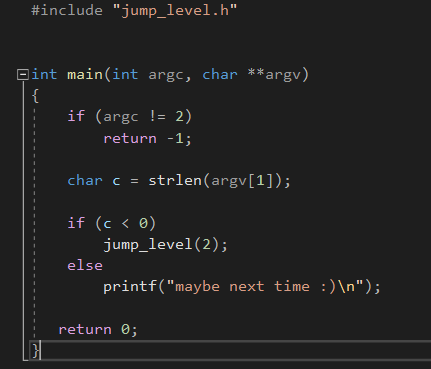
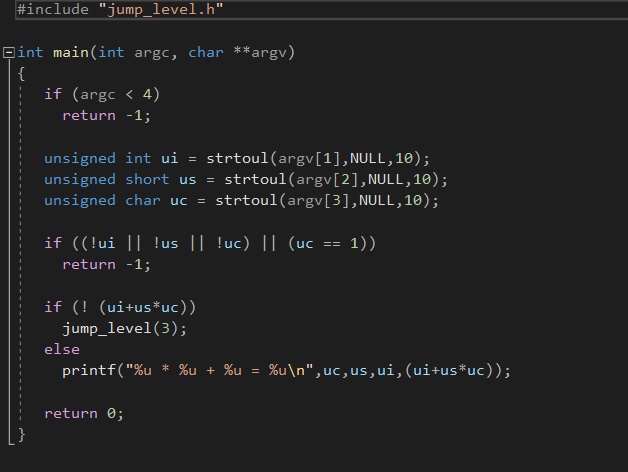
*1*:

Зная ,что значения в массиве типа char находятся в диапазоне (-128 ; 127),мы можем передать количество символов, которые по длине будут больше 127еми.В следствии чего будет переполнение массива.



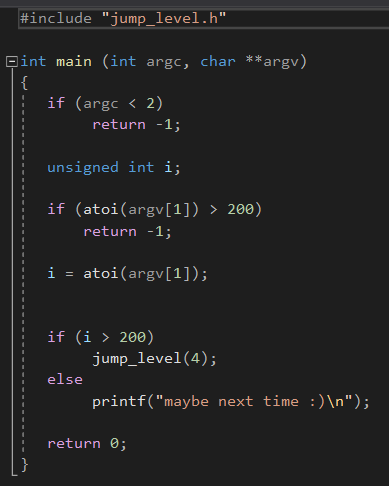
2:

Как известно, тип unsigned int имеет диапазон (0 ; 4294967295).Число 4294967295 можно представить в бинарном виде : 11111111111111111111111111111111.А число на единицу больше будет выглядеть следующим образом 100000000000000000000000000000000 .Это переполнение типа unsigned int приведет к тому ,что в скобках (ui+us\*uc) будет 0.А для этого нужно передать 4294967292 2 2.



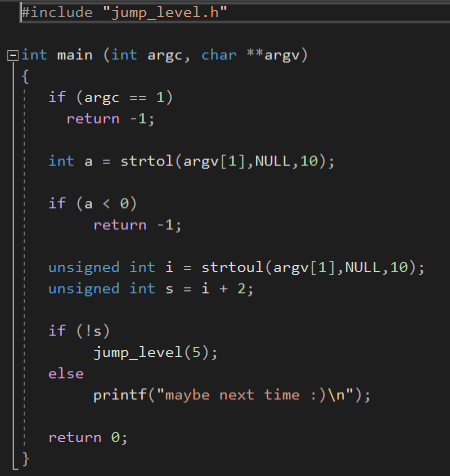
3:

Если мы передадим значение -1,то учитывая что переменная имеет тип unsigned int, это приведет к тому, что число оно перейдет к максимальному значению unsigned int,которое однозначно больше чем 200



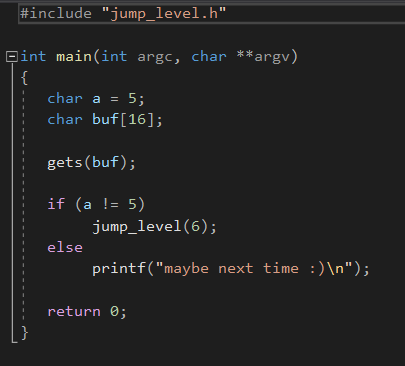
*4*:

По аналогии с предыдущими случаями нам нужно переполнить тип unsigned int на единицу ,т.е. 4294967296.А так как мы к переменной прибавляем 2,то нам нужно передать число 4294967296-2=4294967294.



