## 6 Security (mgk25)

(*a*) During a security review, you encounter the following C function, which may be called by untrusted code:

```
int table[800];

int insert_in_table(int val, int pos) {
    if (pos > sizeof(table) / sizeof(int)) return -1;
    table[pos] = val;
    return 0;
}
```

Identify potential vulnerabilities and provide a fixed version. [4 marks]

(*b*) When you log into a system that uses Kerberos authentication by providing a password (e.g., using the Unix/Linux/macOS command `kinit`):

(*i*) What data does your computer send to and receive from the key-distribution centre (KDC) and which parts of that data are encrypted with whose key or password? [9 marks]

(*ii*) What is the purpose of a ticket-granting ticket? [2 marks]

(*iii*) Where are Kerberos tickets stored? [2 marks]

(*c*) Suggest and briefly explain three countermeasures used by a typical Linux distribution to mitigate the risk of stack-overflow vulnerabilities in included software. [3 marks]