Modern Computing for Mathematicians (Math 587)

Written Assignment No. 2

due March 3, 2009

Prepare this assignment on paper by (a) writing your responses in LaTeX with no line longer than 70 characters, (b) compiling the LaTeX file with `pdflatex` to a PDF file, (c) printing the LaTeX source as plain text, (d) printing the compiled version, and (e) submitting the versions printed in (c) and (d) together at the class meeting. In the write-up for each exercise repeat its statement before introducing your solution. A very simple sketch of how this might be done is available in the course web as:

```
assgt/tex/assgt2-example.tex
assgt/tex/assgt2-example.pdf
```

Be sure to explain what you have done to answer these questions.

1. Two parties A and B agree to construct a private key in the multiplicative group modulo the number 40487 by negotiations in public using the method of Diffie-Hellman key exchange. They agree to use 5 as the generator. If A uses 127 as secret exponent,

   (a) what value does A send to B?

   (b) if, for the same transaction, B sends the value 16874 to A, what value is the jointly constructed private key?

2. Recall that ASCII codes corresponding to the characters used in normal English text strings are values from 1 to 126, and, therefore, may be regarded as elements of the multiplicative group modulo the prime 127.

   Two parties agree to exchange messages using El Gamal cryptography based on the multiplicative group modulo 127, generator 3, and secret exponent 29 with the resulting public key 55. Under this agreement one of them sends the other the following vector of pairs representing coded text:

```
[ [24, 116], [78, 38], [80, 108], [86, 50], [93, 90],
[111, 98], [26, 32], [100, 94], [121, 126], [101, 50], [75, 73],
[65, 51], [31, 40], [108, 41], [82, 27], [103, 17], [39, 106],
[117, 67], [114, 13], [45, 86], [104, 23], [28, 10], [54, 59],
[109, 75], [1, 103], [47, 54], [66, 69], [32, 57], [34, 43],
[110, 94], [41, 126], [44, 105], [55, 47], [2, 105], [27, 33],
[95, 69], [42, 21], [118, 101], [106, 1], [41, 112], [94, 106],
[59, 114], [31, 56], [119, 57], [34, 86], [4, 1], [50, 30],
[54, 94], [119, 25], [110, 3], [85, 76], [85, 25], [38, 5],
[40, 11], [36, 104], [10, 41], [57, 74], [115, 72], [36, 75],
[79, 37], [42, 118], [49, 79], [102, 13], [98, 39], [11, 65],
[30, 103], [99, 90], [10, 120], [82, 125], [24, 47] ]
```

   What is the coded text? (A file suitable for reading this vector of pairs into `gp` is `"assgt/coded-string"`.)