Software Project

Nathan O’Connor

Discrete Mathematics

Software Development

Year 2

K00252751

**Questions posed within project proposal pdf are coloured red.**

**Sample data is coloured in black.**

# Program 1 – Prime Factorisation

**Testing**

|  |  |  |
| --- | --- | --- |
| **Input** | **Expected output** | **Actual output** |
| 30 | 2^1  3^1  5^1 | 2^1  3^1  5^1 |
| 31 | 31^1 | 31^1 |
| 487 | 487^1 | 487^1 |
| 8893 | 8893^1 | 8893^1 |
| 987654323 | 987654323^1 | 987654323^1  \*\* takes longer than 1 minute. |
| 131317171919 | 19^2  101^1  3601579^1 | 19^2  101^1  3601579^1 |
| 5018 | 2^1  13^1  193^1 | 2^1  13^1  193^1 |
| 1999 | 1999^1 | 1999^1 |
| 2000001 | 3^1  666667^1 | 3^1  666667^1 |
| 202025 | 5^2  8081^1 | 5^2  8081^1 |
| 6987 | 3^1  17^1  137^1 | 3^1  17^1  137^1 |
| 5463 | 3^2  607^1 | 3^2  607^1 |
| 2978 | 2^1  1489^1 | 2^1  1489^1 |
| 21765 | 3^1  5^1  1451^1 | 3^1  5^1  1451^1 |

# Program 2 – Extended Euclidean algorithm

**Testing**

|  |  |  |
| --- | --- | --- |
| **Input** | **Expected output** | **Actual output** |
| (8359, 4962) | [1, -1877, 3162] | d: 1  x: -1877  y: 3162 |
| (95243, 24138) | [1, 461, -1819] | d: 1  x: 461  y: -1819 |
| (4206969, 123456) | [3, -10213, 348025] | d: 3  x: -10213  y: 348025 |
| (66677788, 564738) | [2, -136705, 16140559] | d: 2  x: -136705  y: 16140559 |
| (28021999, 20012) | [1, -6509, 9114291] | d: 1  x: -6509  y: 9114291 |
| (1515663399, 2324245) | [1, -646111, 421335442] | d: 1  x: -646111  y: 421335442 |
| (242424777888, 816161616) | [144, 706312, -209796107] | d: 144  x: 706312  y: -209796107 |
| (148, 75) | [1, 37, -73] | d: 1  x: 37  y: -73 |
| (45, 68) | [1,2,-3] | d: 1  x: -3  y: 2 |
| (9008, 1200) | [16,2,-15] | d: 16  x: 2  y: -15 |
| (396732, 412345) | [1,109849,-114172] | d: 1  x: -114172  y: 109849 |
| (3567123478, 3019223) | [1,-1055064,1246527191] | d: 1  x: -1055064  y: 1246527191 |
| (69, 100) | [1,-20,29] | d: 1  x: 29  y: -20 |
| (112, 212) | [4,9,-17] | d: 4  x: -17  y: 9 |

(b) 88243(x) + 16947(y) =1

To test this I will use 88243 as input a and 16947 d: 1, x: -2372, y: 12351

88243(-2372) + 16947(12351) =1

# Program 3 – RSA Encryption

**Testing**

|  |  |  |
| --- | --- | --- |
| **Input** | **Expected output** | **Actual output** |
| “PLEA”  P=16120501  n=125590273  e=7 | 106118249 | 106118249 |
| “SECO”  P=19050315  n=125590273  e=7 | 108681457 | 108681457 |
| “LIKE”  P=12091105  N=50000987  e=11 | 35131165 | 35131165 |
| “NOW”  P=141523  N=50000987  e=11 | 17244702 | 17244702 |
| “NEW”  P=140523  N=222440609  e=5 | 6723509 | 6723509 |
| “WHY”  P=230825  N=222440609  e=5 | 178487530 | 178487530 |
| “H”  P=8  p=5,  q=11,  e=7 | 2 | 2 |
| P=44  N=1517  E=49 | 1069 | 1069 |
| P=888999000  N=(153817\*1542689)  E=202404606 |  | 202609913015 |

# Program 4 – RSA Decryption

**Testing**

|  |  |  |
| --- | --- | --- |
| **Input** | **Expected output** | **Actual output** |
| C=106118249  N=125590273  E=7 | 16120501 | 16120501 |
| C=108681457  N=125590273  E=7 | 19050315 | 19050315 |
| C=35131165  N=50000987  E=11 | 12091105 | 12091105 |
| C=17244702  N=50000987  E=11 | 141523 | 141523 |
| C=6723509  N=222440609  E=5 | 140523 | 140523 |
| C=178487530  N=222440609  E=5 | 230825 | 230825 |
| C=2  N=55  E=7 | 8 | 8 |
| C=1069  N=1517  D=529  E=49 | 44 | 44 |
| Decrypt message from program 3 part (ii)  C=202609913015  N=237291793913  E=202404606  D=474581891321 | --- | 22229262441  Explanation on next page |

Why the RSA algorithm appears not to work when decrypting in part (ii):

**This is because the ciphertext generated from program 3 part(ii) resulted from an encryption whose keys did not meet the standards required.**

**Information form program 3 (ii) below,**

Encryption key e and phi must be coprime, i.e. their greatest common divisor is 1. This is not the case as proven below.

P=888999000

P=153817

Q=1542689

Phi=237290097408

E=202404606

ExtEucAlgo(237290097408, 202404606) =

d: 6

x: -4501972

y: 5277910397

If this system was fine d would equal 1.

For contrast below I have checked the first encryption item from program 3’s test sheet (which is an example from the lecture notes),

N=125590273

E=7

P=5021

Q=25013

Phi=125560240

ExtEucAlgo(125560240, 7)=

d: 1

x: 1

y: -17937177