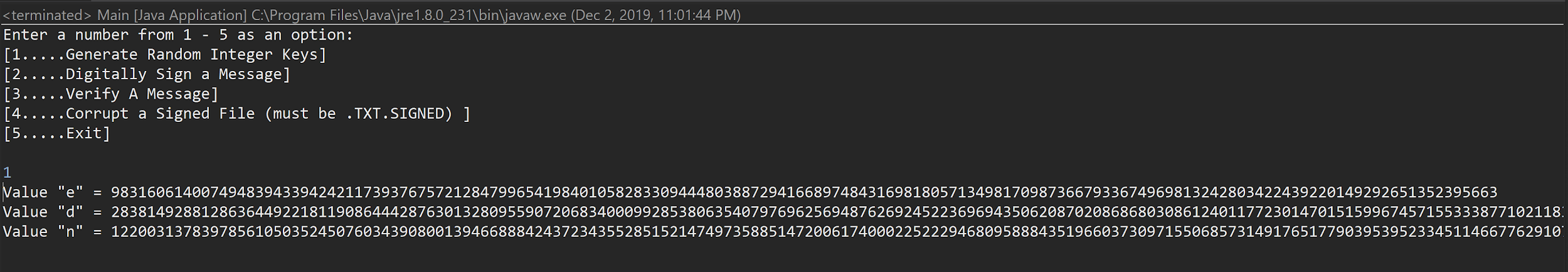
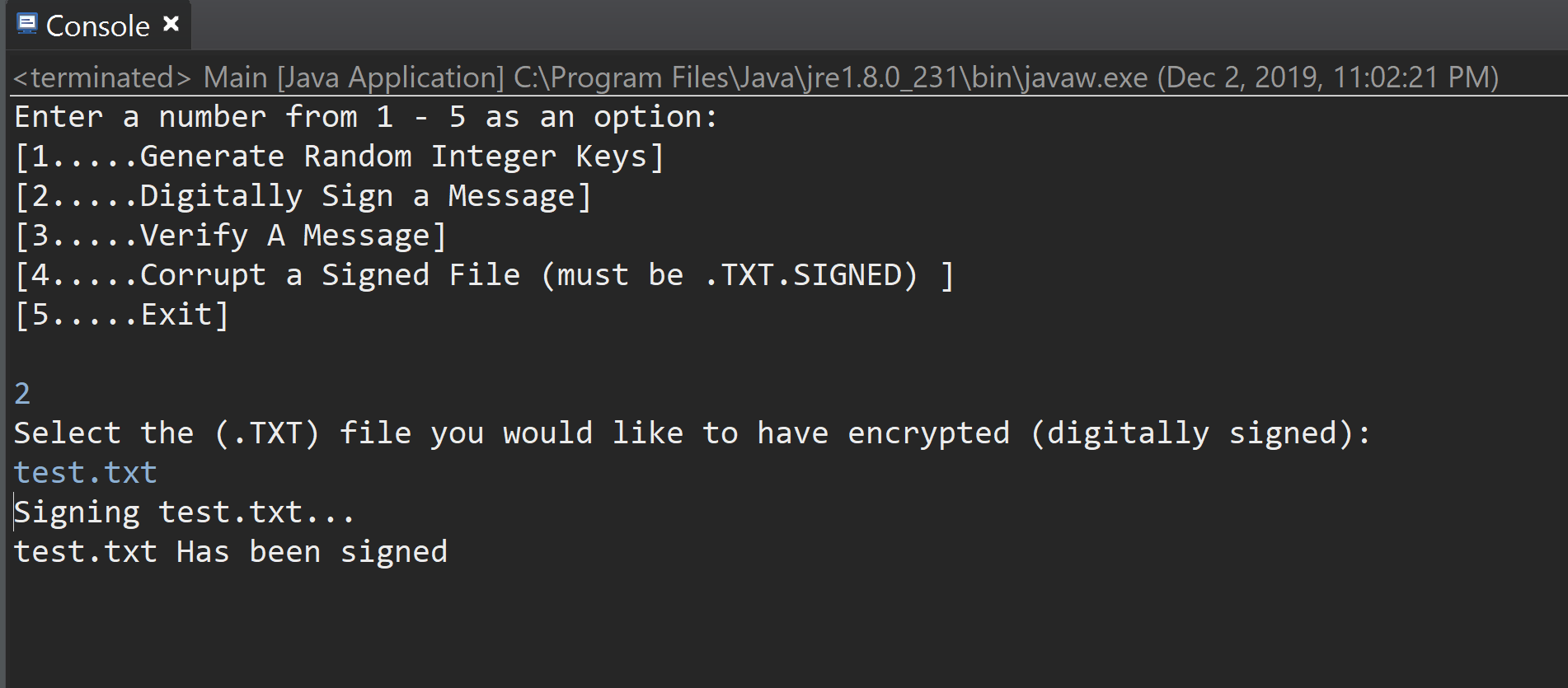
George Beltran, Albert Ramirez, Kayleen Ponce

