

1. **Instructor:** Bruce Dodson, Room 207 XS, Phone x8-3745, e-mail bad0@lehigh.edu.

2. **Text:** Buchmann, *Introduction to Cryptography, Second Edition*. Selected portions of Chapter 1 - 10 and Chapter 13 will be covered. In particular, we will explain how breaking the RSA-keys RSA-155 (with 512-bits binary; on the cover of the first edition of our text) and RSA-576 (cover, second edition) involve a distributed internet computation.

The current record is RSA-768, with 233-decimal digits. Improvements in methods for breaking RSA-keys has focused attention on the alternative Elliptic Curve Cryptography, ECC, and we hope to include an introduction to elliptic curves, both in Number Theory and in cryptographic applications, depending upon interest.

3. **Objectives:** We will describe (some) fast random encryption systems, such as DES and AES (Advanced Encryption Standard, 128-bits), and how they differ from encryption using hard math computations (RSA and “discrete logs”). In both cases the emphasis will be on how security requirements change over time due to improvement in computation, both from new hardware and from new algorithms. We may also cover some additional topics depending upon interest.

Complete descriptions will be given of the mathematical background, including modular arithmetic (especially fast exponentiation) and congruences, polynomials and matrices.

4. **Attendance:** Attendance is expected at all lectures. If necessary, attendance will be encouraged using in-class quizzes, possibly without further announcement.

5. **Homework:** Carefully written solutions to homework will be included as a part of both lectures and your grade in the course. Some assignments will involve mathematical proofs, at a level depending upon student background.

6. **Exam:** We will have an hour exam based on material from Chapters 1, 2 and parts of 3. This will be the only exam material, and if necessary there will be retest(s) to make sure everyone is comfortable with this background.

7. **Presentations:** Near the end of the semester, each student will be expected to give an in-class presentation on a topic of interest. Depending upon topic somewhere between 20-minutes to a full 50-minutes will be available. There will be specific suggestions based on text material (for people that want suggestions).

8. **Grades:** Grades are based on:

One Hour Exam	100
Class Presentation	200
Homework and Quizzes	200
Total	500

9. **First assignment:** Read 1.1-1.2, 1.3, 1.11 (without proofs), 2.11, 2.12, 7.1-7.2, 7.4-7.5. We will return to Ch. 1 for GCDs. The first homework problems (from the Ch 1 and Ch 2 reading) will be given soon.