Applied Cryptography – CS483

Michael Kang, Noah Branch

12/2/2019

2. ME = MA

SE = SignE(MA)

5. EncA(X)

Eve



4. EncE(X)

3. Verify SignE

1. MA = (Time Stamp, Session ID, B, EncB(X)

SA = SignA(MA)

Alice

Bob

After this process Eve and Bob will know X and since Alice is only expecting a encryption with X, Eve can just encrypt the X bob sent back and it be valid.

1. Eve and Edward can interact with Alice and bob to essentially use their shared key. After watching Alice and Bob, Eve can interact with Alice and Edward can interact with bob. Afterwards Eve and Edward interact to recover the shared key of Alice and Bob.

Eve now has Alice’s Ra

1. R­­­aemodN
2. R­­­a xor Rev
3. R­­­a xor Rev
4. R­­­evemodN

Eve

Steve

Alice

Ed now has Rb

1. R­­­bemodN
2. R­­­b xor Red
3. R­­­b xor Rev
4. R­­­edemodN

Ed

Steve

Bob

Now Ed and Eve can repeat the same protocol with each other but instead of using their shared key they can use Alice and bobs. That way the server sends Alice and Bobs shared key xored together . Edward and eve now have both Alice and Bobs Shared key.

1. R­­­aemodN
2. R­­­a xor Rb
3. R­­­a xor Rb
4. R­­­bemodN

Eve

Steve

Ed