640:103:99 (Spring, 2000)
The Mathematics of Communications: keeping secrets

Three may keep a secret, if two of them are dead.
Benjamin Franklin (July, 1735)

- The course meets Mondays and Wednesdays 4^{th} periods (1:10–2:30 PM) in ARC 203 on Busch campus. Admission is by permission (this is an honors course).

- Instructor: S. Greenfield, Department of Mathematics
  - ⋆ Office: 542 Hill Center, Busch
  - ⋆ Telephone: 445-3074 (this has an answering machine)
  - ⋆ E-mail: `greenfie@math.rutgers.edu` (probably the best way to communicate!)
  - ⋆ Office hours: To be announced – probably Monday 3^{rd} period (11:30–12:50) and Wednesday 2^{nd} period (9:50–11:10) or drop in or make an appointment.
- Teaching assistant: S. Radomirovic, Hill 101, `sasar@math.rutgers.edu`

- Text and other resources:
  - ⋆ The official text is *Cryptology* by Albrecht Beutelspacher, published by the Mathematical Association of American (1994). Copies are available in the bookstore.
  - ⋆ You should have a calculator available which can do 6 to 8 digit arithmetic. You will need this for work in and out of class.
  - ⋆ Some familiarity with computers and the Rutgers computer systems: 1) be able to send and receive e-mail; 2) be able to access and search the Internet; 3) be able to use simple aspects of the computer program `Maple` (installed on `Eden` and most Rutgers computer systems).

- The topics of the course will be selected from computer science, history, mathematics, and public policy. You should become familiar with some of the mathematics which supports secret communication. We also will investigate some of the history of such communication and a few of the current controversies which accompany it.
  - ⋆ Mathematics: notation and basic ideas about arithmetic; the elements of number theory and probability required to support some extremely ingenious schemes for hiding and sharing knowledge. How difficult is computation? What is information?
  - ⋆ History: groups within almost every known culture have wished to conceal records and communications. What have they done, what success have they had, and what have been the consequences?
  - ⋆ Public policy: with the advent of widespread use of digital computers and their interconnection, questions involving cryptography have become important. We will try to address such questions as ownership and reproduction of intellectual property, privacy of telephone and electronic communications, privacy of medical records, anonymity of financial transactions, and trustworthy communications. These are related to legal questions and business practices, and certainly involve some knowledge of what is possible and what is likely to be practical.

- The math background needed for this course is good knowledge of high school algebra and some knowledge of analytic geometry. Students will write short papers, and research on the web and in libraries will be needed. The most important traits will likely be energy, intelligence, diligence, and, most of all, willingness to question the instructor.

- Workload and grades: few of the classes will be lectures. Most will involve some student activities, and class participation will be a large component of the grade. The material is not standard so students should plan to attend every class. Exams will be announced in advance. Students will write short papers and will make group presentations on topics connected with the course.