

MAT 331, Spring 2004

Project 3: Cryptography

Due Tuesday, May 11

For this project, you should pick an encryption scheme, describe how it works, implement it if possible (preferably in *Maple*), and give some explicit examples of its operation. It would be nice (but not required) to discuss mathematical aspects of the encryption scheme, history related to it and its use, and its strengths and weaknesses. You should use the library for your sources. Try to avoid internet sources. I might put some trusted cryptography-related links in the class web page so you can consult them. You may instead write about a topic related to cryptography, such as steganography (data hiding), pseudo-random number generators, digital signatures and cryptographic hashing, cryptographic protocols, authentication, cryptanalysis (code breaking), etc. You cannot use an encryption scheme that we have discussed in class.

Some topics you might consider are

- transposition methods
- the Playfair cipher
- Vignère's autokey system
- rotor-like algorithms, such as the German enigma machine
- Knapsack methods
- probabilistic methods
- El Gamal encryption
- elliptic curve cryptography
- automatic breaking of a Vignère cipher
- zero-knowledge proofs
- playing poker over the telephone
- secret-sharing algorithms

If the topic you choose is not appropriate for implementation, your paper should make up for that with a more detailed discussion.

This project is primarily expository in nature. In your report, please pay attention to organization, sentence structure, spelling, grammar, etc. 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 encryption scheme). You should treat this report like a term paper. A good paper should be complete and self-contained, discussing any necessary background material. Think of yourself six months ago as a typical reader. Try to use a word processor for the paper, and complement it with a Maple work sheet with the implementation.