Quiz 4 [CS5700 Fall 2019]

Name: Yuanjie Yue Score: _____

[Q1] Answer the following questions

- [10 pts] What's the main difference between symmetric key encryption algorithms and asymmetric key encryption algorithms?

In symmetric key encryption, sender and receiver share the same single key to encrypt and decrypt. However, for asymmetric encryption, the key used for encryption and decryption is different, sender encrypts message with receiver's public key and receiver decrypt this message with his own private key.

- [15 pts] Give two examples of symmetric key encryption algorithms, and one example for asymmetric key encryption algorithm.

Symmetric key encryption: DES and AES
Asymmetric key encryption: RSA

- [10 pts] In general, is symmetric key encryption algorithms more computationally expensive compared with asymmetric key encryption algorithms?

No, it is not. The compute work in symmetric key encryption are mostly substitution and shift, while in asymmetric key encryption, it is need to generate some big prime number.

[Q2] Answer the following questions

- [10 pts] Cryptographic hash functions map text of arbitrary length to a fixed length message digest. Please give at least two examples of commonly used cryptographic hash functions.

MD5
SHA-1

- [30 pts] How do you combine asymmetric key algorithms with cryptographic hash functions, and design digital signatures?

Before sending message, the sender could use the hash function to generate digest of the message and encrypt it with his private key, making it into a digital signature. Then he could send this digital signature along with his message which is encrypted by the receiver's public key.
When receiving the message, the receiver could first decrypt the message with his own private key, and then decrypt the digital signature with the sender's public and get the digest of the message. Next, the receiver could apply the same hash function that the sender use to get the digest of the message he got and compares it with the digest that is decrypted, if the two versions of digest are the same, that means the message is truly from the sender and the content has not been changed along the way.

[Q3] Answer the following questions

- [25 pts] In you own words, what are certificates? What's their purpose?

The certificates are issued by the Certificate Authority, it is got by encrypting one's public with the CA's private key. We are doing this because there is a problem with the digital signature, that one may have the wrong public key of the other side, thus he might be deceived by some malicious party in the communication. To make sure one could get the real the other side's public key, either side should go to CA to get a certificate of their public key, thus they could send this certificate along with their encrypted message and digital signature. In this case, after one got the message, he could first decrypt the certificate with CA's public key and get message sender's public key, with which he could decrypt the digital signature, he could verify the sender's authentication.