MAT 331, Spring 98

Project 2: Cryptography

Due 9 April 1998

For this project, you should pick an encryption scheme (or several, if you so choose), describe how it works, implement it (preferably in maple), and give some explicit examples of its operation. It would be nice (but not required) to discuss the mathematical aspects of the cipher (if relevant), history related to it and its use (if you find any), and/or strengths and weaknesses of this code. You should use the library and/or the Internet for your sources— I have put a number of cryptography-related links on the web page. You may, if you choose, write about a topic related to cryptography instead, such as steganography (data hiding), pseudo-random number generators, or digital signatures. You cannot use a cipher that we have covered (or will cover) in class. (This includes the RSA algorithm, which we will begin soon).

Some ciphers you might consider are:

- transposition methods
- the Playfair cipher
- Vignère's autokey system
- rotor-like algorithms, such as the German enigma.
- Knapsack methods
- probabilistic methods
- elliptic curve cryptography

Encryption schemes such as DES and block ciphers are probably not appropriate, because implementation generally requires bit-level manipulations. Encryption schemes with some amount of a mathematical component are preferred.

This project is primarily expository in nature. In your write-up, please 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 your cryptosystem). You should treat this like a paper. A good paper should be complete and self-contained, going over any necessary background material. Think of yourself six months ago as a typical reader.