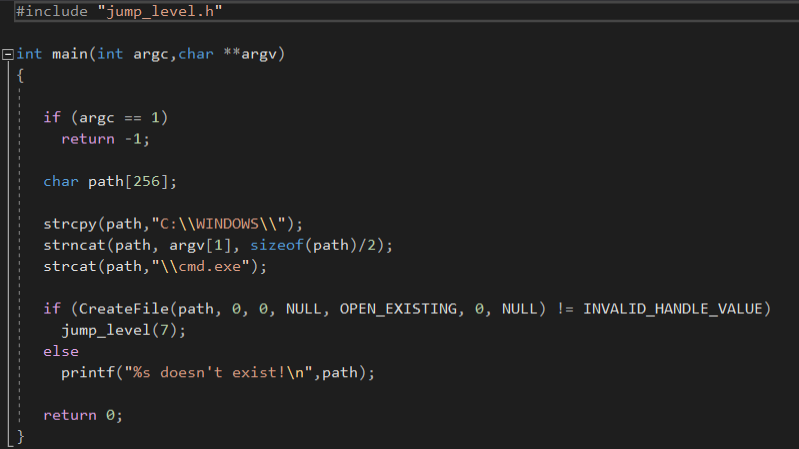
*5*:

Если передать строку длиной 16 и более символов,то buf переполнится ,а в элемент (а) запишется один из элементов ,не вместившихся в buf изменив переменную a.



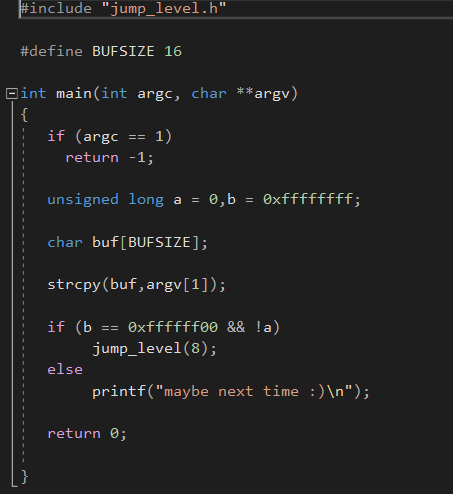
*6*:

Вводим System32 - название папки, т.к. именно в этой папке лежит cmd.exe.



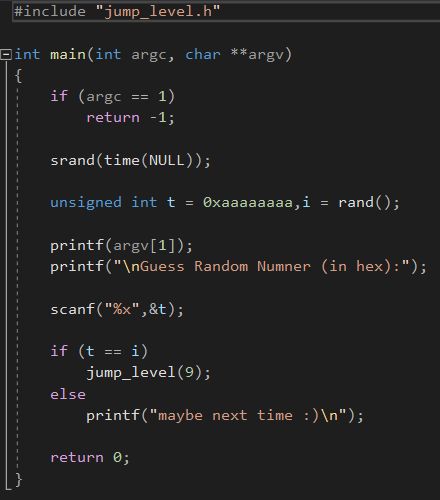
*7*:

Вводим 16 символов ,следовательно знак конца строки '\0' запишется в младший байт b, а сама переменная (a) при этом не изменится



*8*:

Передадим недостающие аргументы в строку формата ,для хранящиеся в стеке, так доходя до i, мы встретим t = 0xaaaaaaaa.Следующая строка является подходящей: "%x %x %x %x %x %x %x %x %x %x %x %x %x %x %x %x %x %x %x %x".



*9*:

Зная что элементы в стек добавляются с конца(сначала пароль, затем логин),при передаче логина и пароля в функцию check\_user пароль будет длиной 32 символа, , то локальная переменная для функции check\_user пароль будет содержать ещё и символы из логина до символа конца строки “ \0”. В логин будет передаваться строка длины( ключ = + пароль+логин).Как следствие идет переполнение key[] и невошедшие символы перейдут в стек до i. Подходящий логин - длина 5.



*10*:

Необходим argv[0] длиной ,превосходящей (BUFSIZE - 1),в таком случае остановка цикла произойдет при i= BUFSIZE. Следовательно при buf[BUFSIZE] = 0 произойдет запись в переменную i.

