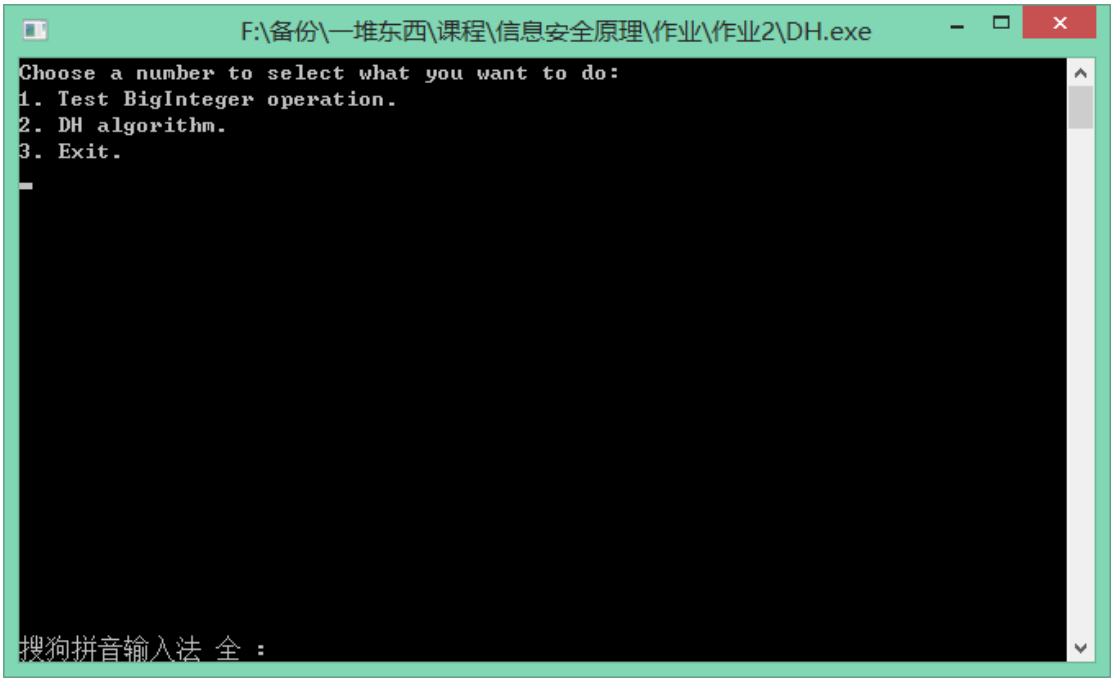
作业二

一、 作业说明

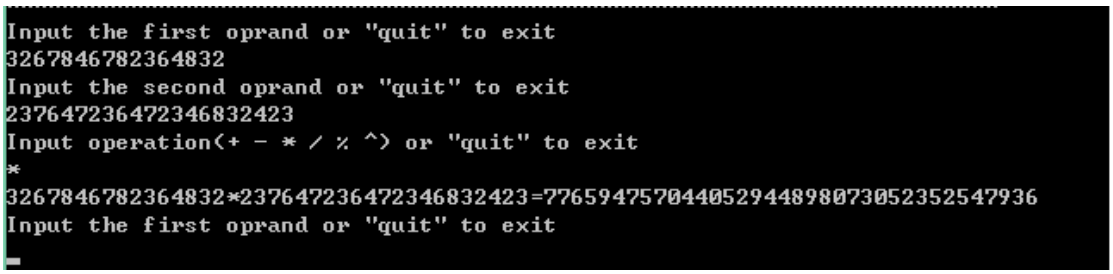
本次作业的源代码，包括头文件 BigInteger.h 和 cpp 文件，BigInteger.cpp 和 main.cpp 已经打包。
可执行文件 DH.exe 文件集成大数运算测试功能和 DH 算法。其中 DH 算法是基于大数运算的，因为取值需要很大。

