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

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

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

      Conversion specifiers:
      %s  String (pointer to a character array).
          Outputs bytes until null terminator.
      %x  Hexadecimal.

      Each of the above conversion specifiers reads a 4-byte argument on the stack.

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 *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.
```

8-bit Two's Complement Hexadecimal Conversion Table

Hex	Unsigned	Signed	Hex	Unsigned	Signed
0xec	236	-20	0xf6	246	-10
0xed	237	-19	0xf7	247	-9
0xee	238	-18	0xf8	248	-8
0xef	239	-17	0xf9	249	-7
0xf0	240	-16	0xfa	250	-6
0xf1	241	-15	0xfb	251	-5
0xf2	242	-14	0xfc	252	-4
0xf3	243	-13	0xfd	253	-3
0xf4	244	-12	0xfe	254	-2
0xf5	245	-11	0xff	255	-1

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).
  - If ASLR is enabled, the code segment is randomized.
  - You can write your answers in Python syntax (as seen in Project 1).
  - On one execution of the program, all stack frames have the same canary value.
- Cryptography:
  - The attacker knows the algorithms being used (Shannon's maxim).
  - $\|$ denotes concatenation.
  - H refers to a secure cryptographic hash function.
  - E_K refers to an AES function using key K.
  - g and p refer to a public generator element and large prime modulus, respectively.
  - IVs are randomly generated per encryption unless otherwise specified.

Below is the code in the *Across the Security-Verse* question, repeated for your convenience.

```
1  void verse() {
2      char miles[256];
3      fgets(miles, 257, stdin);
4  }
5
6  void spider() {
7      verse();
8  }
9
10 void main() {
11     char *peter = (char *) malloc(128);
12     gets(peter);
13     printf("%x", peter);
14     spider();
15 }
```

Below is the code in the *Snacktime* question, repeated for your convenience.

```
1  void goldfish(char* potato) {
2      fgets(potato, 256, stdin);
3
4      int8_t chip = strlen(potato);
5      printf("%s", &potato[chip]);
6
7      gets(potato);
8  }
9
10 void main() {
11     char cola[256];
12     goldfish(cola);
13 }
```