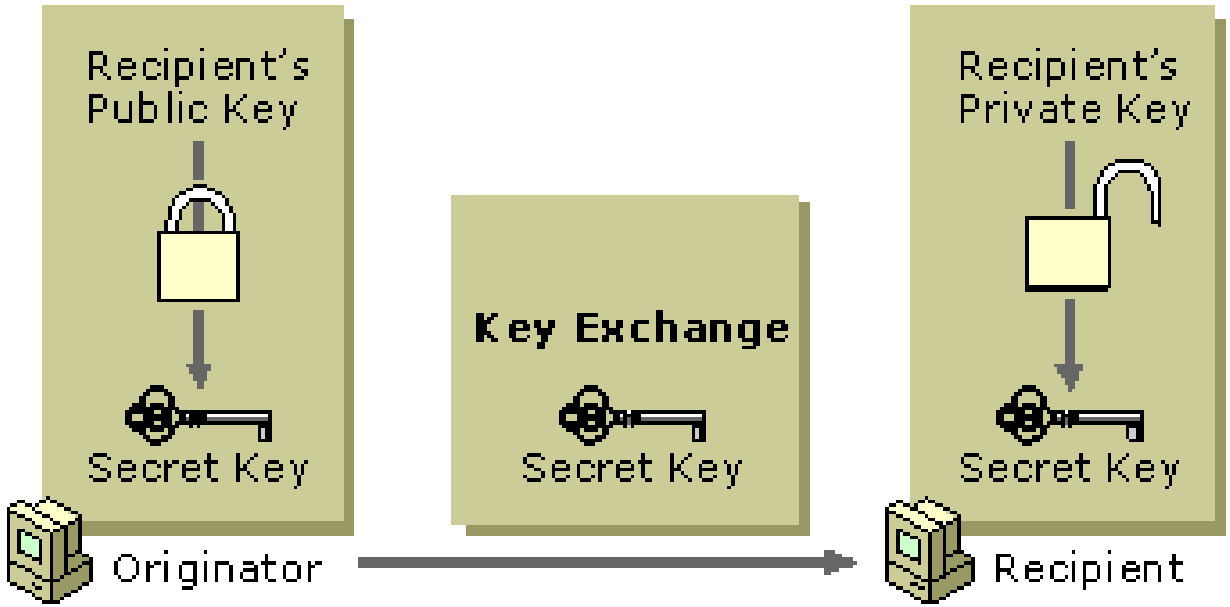
How we derive keys

Hierarchical cryptography



How keys are shared

Public key cryptography



Updating files

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

$\longrightarrow$

Level 1
Project manger

Level 2
Project member

Level 3
Project intern

Not so clearly useful in social environments:

- Mum
- Friend
- Uncle

$\longrightarrow$?

Future work

Multiple hierarchies

Group 1:

Files flow upwards $\longrightarrow$

Low 5 4 3 2 1 **High**

Group 2:

Files flow upwards $\longrightarrow$

Low 5 4 3 2 1 **High**

Where each hierarchy is unrelated

Future work

Adjustable lower bounds

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

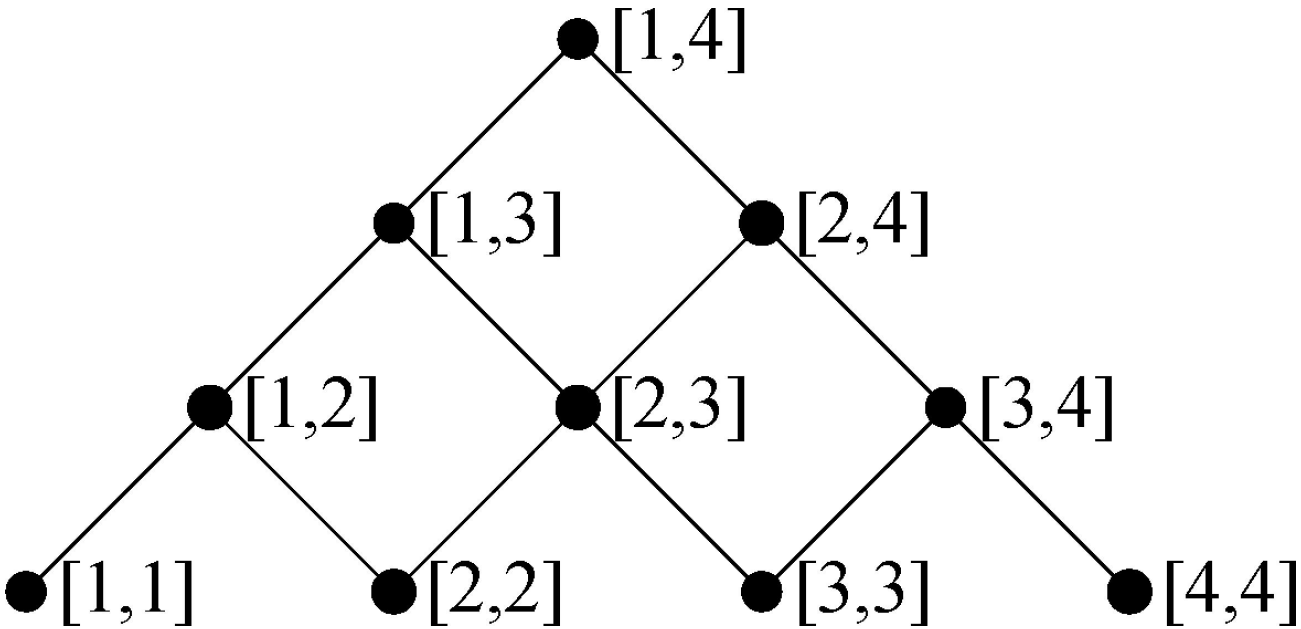


Image source: Jason Crampton, "Practical and Efficient Cryptographic Enforcement of Interval-Based Access Control Policies", 2011.