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.

1. Variation 1 is not secured because the message is not encrypted. Signature is not encryption and is only used for verifying if information was changed. The message can be recovered based on only the signature alone, potentially leaking important information.

For variation 2, it’s very secure because both the signature and the message is encrypted and it will be hard to modify the content, bolstering the integrity of the message. However, more calculation is needed to first, decrypt both the signature and the message, then verify. Hackers will only have access to the encrypted concatenation and less information is available, posing less risk. Also, variation 2 guarantees that the content of decrypted message is correct.

For variation 3, it’s secured because the message is encrypted, and the signature verifies the encrypted message, bolstering the confidentiality of the data. Variation 3 is more efficient because the receiver only needs to verify the signature and decrypt the message. However, hackers will have access to the encrypted message and the signature of the encrypted message itself, potentially riskier. For variation 3, the receiver could accidentally use the wrong key. That means signature authenticate correct encryption, but user use the wrong key to decrypt, getting garbled information and using it.

1. For variation 1, there are two cases. Case one is when Bob keeps a record of the nonces and we assume that session keys are not reusable. Eve would try a replay attack; record the third step, send it to Bob, posing as Alice. Since the session key can’t be reused, Bob would know this is a replay attack and Eve is unsuccessful. This implementation would be secure.

Case two is when Bob doesn’t keep a record of the nonces. Eve will record the third step, posing as Alice, and send it to Bob. Since Bob can’t verify if the message is from Alice or not, Eve would be successful. This protocol isn’t secure.

For variation 2, Eve will try a replay attack by recording the third step, send it to Bob, posing as Alice. However, Bob will send a message back and verify if the person is Alice or not by encrypting the nonce with the session key. Eve would have no way to prove to Bob that she is Alice unless by breaking the encryption, practically impossible, to send a verifying message by adding 1 to the nonce. Eve will be unsuccessful, and this protocol is secure.