Main Project 2020

Limerick Institute of Technology

Joe Morais (K00254840)

Software Development Year 2

Discreet Mathematics

Main Project

Program 1: Prime Factorization

Input	Output
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 2: Extended Euclidean Algorithm

i.

Input		Output		
a	**b**	**d**	**x**	**y**
8359	4962	1	-1877	3162
95243	24138	1	461	-1819

ii.

Using the application, I solved 88243x + 16947y = 1

Input		Output		
x	**y**	**d**	**a**	**b**
88243	16947	1	-2372	12351

Program 3: RSA Encryption

i.

Input			Output
p	**n**	**e**	**Ciphertext**
44	1517	49	1069

ii.

When attempting to calculate the Ciphertext using n = (153817 * 1542689), e = 202404606 and P = 88999000 the program continuously looped through the power/exponent loop. I believe the numbers were too big to be calculated.

Program 4: RSA Decryption

i.

Input			Output
c	**d**	**n**	**Plaintext**
1069	1517	529	481

ii. / iii.

Due to computational errors during part ii of the previous question, I am unsure if my algorithm is wrong. Further notes on the next page.

I tested both encryption and decryption with multiple variables all of which seem to work. Even though I used BigInteger variables, the problem was performing an exponent calculation with very large integers.

For example, the encryption code can prove that:

Input			**Output**
p	**n**	**e**	**Ciphertext**
20	33	7	26
21	31	4	18

Similarly, the decryption code can prove that:

Input			**Output**
c	**d**	**N**	**Plaintext**
41	7	77	13
26	7	77	5