二、 具体操作步骤

1. 运行程序，出现如下界面



2. 示，选择功能 1，进入大数运算的测试
3. 示，分别输入第一个和第二个运算操作数，再输入操作符，即可输出相应的算式和运算结果

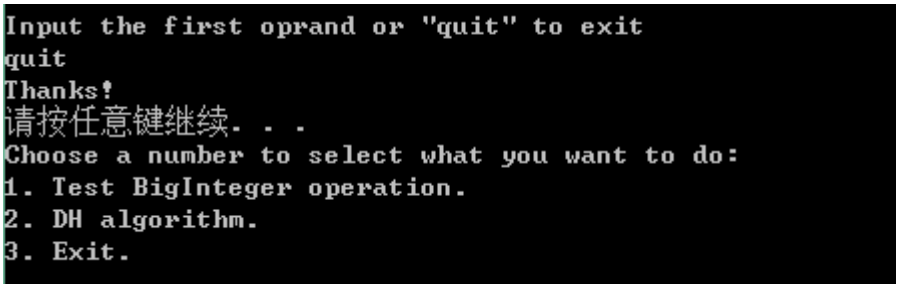


运算包括加（+），减（-），乘（*），除（/），求余（%），指数运算（^），上图为两个大

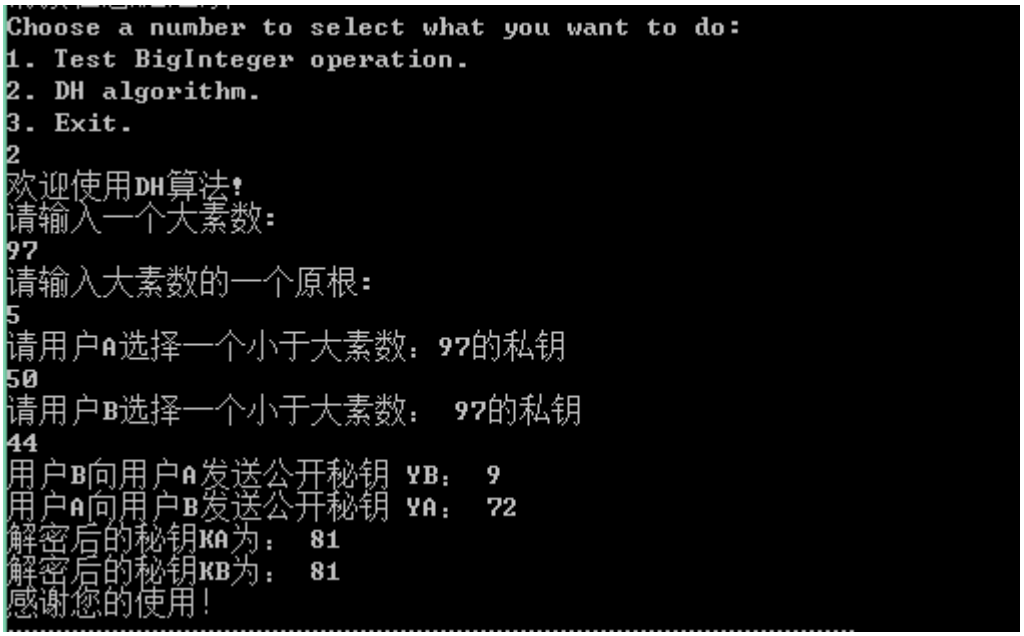
整数的乘法运算，可根据需要进行其他测试

需要注意的是，指数运算由于运算量很大，2^20000 大约需要 1 分多钟的时间才能得出运算结果，太大的数很可能长时间无法得到结果

4. quit”返回选择界面



5. 进入 DH 算法



按照提示输入一个大素数，一个原根，以及 A,B 各自选择的私钥，就可以输出相应的公钥信息，以及最后加密得到的秘钥。

即使输入的不是素数和原根也可以得到结果，只是不安全而已。