Traditional password entry schemes are susceptible to “shoulder surfing” in which an attacker watches an unsuspecting user enter their password or Pin number and uses it later to gain access to the account. One way to combat this problem is with a randomized challenge-response system. In these systems, the user enters different information every time based on a secret in response to a randomly generated challenge. Consider the following scheme in which the password consists of a five digit PIN number (00000 to 99999). Each digit is assigned a random number that is 1, 2, or 3. The user enters the random numbers that correspond to their PIN instead of their actual PIN numbers.

For example consider an actual PIN number of 12345. To authenticate the user would be presented with a screen such as

PIN 0 1 2 3 4 5 6 7 8 9

num 3 2 3 1 1 3 2 2 1 3

The user would enter 23113 instead of 12345.This doesn’t divulge the password even if an attacker intercepts the entre because 23113 could correspond to other PIN numbers such as 69440 or 70439. The next time the user logs in, a different sequence of random numbers would be generated such as:

PIN 0 1 2 3 4 5 6 7 8 9

num 1 1 2 3 1 2 2 3 3 3

Your program should simulate the authentication process. Store an actual PIN number in your program. The program should use an array to assign random numbers to the digits 0 to 9. Output the random digits to the screen, input the response from the user and output whether or not the user’s response correctly matches the PIN number.