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

```
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.

char *gets(char *s);

    gets() reads a line from stdin into the buffer pointed to by s until
    either a terminating newline or EOF, which it replaces with a null
    byte ('\0').
```

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).
- Cryptography:
  - The attacker knows the algorithms being used (Shannon's maxim).
  - $\oplus$ denotes bitwise XOR.

Andor, or XOR? Code

Below is the code in the *Andor, or XOR?* question, repeated for your convenience.

```
1  void galaxy(char *clone) {
2      char droid[64];
3      int i = 0;
4      int j = 0;
5      char force[24];
6      gets(droid);
7      gets(force);
8      gets(clone);
9
10     while (0 <= i && i < 24 && 0 <= j){
11         if (clone[i] == 0x54) {
12             clone[i] = force[i] ^ droid[j];
13         } else {
14             clone[i] = force[i] ^ clone[i];
15         }
16         i++;
17         j++;
18     }
19 }
20
21 int main() {
22     char rebel[16];
23     galaxy(rebel);
24     return 0;
25 }
```