

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

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`.

Note that `fread()` does not add a null byte after input.

```
char *fgets(char *s, int size, FILE *stream);
```

`fgets()` reads in at most one less than `size` characters from `stream` and stores them into the buffer pointed to by `s`. Reading stops after an EOF or a newline. If a newline is read, it is stored into the buffer. A terminating null byte (`'\0'`) is stored after the last character in the buffer.

```
int strcmp(const char *s1, const char *s2);
```

The `strcmp()` function compares the two strings `s1` and `s2`. It returns an integer less than, equal to, or greater than zero if `s1` is found, respectively, to be less than, to match, or be greater than `s2`.

```
size_t strlcpy(char *dst, const char *src, size_t dstsize);
```

`strlcpy()` copies up to `dstsize - 1` characters from the string `src` to `dst`, NUL-terminating the result if `dstsize` is not 0.

SQL Syntax

```
SELECT column1, column2, ...  
FROM table_name  
WHERE condition;
```

```
INSERT INTO table_name (column1, column2, column3, ...)  
VALUES (value1, value2, value3, ...);
```

```
UPDATE table_name  
SET column1 = value1, column2 = value2, ...  
WHERE condition;
```

```
DELETE FROM table_name WHERE condition;
```

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.
 - 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.
 - IV s are randomly generated per encryption unless otherwise specified.
 - Enc refers to an IND-CPA secure encryption scheme unless otherwise specified.
- Networking:
 - DNSSEC does not use ZSKs/KSKs, unless otherwise specified.