

This sheet will not be graded (feel free to write on it).

C Function Definitions

```
void *memcpy(void *dest, const void * src, size_t n);
```

The `memcpy()` function copies `n` bytes from memory area `src` to memory area `dest`.

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

The `strncpy()` function copies at most `n-1` characters from the string pointed to by `src` to the buffer pointed to by `dest`. If the source string is shorter than `n-1` characters, the remaining bytes in `dest` are padded with `'\0'`. A null terminator is always added.

General Exam Assumptions

Unless otherwise specified, you can assume these facts on the entire exam:

- Memory Safety:
 - 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 in Python syntax (as seen in Project 1).
 - Unless otherwise specified, all other memory safety defenses are disabled.
 - Unless otherwise specified, each x86 instruction is 4-bytes long in machine code.
- Cryptography:
 - The attacker knows the algorithms being used (Shannon's maxim).
 - $\parallel$ denotes concatenation.
 - H refers to a secure cryptographic hash function.
 - g and p refer to a public generator element and large prime modulus, respectively.
 - IVs are randomly generated per encryption unless otherwise specified.
 - Enc refers to an IND-CPA secure encryption scheme, unless otherwise specified.