CS526 Report - Zhuosheng Jiang

In this project, I firstly write some debug functions such as hex to string and string to hex .etc. This will help to find problems easier. Then I use c++ string in the most time of the project, because it can perfectly deal with null terminator in the middle of string, and I also build mutiple functions that contains RSA or Hash functions, in which way this made me easily to implement the protocol. There are several problems I have encountered in this project. As I written before, as results of hash or encryption, there will be weird bytes such as null terminator occurred anywhere in strings. The second problem is that in what format I choose to save log, because of debugging process I chose Hex to store all informations, which means there are lots of bytes to hex and hex to bytes operation inside my program and this really increased difficulty to implement this program. The last problem is about RSA encryption and signature, after I debugged for half an hour I just realized that RSA can only do its magic when plain texts are within certain length, which means I need to apply hash function on plain texts that are needed to be signed. I choose SHA256, AES 256 and RSA in my project. The reason of choosing SHA256 as my my hash function is because it is not only one of the most secure hash functions but also very easy to implement. After searching about how key size matters in AES, I found that keys of 256 bits are sufficient enough and another reason is that SHA256 will return a key that is exactly 256 bits. This make me easy to implement the whole program. RSA is necessary to transit keys and verification between T and U. There are many things we I learnt from this project is that it is better to design whole program at the beginning. Because that I didn't designed this whole program very well, so that many functions or struct are very mess. It is quite hard to reform these codes, but fortunately I think I have build a pretty well debug struct that make me easy to find bugs.