9 Security I (MGK)

(*a*) While inspecting the discretionary access-control arrangements on a Unix computer, you find the following setup:

Members of group `staff`: `alex`, `benn`, `cloe`
Members of group `gurus`: `cloe`

```
$ ls -ld . * */*
drwxr-xr-x  1 alex staff    32768 Apr  2  2010 .
-rw----r--  1 alex gurus    31359 Jul 24  2011 manual.txt
-r--rw--w-  1 benn gurus     4359 Jul 24  2011 report.txt
-rwsr--r-x  1 benn gurus   141359 Jun  1  2013 microedit
dr--r-xr-x  1 benn staff    32768 Jul 23  2011 src
-rw-r--r--  1 benn staff    81359 Feb 28  2012 src/code.c
-r--rw----  1 cloe gurus      959 Jan 23  2012 src/code.h
```

The file `microedit` is a normal text editor, which allows its users to open, edit and save files.

(*i*) Draw an access control matrix that shows for each of the above five files, whether `alex`, `benn`, or `cloe` are able to obtain the right to read (R) or replace (W) its contents. [12 marks]

	manual.txt	report.txt	microedit	src/code.c	src/code.h
alex					
benn					
cloe					

(*ii*) Which users have at least all the access rights of which other users? [2 marks]

(*b*) Explain briefly *three* mechanisms that the operating system kernel of a desktop computer can use to generate unpredictable numbers for use in cryptographic protocols as soon as it has booted. [6 marks]