8 Security I (MGK)

(a) Windows implements static inheritance for the access-control lists of NTFS files and folders.

(i) What does static inheritance mean here and how does it differ from dynamic inheritance?  [4 marks]

(ii) Five flag bits (ci,oi,np,io,i) in each NTFS access-control entry (ACE) manage how it is inherited. Briefly describe the purpose of each bit.  [5 marks]

(iii) User mike gives his folder project the following access-control list:

```
project
  AllowAccess mike: full-access (oi,ci)
  AllowAccess alice: read-execute (ci,np)
  AllowAccess bob: read-only (oi)
```

It contains one folder and two text files, none of which have any non-inherited access-control entries:

```
project\doc.txt
project\src
project\src\main.c
```

For each of these three objects, list all inherited access-control entries, showing in parentheses the inheritance-control flag bits that are set (using the same notation as above).  [5 marks]

(b) Describe the purpose and four typical functions of a root kit.  [6 marks]