COMP3632 Assignment 2: Written Portion

Sim, Kyu Doun

20306527

1. Alice and Bob

(a)

Alice 128 bit secret key: secret key should be long lasting, encryption, it shouldn’t use to authenticate, Alice should be the only one who knows the secret key

The HMAC is redundant. The Hash- MAC cannot be used to authenticate this message to prove that it is Alice.

(b) Bob should ask a CA to sign his public 256-bit RSA key using CA’s private signature key, not the 256bit ECC key. The ECC key is a PKE and is only used for encryption. A public verification key should only sign private signature key.

(c)

(d) A password should never be encrypted, but rather be hashed and stored.

2.

3.

4. Superfish

1. Planted malware and Spyware or keylogger
2. Superfish can change the content because

Create its own certificate, which is fake,

Computer -> Public Key -> Browser

Create own CA, this is trust worthy, encrypt everything using the CA

Superfish decrypt, gains info and encrypts it again

1. Asdf
2. Users could check

Steal the signing key authenticate what ever they want

