This sheet will not be graded (feel free to write on it). You do not need to turn it in at the end of the exam. Please do not open the appendix until the exam begins.

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.

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

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

      Conversion specifiers:
      %c  Character.
      %d  Signed integer.
      %n  Writes the number of bytes printed so far, as a 4-byte
          integer, to the corresponding memory address.
      %s  String.
      %u  Unsigned integer.
      %x  Unsigned integer, in hexadecimal.

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

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').

void *memset(void s, int c, size_t n);

      The memset() function fills the first n bytes of the memory area
      pointed to by s with the constant byte c.
```

Cipher Block Modes of Operation

The following are the encryption formulas for common block cipher modes taught in the course:

- AES-ECB
  - Encryption: $C_i = E_K(M_i)$
  - Decryption: $M_i = D_K(C_i)$
- AES-CTR
  - Encryption: $C_i = E_K(\text{Nonce} + i) \oplus M_i$
  - Decryption: $M_i = E_K(\text{Nonce} + i) \oplus C_i$
- AES-CBC:
  - Encryption:

    $$C_i = E_K(M_i \; \oplus \; C_{i-1})$$
    $$C_0 = IV$$
  - Decryption: $M_i = D_K(C_i) \oplus C_{i-1}$

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).
  - You can write your answers in Python syntax (as seen in Project 1).
  - All memory safety defenses are disabled.
  - Each x86 instruction is 4 bytes long in machine code.
  - The `main` function acts like all other functions, with an RIP and SFP at the top of its stack frame.
- Cryptography:
  - The attacker knows the algorithms being used (Shannon's maxim).
  - $\|$ 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.
  - Enc refers to an IND-CPA secure encryption scheme.
- Networking:
  - All DNS records are cached by the recursive resolver.
  - Assume Bailiwick checking is always enabled in DNS.
  - Every zone in DNS has its own name server. For example, a query for `joy.cs161.org` gets answered by the `cs161.org` name server, not the `.org` name server.