Crypto: Project 2

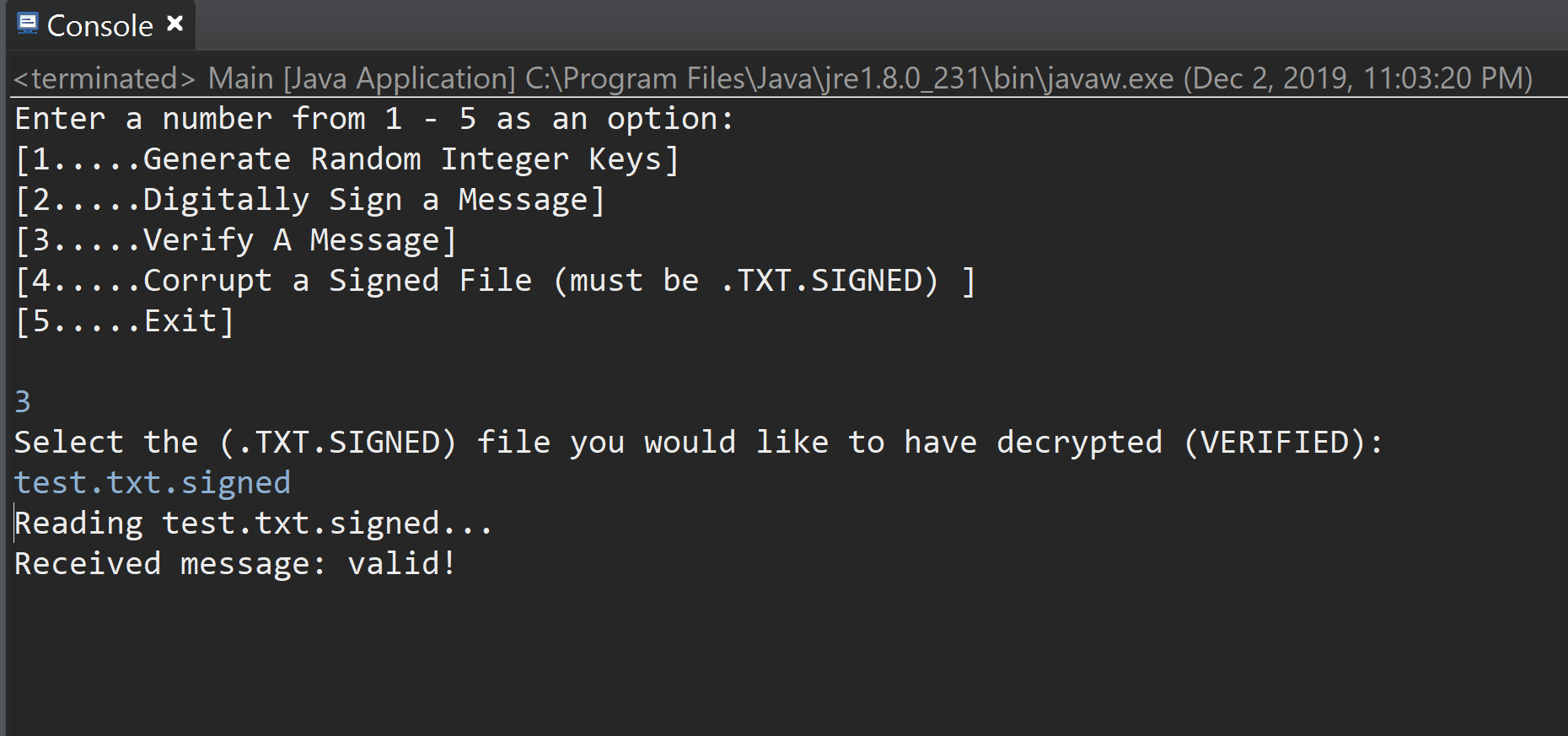
December 3, 2019



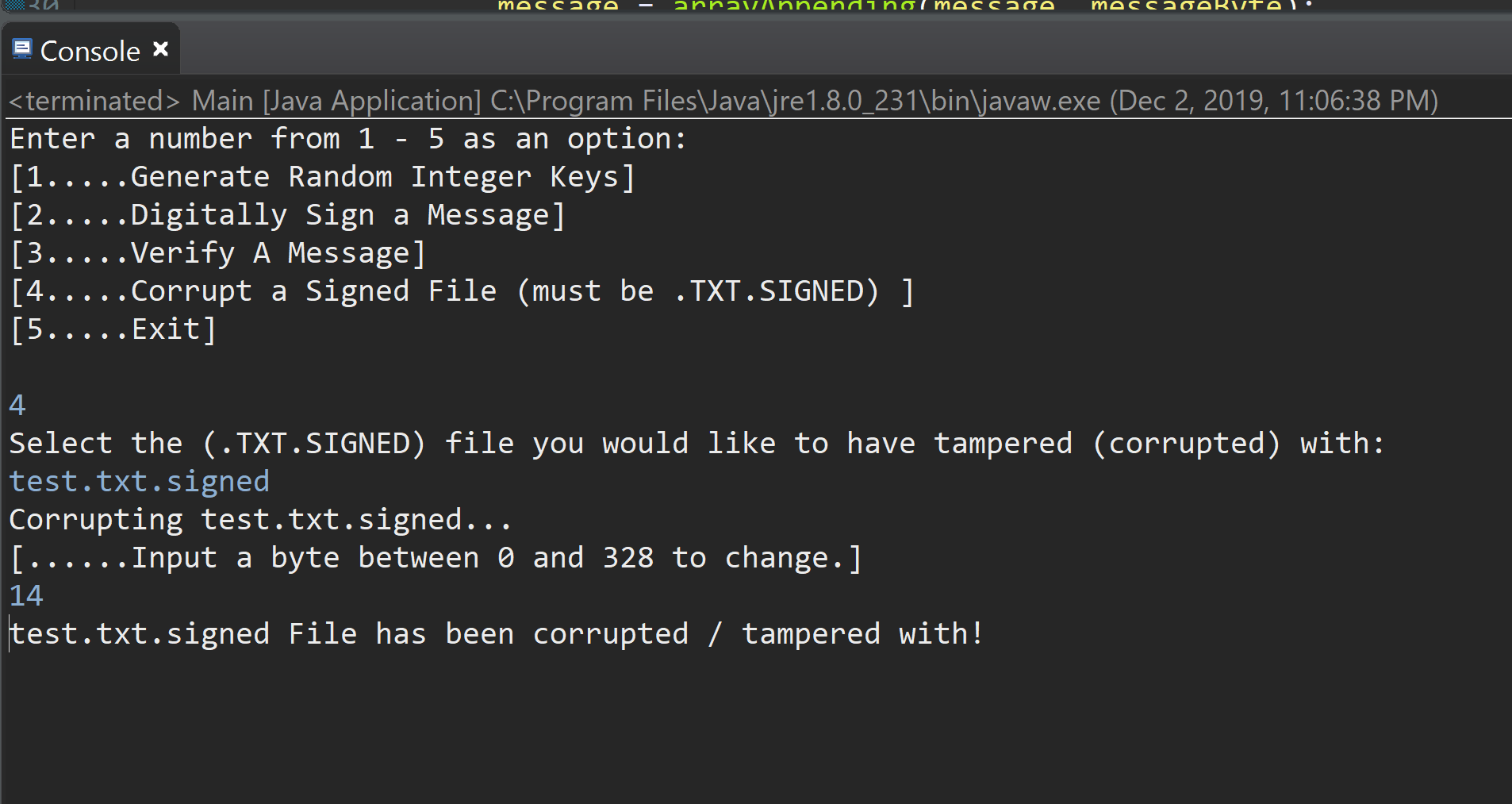
1. Key Generation Program



1. Send



1. Print out Signed File



1. Received
2. Tampered

This project was done in Java since our class is taught in Java. We all worked in a windows operating system and used the Eclipse IDE. In order to compile and run this project all four files are needed(KeyGen.java, DigitalSignature.java, ChangeByte.java, and Main.java).

The code of all files must be error free and once they’re all error free you run the Main.java file. A prompt asking you to choose from 1-5 will show up in the console. Depending on what option choose from 1-5 you will be asked to input a “.txt” file or a ”.txt.signed” file (the files must be saved in the file where your .java files are saved). To obtain the correct output, first, option 1 (Generate Random Integer Keys) must be selected. This option will output 2 files, “privkey.rsa” and “pubkey.rsa”, which should contain “e and n” and “d and n”, respectively. The random keys are then used for option 2 (Digitally Sign a Message), which will sign a .txt file of your choice, “test.txt”. This will then output a “test.txt.signed” file, which is what we will verify with option 3, “Verify A Message”. This will return that the message was valid. Next, the outputted message will be corrupted, “4. Corrupt a signed file”, and we will then verify it once more with option 3, which will this time yield an “invalid” signature.

Kayleen Ponce - 33%

Albert Ramirez - 33%

George Beltran - 33%