REPORT: Paper Examples checked using programme

Example 1:

$$p = 5$$

$$q = 11$$

$$N = (p * q) = 55$$

$$phi = (p - 1) * (q - 1) = 40$$

Encryption key can be any number where:

$$1 < e < phi$$

$$coprime\ with\ N\ and\ phi$$

I will pick 7 since it applies to the rules above:

$$e = 7$$

Choose d to satisfy ed ≡ 1 (mod phi) or ed = 1 + k*phi where k is an integer:

$$d = 23$$

$$23 * 7 = 1 + (4 * 40)$$

Encryption lock = (7, 55)

Decryption lock = (23, 55)

Encrypt the number 12:

$$c = m^e (mod\ N)$$

$$12^7 (mod\ 55) = 23$$

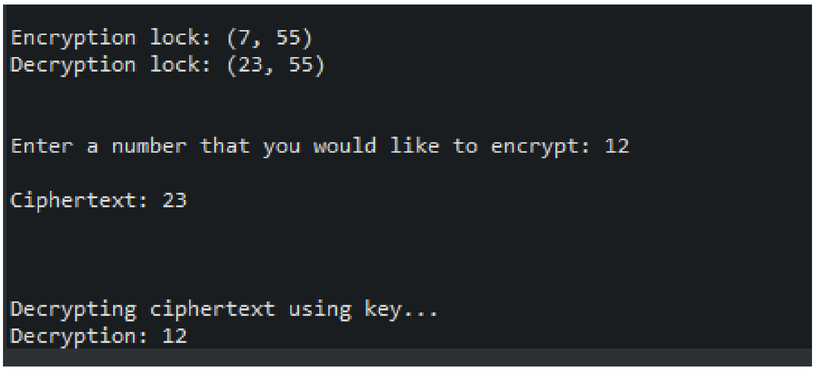
Ciphertext = 23

Decrypt the ciphertext:

$$23^{23} (mod\ 55) = 12$$

Decrypted plaintext = 12

Proof check using prototype program (PrototypeEncryption.java):



```
Encryption lock: (7, 55)
Decryption lock: (23, 55)


Enter a number that you would like to encrypt: 12

Ciphertext: 23



Decrypting ciphertext using key...
Decryption: 12
```

Example 2:

$$p = 11$$

$$q = 13$$

$$N = (p * q) = 143$$

$$phi = (p - 1) * (q - 1) = 120$$

Encryption key can be any number where:

$$1 < e < phi$$

$$coprime\ with\ N\ and\ phi$$

I will pick 7 since it applies to the rules above:

$$e = 43$$

Choose d to satisfy ed ≡ 1 (mod phi) or ed = 1 + k*phi where k is an integer that exists:

$$d = 67$$

$$43 * 67 = 1 + (24 * 120)$$

Encryption lock = (43, 143)

Decryption lock = (67, 143)

Encrypt the number 123:

$$c = m^{e}(mod\ N)$$

$$123^{43}(mod\ 143) = 85$$

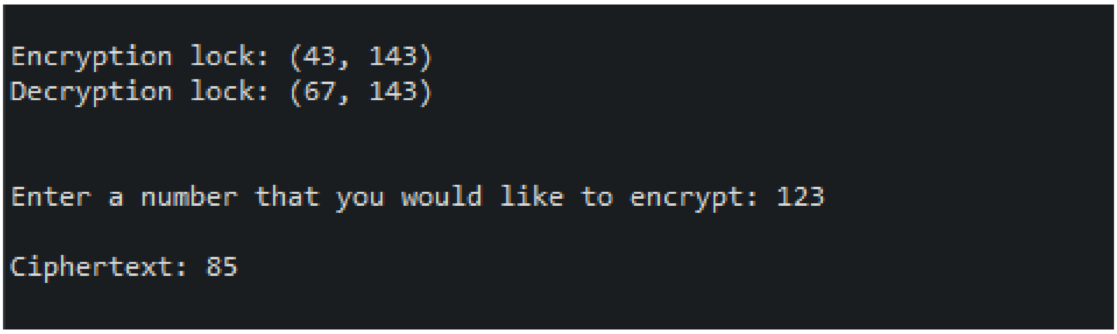
Ciphertext = 85

Decrypt the ciphertext:

$$85^{67}(mod\ 143) = 123$$

Decrypted plaintext = 123

Proof check using prototype program (PrototypeEncryption.java):



```
Encryption lock: (43, 143)
Decryption lock: (67, 143)


Enter a number that you would like to encrypt: 123

Ciphertext: 85
```

Example 3 with large primes:

$$p = 263$$

$$q = 383$$

$$N = (p * q) = 100729$$

$$phi = (p - 1) * (q - 1) = 100084$$

Encryption key can be any number where:

$$1 < e < phi$$

$$coprime\ with\ N\ and\ phi$$

I will pick 7 since it applies to the rules above:

$$e = 73147$$

Choose d to satisfy ed ≡ 1 (mod phi) or ed = 1 + k*phi where k is an integer that exists:

$$d = 65099 \quad k = 47578$$

$$\mathrm{ed} = 1 + \mathrm{k} * \mathrm{phi}$$

$$73147 * 65099 = 1 + (47578 * 100084)$$

Encryption lock = (73147, 100729)

Decryption lock = (65099, 100729)

Encrypt the number 23455:

$$c = m^{e} (mod\ N)$$

$$23455^{73147} (mod\ 100729) = 16205$$

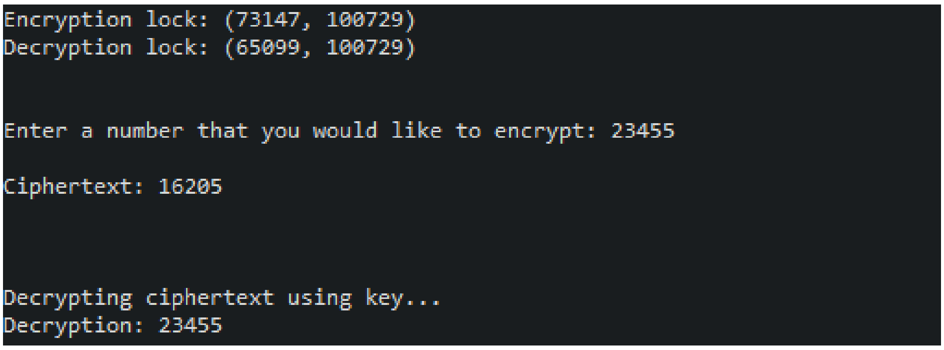
Ciphertext = 16205

Decrypt the ciphertext:

$$16205^{65099} (mod\ 100729) = 23455$$

Decrypted plaintext = 23455

Proof check using prototype program (PrototypeEncryption.java):



```
Encryption lock: (73147, 100729)
Decryption lock: (65099, 100729)


Enter a number that you would like to encrypt: 23455

Ciphertext: 16205



Decrypting ciphertext using key...
Decryption: 23455
```