Jack Skrable 12-09-2019
CS789: Cryptography
Term Project

Code for all ciphers can be found at https://github.com/jskrable/cs789. Detailed instructions on executing the code and unit tests are in README.md.

Exchange Transcript (formatted for easy reading)
GREEN is the header showing which steps are happening
BLACK are the messages exchanged between the parties
RED is the code I used to generate my messages

Shrunkhala Nehete 5:49 PM
El Gamal Run #1
Alice: Shrunkhala
Bob: Jack
Alice's public key: (44999719, 2332263, 42094082)

Jack 5:50 PM
```
e = ciphers.ElGamal(10, 44999719, 2332263, 42094082)
e.encrypt(555555)
```
Bob's public key: (44999719, 2332263, 19698863)
Bob's ciphertext: 8739995

Shrunkhala Nehete 5:51 PM
Bob's plaintext: 555555

Jack 5:51 PM
That's correct.

Shrunkhala Nehete 5:51 PM
El Gamal Run #2
Alice: Jack
Bob: Shrunkhala

Jack 5:52 PM
```
e = ciphers.ElGamal()
print(e.mod, e.base, e.key_pub)
```
Alice's public key: (176763257633, 3, 75821444783)

Shrunkhala Nehete 5:52 PM
Bob's public key: (176763257633, 3, 161888414703)
Bob's ciphertext: 65550245186

Jack 5:52 PM
```
e.decrypt(161888414703, 65550245186)
```
Bob's plaintext: 77773333

Shrunkhala Nehete 5:53 PM
That's correct.
El Gamal Run #3
Alice, Bob: Shrunkhala
Eve: Jack
Alice's public key: (33539071, 8961536, 3207432)
Bob's public key: (33539071, 8961536, 8465981)
Bob's ciphertext: 15839948

Jack 5:55 PM
```
e = ciphers.ElGamal(15, 33539071, 8961536, 3207432)
e.crack(8465981, 15839948)
```
Bob's plaintext: 32117494

Shrunkhala Nehete 5:56 PM
That's correct.
El Gamal Run #4
Alice, Bob: Jack
Eve: Shrunkhala

Jack 6:11 PM
```
e = ciphers.ElGamal()
print(e.mod, e.base, e.key_pub)
key_B, ciphertext = e.encrypt(123456)
print(e.mod, e.base, e.key_B)
print(ciphertext)
```
Alice's public key: (264424247, 5, 147534506)
Bob's public key: (264424247, 5, 241314884,)
Bob's ciphertext: 17055128

Shrunkhala Nehete 6:12 PM
Bob's plaintext: 123456

Jack 6:12 PM
That's correct

Shrunkhala Nehete 6:12 PM
RSA Run #1
Alice: Shrunkhala
Bob: Jack
Alice's public key: (1734264907, 1497700811)

Jack 6:13 PM
```
r = ciphers.RSA(15, 1734264907, 1497700811)
r.encrypt(666444)
```
Bob's ciphertext: 1184449450 (edited)

Shrunkhala Nehete 6:15 PM

Bob's plaintext: 666444

Jack 6:15 PM
That's right

Shrunkhala Nehete 6:15 PM
RSA Run #2
Alice: Jack
Bob: Shrunkhala

Jack 6:16 PM
```
r = ciphers.RSA(8)
print(r.n, r,e)
```
Alice's public key: (8951908521509, 2153663)

Shrunkhala Nehete 6:16 PM
Bob's ciphertext: 2933623577466

Jack 6:16 PM
```
r.decrypt(2933623577466)
```
Bob's plaintext: 89898989

Shrunkhala Nehete 6:16 PM
That's correct.
RSA Run #3
Alice, Bob: Shrunkhala
Eve: Jack
Alice's public key: (537500521, 75993159)
Bob's ciphertext: 190307349

Jack 6:18 PM
```
r = ciphers.RSA(15, 537500521, 75993159)
r.crack(190307349)
```
Bob's plaintext: 45362718

Shrunkhala Nehete 6:18 PM
That's correct.
RSA Run #4
Alice, Bob: Jack
Eve: Shrunkhala

Jack 6:19 PM
```
r = ciphers.RSA(8)
print(r.n, r.e)
```
Alice's public key: (332629859, 26833)
Bob's ciphertext: 102767662

Shrunkhala Nehete 6:20 PM
Bob's plaintext: 333333

Jack 6:20 PM
That's correct.
Great!