Lab2 Report

2021/07/14

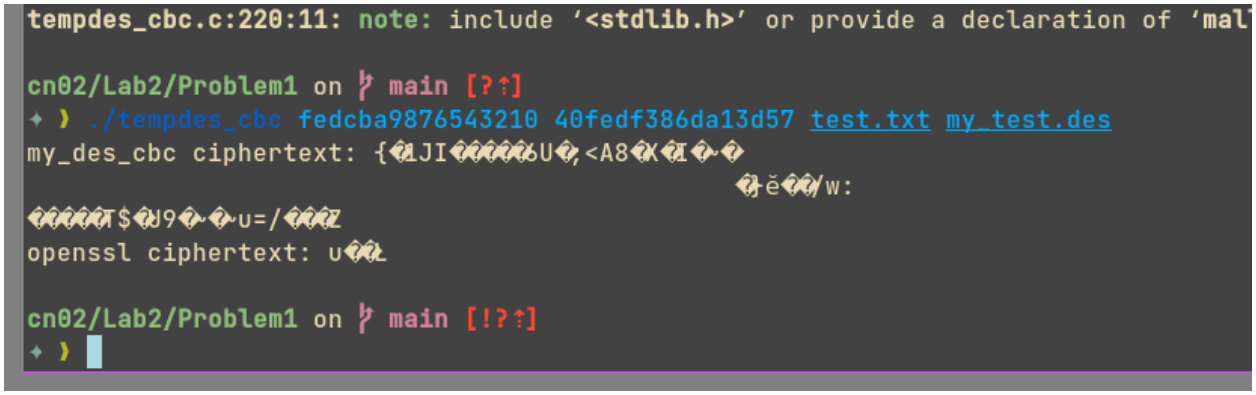
S1270174 Ryoma Okuda

(problem 1)

Initially i executed one command:

`./tempdes_cbc fedcba9876543210 40fedf386da13d57 test.txt my_test.des`

Result is this:



Test.des

§æ—ç‡4›XmÓ,gÎ0∞‘ï>ÉµÍRÎ≤#ûUhÖ´∑ÉÖ°õÿGÔ›ÂÏQ„bé…¸„,?ö
-q∫pF

My+test.des

§æ—ç‡4›XmÓ,gÎ0∞‘ï>ÉµÍRÎ≤#ûUhÖ´∑ÉÖ°õÿGÔ›ÂÏQ„bé…¸„,?ö
-q∫pF

(problem 2)
(1)Though I tried my best, all the codes execute error SIGABRT (Abort) so that I could not prove the running correctly. But I will put all the codes.
(2)
As I could not prove the result, below consumptions are all basically what I learned from the internet, not my result.

(e) DES depends on the number of the bytes of data for faster encryption which means that RSA decryption is faster than encrypt.

(f) SHA1 can only encrypt but DES can both encrypt and decrypt which means that DES has its own symbols but SHA1 doesn't.

(g) RSA is pretty stable which means that decryption time and encryption time is nearly the same because they are just doing the same thing. Also big number of the bytes of data will be longer time to decrypt and encrypt.