Assignment 2 - Cryptography, buffer overflow, reverse engineering
There is an associated zip file for this assignment. The binary files are compiled on the Kali Linux system you have been provided. We only guarantee support for the provided servers. (if you have an x86 machine, you should be able to run them locally on a Linux/Unix terminal)

Question a - Symmetric encryption decryption [45%]
We have a message encrypted via the protocol specified in **sym.c**. However, we lost the encryption key to decrypt the message. Can you figure out what the lost message is? The encrypted message is included in the zip file as **sym.txt**.

Question b - Reverse Engineering [35%]
There is a hidden flag inside the program **vuln**, but we can't figure out how to get to it! Can you reverse engineer the program to figure out what the flag is, then can you get the program to print the flag?
Note: The flag will follow the format: flag{some_text}

Question c - Buffer Overflow attack and reverse engineering [20%]
In your zip file, you will find a binary file named **bufover**. You must use a buffer overflow attack to successfully retrieve the flag.
The output will display **Correct password! Here is the flag: {}** if successful. Else, it will display **Incorrect password!**
Hint: the program has a hardcoded password where it's being used to compare against the password you enter. Can you overwrite the hardcoded password?

Question d - Extra credit [5%]
There is a much easier way to obtain the flag in the binary file **bufover** than executing a buffer overflow attack. What's the default password hardcoded into the binary? Remember to show your steps (evidence!) in your report.