[Report File]

[math assignment]

DeaN FORDE, K00222619

[2018]

**Program 1:**

**Where n is test data and sum is result.**

|  |  |
| --- | --- |
| **n** | **Sum** |
| **1000** | **233168** |
| **10000** | **23331668** |
| **25000** | **145829168** |
| **50000** | **583291668** |

**Program 2:**

**Where n is test data and factors is result.**

|  |  |
| --- | --- |
| **n** | **factors** |
| **30** | **2\*3\*5** |
| **31** | **31 is prime** |
| **487** | **487 is prime** |
| **8893** | **8893 is prime** |
| **987654323** | **987654323 is prime** |
| **131317171919** | **19\*19\*101\*3601579** |

**Program 3:**

**Where n is test data and sum is result.**

|  |  |
| --- | --- |
| **n** | **sum** |
| **10000** | **3382** |
| **1000000** | **1089154** |
| **2500000** | **1089154** |
| **5000000** | **4613732** |

**Program 4:**

**Where a and b is test data and “result” is result.**

|  |  |  |
| --- | --- | --- |
| **a** | **b** | **result** |
| **8359** | **4962** | **GCD = 1; x = -1877; y =3162;** |
| **95243** | **24138** | **GCD = 1; x = 461; y =-1819;** |
| **88243** | **16947** | **GCD = 1; x = -2372; y =12351;** |

**Program 5:**

**Where P, e and n is test data and C is result.**

|  |  |  |  |
| --- | --- | --- | --- |
| **P** | **e** | **n** | **C** |
| **44** | **49** | **1517** | **1069** |
| **888999000** | **202404606** | **237291793913** | **202609913015** |

**Program 6:**

**Where C d n is test data and P is result.**

|  |  |  |  |
| --- | --- | --- | --- |
| **C** | **d** | **n** | **P** |
| **1069** | **529** | **1517** | **44** |

**ii. You cannot compute Bobs corresponding exponent as e is not a prime number and neither is phi therefore it is impossible to calculate exponent d.**

**iii The fact that a decryption key does not exist for Bob means that one does not exist for Alice.**