Crackmes: Beginner Crackme

The following writeup is for <u>beginner crackme</u> on crackmes, it involves reverse engineering a binary to find the password.

Let's start by loading the binary into IDA and open the main function:

```
push    offset aNick    ; "Nick"
lea     ecx, [ebp+var_30]
call    sub_41106E
mov     [ebp+var_4], 0
push    offset a4ace00f ; "4ACE00F"
```

These strings immediately stand out and if we try this as a username:password pair we successfully login: