You are the lead programmer in a software house specializing in providing solutions for companies looking to build security systems. You get a new client on 1st March that hires you to make a login system for its employees.

12th March. The client asks you to build a security system that requires a password for login. The security system should allow the user to input a password, and if the password is "login123!\" then the system should display a message saying login successful, otherwise the system should point out that the login attempt was unsuccessful.

23rd March. After a brief internal trial, the company realizes that its security system is too weak. They want you to up their security by using two-factor authentication. Under the new security protocol, employees are required to input both their password and their phone number that is in their HR records. Under the new security protocol, the system should allow a user access only if they enter a password "login123!\" and their phone number 99452651.

30th March. A disgruntled employee in the company bribes you to put in a backdoor into the security system. If someone enters password "backdoorLogin", regardless of the phone number, the system should display a message that the user has hacked into the system backdoor.

1st April. The company further realizes that hackers are trying to use a brute force attack to gain access to their system. They ask you to limit users to have at most 3 login attempts. After 3 login attempts, the system should display a message saying that the system is locked and they should contact the system administrator.