CS381 Exercise 12

Name: Zhang Yupeng

Student ID: 5130309468

1. Alice and you work together in SJTU. Both of you have public-key certificates issued by CA of SJTU, CA_{SJTU} ‘s certificate is issued by a root-CA imbedded in browser. Therefore Alice and you trust each other’s key.

a) After 1 year, the root-CA says that CA_{SJTU} ‘s certificate has expired (so that your browser says Alice’s key is not valid), but CA_{SJTU} tells you directly that Alice’s key is still secure. Question: can you trust Alice’s key or not, and why?

Solution:

We cannot trust Alice's key because that CA_{SJTU}'s ceritficate has expired, therfore it may be compromised. So if the secret key of CA_{SJTU} is leaked, anyone can generated a valid certificate of Alice and communication with others in Alice's identification, so Alice cannot be trusted.

b)If CA_{SJTU} says Alice’s certificate has expired, but Alice tells you on the phone that her key is still secure. Can you trust Alice’s key or not, and why?

Solution:

We cannot trust Alice's key because even Alice tells you on the phone that her key is still secure, since her certificate has expired, her secret key may be leaked, so Alice cannot be trusted.