Cryptography is the study of secure communication and related issues. Of foremost importance in cryptography is the creation and maintenance of \textit{ciphers}, which are schemes to securely transmit or store messages or data in the presence of a malicious entity known as an \textit{attacker}. However, cryptography has also expanded so that \textit{confidentiality}, \textit{data integrity}, \textit{authentication}, and \textit{non-repudiation} are included under its auspices.

Fundamental to the idea of modern cryptography are so-called \textit{public-key cryptosystems}, where the essential concept is that of \textit{asymmetric encryption}, i.e., the decryption scheme is not simply a reversal of the encryption scheme. The idea of public-key cryptography was first introduced in the landmark paper \textit{New directions in cryptography} of Whitfield Diffie and Martin Hellman in 1976, although it was previously discovered by GCHQ but remained unpublished. Any public-key cryptosystem must be based on what are called \textit{one-way functions}, which are easy to compute, but difficult to invert without secret knowledge.

In this course, we will begin with an overview of the origins of public-key cryptography which are still in use today (DH, RSA). Prior knowledge of cryptography, public-key or otherwise, is neither assumed nor required. We will then provide a gentle introduction to computational complexity theory, which is the study of how difficult various problems are to solve. Computational complexity is essential to cryptography because it tells us which mathematical problems might be ripe for exploitation as cryptosystems. We will then briefly review the algebra necessary for the remainder of the course, including various facts about finite fields, field extensions, polynomial rings, and ideals. Finally, we will introduce elliptic curves and describe the modern ElGamal cryptosystem based on them. Time permitting we will cover one of the other topics included in our text: hidden monomial cryptosystems, combinatorial–algebraic cryptosystems, or hyperelliptic curves.

We will use \textit{Algebraic Aspects of Cryptography}, by Neal Koblitz who is one of the founders of elliptic curve cryptography. Prerequisites include the content of MATH-420, namely, finite fields and field extensions, modular arithmetic, polynomial rings and ideals.

Course objectives

- describe the key purposes of cryptography;
- explain how a public-key cryptosystem works, especially Diffie–Hellman and RSA and the trapdoor problems on which they are based (discrete logarithm, integer factorization);
- evaluate the computational complexity of simple algorithms;
- identify where various problems lie in the hierarchy of complexity theory;
- perform computations on elliptic curves and explain the supposed security of elliptic curve cryptosystems.
Course Outline And Topics

1. Cryptography
   (a) Symmetric ciphers
   (b) Origins of public-key cryptography
   (c) RSA
   (d) Digital signatures and other cryptographic applications

2. Computational complexity
   (a) Big-O
   (b) Length of numbers
   (c) Time estimates
   (d) P, NP and NP-completeness
   (e) Randomized algorithms

3. Necessary algebra
   (a) Finite fields
   (b) Field extensions
   (c) Polynomial rings

4. Elliptic curve cryptography
   (a) Elliptic curves
   (b) ElGamal cryptosystem and ECDSA
   (c) