COMP3334 Lab2

JAHJA Darwin, 16094501d

Task 2

To prevent online dictionary attack:

1. We can prompt users CAPTCHA after he/she failed five login attempts, or we can prompt users CAPTCHA each time when he/she logs in. This prevents attackers using bots to do such kind of brute force attacks.
2. Another way is to incrementally increase the response time each time when a user failed the login attempt. This effect is bind with the client's IP address. The aim is to decrease the effect of a possible brute force attack.

Task 3

The above authentication protocol is not able to identify Bob (the server). As Alice is using a public key to request authentication, if there is a middle man (attacker) between Alice and Bob, the middle man can also use that public key to generate $PKE(R)$ and send it back to Alice. In this situation, Alice may not be able to identify whether the response is from Bob or from the middle man. Therefore, this protocol cannot identify Bob.