CS4600 Homework 4

1. Since Eve has edit access to Alice’s and Bob’s public keys on the server, Eve can replace Alice’s and Bob’s public key with Eve’s own public key. That way when Bob and Alice encrypt messages, they will use Eve’s public key which Eve can decrypt with her private key. That means Eve can read encrypted messages and forge messages from either party.

Alice and Bob can detect Eve’s subversion of public keys when they can’t decrypt the messages sent to each other because the public key encryption uses Eve’s public key to encrypt.