MAT 331, Fall 2019

Project 3: Encryption

Due Wednesday, 18 December 2019

In this project, you are to put into practice some of the ideas of encryption that we have studied in class. For this project, you are to choose one of the enciphering methods listed below, research it, implement it in Maple, and describe the method and any relevant aspects of it (whether they are concerned with its history, its security or lack thereof, or other aspects you may choose). You should choose some suitable test cases to demonstrate your implementation, and I must be able to use your implementation to encrypt/decrypt messages of my choosing.

You should address the issue of whether your cipher must use an alphabet of a specific size, or can be adapted to other character sets. (For example, the Solitaire cipher is designed to be used with a deck of cards, and hence a 26-letter alphabet is important.)

The suggested encryption schemes are

- Four-Square cipher.
- Solitaire cipher.
- Diffie-Hellman key exchange protocol (not encryption, but related).
- The Cayley-Purser algorithm.
- El Gamal encryption.

As before, it is important to realize that exposition is an important part of this project.

It is important that you cite your sources. No particular format is required, but it should be clear what sources you used. Using material without giving proper credit constitutes plagiarism; be honest and generous with credit.