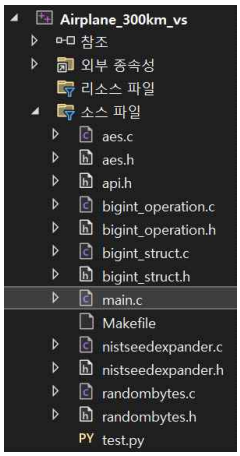
라이브러리 사용 설명서

Team. Airplane

Ⅰ. 동적 빅넘버 연산 라이브러리



1. 윈도우

   "big_number_window" 파일 속 코드를 프로젝트를 생성하여 visual studio에서 작동시킨다.

2. 리눅스

   "big_number_linux" 파일로 이동한다.

   Makefile의 구성 및 수행 절차

   - make all
   - .\test

makefile은 각 헤더를 모아놓은 include 파일과 각 c 파일들로 구성이 되어 있으며 obj 파일로는 test 파일을 생성한다. 따라서 위의 수행 절차를 따르면 쉽게 컴파일 가능하다. gcc 혹은 g++로 컴파일을 필요할 경우 makefile 내부에 주석 처리되어있는 부분을 해제하여 해당 컴파일로 바꿀 수 있다.

```
sj@ubuntu:~/Downloads/js_test$ make all
gcc     -g -I./include ./bigint_operation.c ./nistseedexpander.c ./aes.c ./bigint_struct.c ./randombytes.c main.c -o test
sj@ubuntu:~/Downloads/js_test$ ./test
```

Ⅱ. ECDH

"ECDH" 파일의 코드를 활용한다.

- g++ .\ECC_two_struct.c .\bignum.c -o test
- .\test.exe

첫 번째 명령어를 사용하여 test 실행 파일을 만들고, 두 번째 명령어를 사용하여 실행시킨다.

```
PS C:\Users\coala_guest\Desktop\WI\Class\3-2\application\ECC> g++ .\ECC_two_struct.c .\bignum.c -o test
PS C:\Users\coala_guest\Desktop\WI\Class\3-2\application\ECC> .\test.exe
[Alice's secret key]
2d5244073e432d4a3a2b196ec95eba75aa6f0425c7806f678e3055b9899adee5
[Alice's public key]
d986de55e7fdf4dacdad6f9ea8d4e11bb3b54ef4d4ff3054992cf9fa6f374f1b
d50647e6606a1c526503fe593c542336e6d6accdd5f5091711e203d6f05288f7

[Bob's secret key]
08c82d6ad6e55cb6ad7b8572c071486d455fbf1ea7b2dcf49ef9fafd5fbde7a5
[Bob's public key]
8234ff7fa54856a5d9a14e028efb694693bd487c48bf37a6df501b28ead2f785
df6dae4b90c29fa19f3ec62ae4fa3eb3ce999f7d467144f278d6c904b6ef8abc

[Alice's shared key]
660a119feaae90989aebbc228c4f27e3ea7e85cbed760a1433a8628ceb90d586
a9bb5c9a57d7e80b8218c60b0853fd26123b96fa96baac9be513ec2b265b4872

[Bob's shared key]
660a119feaae90989aebbc228c4f27e3ea7e85cbed760a1433a8628ceb90d586
a9bb5c9a57d7e80b8218c60b0853fd26123b96fa96baac9be513ec2b265b4872
```