MATH 135 Algebra, Assignment 10 Due: Wed Nov 25, 8:30 am

1: (a) The name of a mathematician was encoded using a Caesar cypher to give the cyphertext below. Decrypt the cyphertext.

ZPXGDY

(b) Two quotes from Bertrand Russell were encoded using a substitution cypher to give the cyphertext below. Use the fact that the most frequently occurring letters in English text are the letters E, T and A (in that order) to help decrypt the cyphertext.

GMQEUBQI MWJMVI QMWS BZ XVUYL ZBE QOCUE PBDYQEV
HDQ YCTCE BZ SUWWUYL ZBE QOCUE PBDYQEV.

RMQOCRMQUPI RMV HC XCZUYCX MI QOC IDHACPQ UY JOUPO
JC YCTCE SYBJ JOMQ JC MEC QMWSUYL MHBDQ,
YBE JOCQOCE JOMQ JC MEC IMVUYL UI QEDC.

2: (a) Find $1263^{1842} \pmod{2357}$ using the square and multiply algorithm.

(b) Use Fermat's Little Theorem and the Square and Multiply Algorithm to show that the integer 2479 is not prime (without testing each prime $p \leq \sqrt{2479}$ to see if is a factor).

3: (a) Encrypt the 1-letter message R using the RSA public key $(e, n) = (13, 77)$.

(b) Let $p = 47$, $q = 61$, $e = 43$ and $n = pq$. Encrypt the 2-letter message GO using the RSA public key (e, n).

4: (a) Decrypt the cyphertext $c = 41$ which was encoded from a 1-letter message using the RSA public key $(e, n) = (29, 65)$.

(b) Let $p = 41$, $q = 67$, $e = 217$ and $n = pq$. Decrypt the cyphertext $c = 811$ which was encoded from a 2-letter message using the RSA public key (e, n).

5: (a) Let $n = 459061$. Given that $n = pq$ for some primes $p < q$ and that $\phi(n) = 457612$, find the prime factorization of n.

(b) Let $n = 806437$. Given that $n = pq$ for some primes $p < q$ with $q - p \leq 100$, find the prime factorization of n.