8 Security I (MGK)

(a) Compare and contrast the security definitions of a pseudo-random generator and a pseudo-random function. [4 marks]

(b) When a Windows NTFS access control entry (ACE) is inherited by a subdirectory, under which circumstances is the “inherit only” flag set or cleared, and why? [4 marks]

(c) What is existential unforgeability of a message authentication code? [4 marks]

(d) Which problem with CBC-MAC is fixed by ECBC-MAC, and how? [4 marks]

(e) A C program running on a 32-bit processor contains the following function:

```c
void f(int *a, int l) {
    int *b, i;
    b = (int *) malloc(l * sizeof(int));
    if (b == NULL) return;
    for (i = 0; i < l; i++)
        b[i] = a[i];
    [...]
}
```

(i) How can a caller cause this function to overwrite unallocated memory? [2 marks]

(ii) Modify the function to remove this vulnerability. [2 marks]