COMP4334 Homework 2

Q1.(1)

SSL record protocol provides confidentiality and message integrity.

Confidentiality use AES encryption to encrypt the data that transferred after a secure connection is established, to make sure the hacker or somebody cannot read the communication content.

Message Integrity use the HMAC to make sure the content in the internet communication is not changed by somebody.

Q1.(2)

SSH is make a secure connection between two systems, which often need the server and client to verify or authrize the both sides, can be use the public key authentication.

SSL is make a secure connection between broswer and server, which often only the server is authenticated.

Q1.(3)

- Establishing a secure connection and share secrets
- Authenticating the server and maybe client

Q2.(1)

Because if A and receiver use same key, the receiver can use this key to make the fake message and say it is A's message, which is not good for identify the message is from who.

Q2.(2)

When every party have the unique set of keys, also each receiver have different set of keys, so the receiver cannot make the fake message and give to another receiver.

Q2.(3)

n = 10, p = 5

S1 = { k1, k2 }

S2 = { k1, k3 }

S3 = { k1, k4 }

S4 = { k1, k5 }

S5 = { k2, k3 }

S6 = { k2, k4 }

S7 = { k2, k5 }

S8 = { k3, k4 }

S9 = { k3, k5 }

S10 = { k4, k5 }

Q3.(1)

Yes, Eve can forge, if without hashing, the textbook RSA signatures easy to be attack. Because of the any of the textbook signatures can use `m = σ^e mod n` to compute. So the Eve can give the message and generate the sign without the key.

Q3.(2)

The hashing can add the security, because hashing the message before generate the signature, which can produce the "almost" unique and fixed size string, to make sure the Eve difficult to compute the message, and find another signature.

Q4

The digital signatures are establishes the trust between the both parties which map the identity and public key together. The users can use CA to verify the digital signatures is real and secure. Which are Authentication and Integrity.

The CA digitally signs each certificate it issues using its private key, ensuring the certificate's authenticity. When another user verifies the signature using the CA's public key, they confirm that the certificate has not been tampered with and was indeed issued by the CA.

Q5.

A ------ encrypt message (with N_1 & ID_A) ------> B

A <------ encrypt message (with N_1 & N_2) ------ B

A ------ encrypt message (with N_2) ------> B

A ------ encrypt message (with signature [E(PRa, Ks)]) ------> B

(1)

In step 2, B send the encrypted message with N_1 and N_2 to A, after the A decrypted the message, can verify the decrypted N_1 and the N_1 sent to B in the step 1 is correct or not.

(2)

In the step 3, the A sent the encrypted message with N_2 to B, after B decrypted the message, B can make sure the decrypted one compare to the nonce 2 is correct or not. Which can verify the from A or is A receive the correct nonce.

(3)

In the step 4, the A sent the encrypted message with another encrypted message (for this one, because encrypted by private key, which is same as generate signature, which means the encyption is encrypt the signature), so when B decrypted the message, B can use A's public key to verify the message is from A or not.