MAT 331, Fall 2008

Project 2: Cryptography

Due Friday, Nov 21st

This project is about the ElGamal cryptosystem (including ElGamal digital signature). You should implement the system (preferably in Maple). Also, you should write a separate paper with two different parts: the first part should describe how ElGamal cryptosystem works, give some explicit examples of its operation and discuss mathematical aspects. You can (although it is not required) discuss its strengths and weaknesses. In this first part, you do not need to mention Maple at all. You should use the library and the Internet for your sources. Make sure you quote all your references and that you process them (not just perform "cut and paste").

In the second part of your paper, you should explain how your Maple code works.

The paper is primarily expository in nature. Hence, it is fundamental to pay attention to organization, sentence structure, and so on. You will be graded on both the quality of your mathematical exposition and on the correctness of your computer work (that is, the implementation of the encryption scheme). A good paper should be complete and self-contained, discussing any necessary background material. Think that you are addressing a reader who might have never attended to our class, but took a few math courses in college.

Keep in mind that, as usual, the writing must be entirely individual and that any form of sharing the paper or the Maple file will be penalized.