Cover Sheet for Activity*

Title: Abstract Algebra Project: Public-Key Cryptosystems

Author(s): Michael Dougherty

Course(s) and textbook(s) (or other info to contextualize the course and activity): A first course in abstract algebra, or any course which uses modular arithmetic.

Type/Size of Institution(s): Any size.

Class Size(s): Any size.

Mathematical Content: Modular arithmetic, Diffie–Hellman key exchange

Learning Objective(s):

- Develop an understanding of the Diffie–Hellman key exchange algorithm and why it is difficult to break.
- Reflect on the differences between public-key cryptography and its private-key counterpart.
- Appreciate the ethical questions which naturally arise when discussing cryptographic applications.

Time Required & Implementation Plan: One day in class is recommended to introduce the Diffie–Hellman algorithm. Students should be given two weeks to complete the project.

Grading and Assessment Recommendations: The first part should be graded based on mathematical accuracy. The second and third parts should be graded by the depth of analysis and clarity of writing.

Required resources and technology: None.

Brief Description/Abstract: How can you communicate securely over an unsecure channel such as the internet? This question was first addressed by a few groups in the 1970s, using what is called "public-key cryptography." One of the answers, called "Diffie–Hellman key exchange," uses modular arithmetic—a relatively simple mathematical tool—to solve this problem, but was so effective in providing secure communication that US intelligence agencies attempted to prevent its dissemination. Ultimately, this protocol became one of the essential components of internet communication and is ubiquitous today. In this project, students learn the basics of the Diffie–Hellman algorithm and examine the ethical issues which arose during its development.

*Supported by NSF Grant 2220314, 2220423, 2220395