Homework 4

Pan Yisheng
515021910384

April 8, 2018

Problem 1. a) Why can a public key not just be transmitted through email or be posted on a website?

b) A certificate does not necessarily have to be signed directly by a CA, there is something called a certificate chain. Can you imagine what a certificate chain is?

c) Who signs the certificate of a CA?

Solution Part a): If a public key is transmitted through email or posted on a website, we can't verify the source's identity because someone else can declare himself as others like some famous website.

b): The certificate chain, also known as the certification path, is a list of certificates used to authenticate an entity. The chain, or path, begins with the certificate of that entity, and each certificate in the chain is signed by the entity identified by the next certificate in the chain. The chain terminates with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in the chain must be verified until the root CA certificate is reached.

If we define $Y << X >>$ means the certificate of user X is signed by Y. Then we can illustrate a certificate chain as $X_1 << X_2 >> X_2 << X_3 >> ...X_N << B >>$ where $CA(X_i, X_{i+1})$ should sign for each other.

c): If a CA is a root CA, it signs itself. If a CA is an intermediate CA, its parent CA signs it.