CS 255 Computer Security
Tanish Arora

1. IOLI -Crackme Passwords

a) **Crackme 0x00:** 250382
b) **Crackme 0x01:** 5274
c) **Crackme 0x02:** 338724
d) **Crackme 0x03:** 338724
e) **Crackme 0x04:** 5555/28678
f) **Crackme 0x05:** 88
g) **Crackme 0x06:** First three letters should be “LOL” with “LOLO” = 6262

2. Bomblab :

a) What is your mother’s maiden name? //written in comments when did gdb
b) Paper (tricky one) : Looking at phase_funcall, the return function helped derive “paper”
c) P@s$wOrd : looking at string_length and the hint we know its password, this took a long time for me to derive, but looking at the register values it helped me the nature of the password
d) Next is also tricky but after a careful look at the sym.phase_quick, I came to a conclusion that in order to defuse this phase, we take an arbitrary int value for x : The solution for this phase then comes : x x+1 x+3 x+6 x+10 x+15
e) Looking onto the phase _jump: After looking at gdb, I see need to enter into eax arguments 0-7 for making a jump on its value. After inputting 0 I get 603, then I tried a random value 6, I got 326 . Hence the solution : 0 603 / 6 326.
My Output :

```
taror002@bolt $ ./bomb

          ,--.!,   ____                  _      _        _
       __/   -*-  | __ )  ___  _ __ ___ | |__  | |  __ _| |__
     ,d08b.  '|`  |  _ \ / _ \| '_ ` _ \| '_ \| |/ _` | '_ \
    0088MM        | |_) | (_) | | | | | | |_) | | (_| | |_) |
     `9MMP'       |____/ \___/|_| |_| |_|_.__/|_|\__,_|_.__/
           cs165

Welcome to my fiendish little bomb. You have N? phases with
which to blow yourself up. See you alive!
(hint: security question)
> What is your mother's maiden name?
Phase 1 defused. How about the next one?
(hint: rock? paper? scissors?)
> paper
Got it. Here is the next phase!
(hint: password)
> P@s$w0rd
Yes, don't trust anyone. Let's move.
(hint: quick)
> 2 3 5 8 12 17
That's number 3. Keep going!
(hint: jump)
> 6 326
Congratulations!
~/CS255/Computer-Security/bomblab
taror002@bolt $
```