SID: _____

This sheet will not be graded (feel free to write on it), but you must turn it in at the end of the exam.

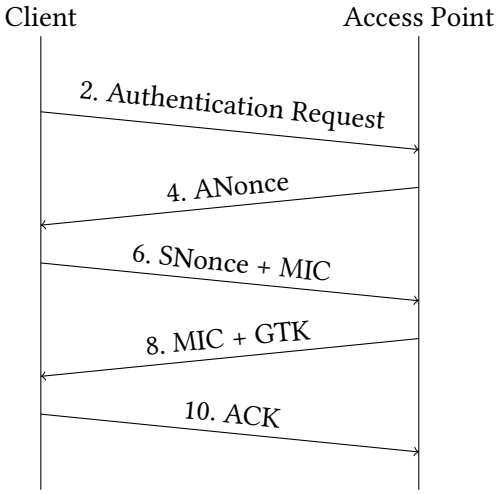
C Function Definitions

```
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.

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 ter-
       minating null byte ('\0')  is  stored  after  the  last
       character in the buffer.
```

Below is a copy of the code snippet from Question 3 (I Understood that Reference!), reproduced for your convenience.

```
1  void vulnerable(int start, char *ptr) {
2      ptr[start] = ptr[3];
3      ptr[start + 1] = ptr[2];
4      ptr[start + 2] = ptr[1];
5      ptr[start + 3] = ptr[0];
6  }
7
8  void helper(int num) {
9      if (num > 124) {
10         return;
11     }
12     char arr[128];
13     fgets(arr, 128, stdin);
14     vulnerable(num, arr);
15 }
16
17 int main(void) {
18     int y;
19     fread(&y, sizeof(int), 1, stdin);
20     helper(y);
21     return 0;
22 }
```

Below is a copy of the WPA 4-way handshake diagram from lecture and Question 8 (I am Inevitable), reproduced for your convenience.



1. Client and AP derive the PSK from SSID and password.

3. AP randomly chooses ANonce.

5. Client randomly chooses SNonce and derives PTK.

7. AP derives PTK and verifies the MIC.

9. Client verifies the MIC.