Student ID: _____

This sheet will not be graded (feel free to write on it), but you must turn it in at the end of the exam.

C Function Definitions

```
size_t fread(void *ptr, size_t size, size_t nmemb, FILE *stream);

      The function fread() reads nmemb items of data, each size bytes long,
      from the stream pointed to by stream, storing them at the location
      given by ptr.

int getchar(void);

      getchar() reads the next character from stdin and returns it as an
      unsigned char cast to an int, or EOF on end of file or error.

int printf(const char *format, ...);

      printf() produces output according to the format string format.

int scanf(const char *format, ...);

      The scanf() function reads input from the standard input stream stdin,
      according to the format string format. This format may contain
      conversion specifications; the results from such conversions, if any,
      are stored in the locations pointed to by the pointer arguments that
      follow format.

size_t strlen(const char *s);

      The strlen() function calculates the length of the string pointed to by
      s, excluding the terminating null byte ('\0').

char *strcpy(char *dest, const char *src);

      The strcpy() function copies the string pointed to by src, including
      the terminating null byte ('\0'), to the buffer pointed to by dest.
      The strings may not overlap, and the destination string dest must be
      large enough to receive the copy.
```

```
char *strncpy(char *dest, const char *src, size_t n);

      The  strncpy()  function copies the string pointed to by src, including
      the terminating null byte ('\0'), to the  buffer  pointed  to  by  dest.
      The  strings  may  not  overlap,  and  at  most n bytes of s are copied.
      Warning: If there is no null byte among the first n bytes of  src,  the
      string placed in dest will not be null-terminated.

      If  the  length of src is less than n, strncpy() writes additional null
      bytes to dest to ensure that a total of n bytes are written.

int remove(char *pathname);

      remove() deletes a name from the filesystem.
```

General Exam Assumptions

- You are on a little-endian 32-bit x86 system.
- There is no compiler padding or saved additional registers.
- If stack canaries are enabled, they are four completely random bytes (**no null byte**).
- You can write your answers to in either Python 2 (as seen in past exams or discussions) or Python 3 syntax (as seen in Project 1).
  - Recall that bytes in Python 3 syntax are written as `b'\xef\xbe\xad\xde'`.
  - Recall that bytes in Python 2 syntax are written as `'\xef\xbe\xad\xde'`.
- $\|$ denotes concatenation.
- Unless otherwise specified, the IV is randomly generated.
- Unless otherwise specified, the following symbols refer to the the following cryptographic functions:
  - Enc/Dec refers to an IND-CPA secure encryption function.
  - MAC refers to an EU-CPA secure MAC function.
  - H refers to a secure cryptographic hash function.
- Unless otherwise specified, M_i refers to the ith block of message M.