University of Baltimore
Math 321: Discrete Structures
Worksheet for Chapter 2: RSA Encryption

The book does example 11 in section 2.6 without much explanation. The calculations in a little more detail are as follows: $S\ T\ O\ P \to 1819\quad 1415,\ \ p=43\ \&\ q=59 \to n=2537,\ \ e=13_{10}=1101_2$

first block: find $C_1 = 1819^{13} \bmod 2537 \qquad 13_{10}=1101_2$

book	n = 2537		M = 1819		power = 1819
i	a(i)	x calc	x mod n	power calc	power mod n
0	1	1819	1819	3308761	513
1	0	1819	1819	263169	1858
2	1	3379702	418	3452164	1844
3	1	770792	2081	not needed	

second block: find $C_1 = 1415^{13} \bmod 2537 \qquad 13_{10}=1101_2$

book	n = 2537		M = 1415		power = 1415
i	a(i)	x calc	x mod n	power calc	power mod n
0	1	1415	1415	2002225	532
1	0	1415	1415	283024	1417
2	1	2005055	825	2007889	1122
3	1	925650	2182	not needed	

The encoded message sent is 2081 2182, to be decoded on the other end.

Your homework:

1) 2.5 #20 (answer: 22)

2) 2.6 #46 (answers: 2299 1317 2117)

3) The three following sets of numbers represent a possible basis for encryption coding:

(a) $p=17, q=37, e=7$ (b) $p=17, q=37, e=11$ (c) $p=41, q=53, e=11$

For each of the sets in 3) above:

→ Use the Euclidean algorithm to verify that e and $(p-1)(q-1)$ are relatively prime.

→ Then use RSA encryption, $C = M^e \bmod n$, to encrypt the word "ante".

answers: (a) 0106 0459 (b) 0089 0476 (c) 0281 1494