9 Security I (MGK)

(*a*) Let $\mathsf{Enc}_{K_\mathrm{E}}$ be the encryption function of an encryption scheme that provides indistinguishability under chosen plaintext attack (CPA security). Let $\mathsf{Mac}_{K_\mathrm{M}}$ be a message-authentication-code function that provides existential unforgeability. Named below are three techniques for applying these two functions together to a message M. For each of them

- briefly explain how $\mathsf{Enc}_{K_\mathrm{E}}$ and $\mathsf{Mac}_{K_\mathrm{M}}$ are combined, and
- state whether the resulting construct is likely to provide indistinguishability under chosen ciphertext attack (CCA security):

(*i*) encrypt-and-authenticate [2 marks]

(*ii*) authenticate-then-encrypt [2 marks]

(*iii*) encrypt-then-authenticate [2 marks]

(*b*) How can an attacker calling the C function `parse_text` below cause a buffer overflow? Explain how and why this works. [6 marks]

```
#include <stdlib.h>
#include <string.h>
#define BUFLEN 4096
int check(int n) {
  if (n > BUFLEN) abort();
  return n;
}
void parse_text(char *text, size_t len) {
  char buf[BUFLEN];
  memcpy(buf, text, check(len));
  /* ... */
}
```

(*c*) Many Unix system administrators create a personal group for each of their users with this user as the sole member.

(*i*) What is the purpose of such a group? [2 marks]

(*ii*) Such personal groups typically have the same name and integer identifier as the corresponding user identifier. Is this practice compatible with the Windows NT mechanism for identifying users and groups? [2 marks]

(*d*) Give two examples for resources where an operating system is expected to implement residual information protection and two alternative mechanisms for implementing it. What are their tradeoffs and threat assumptions? [4 marks]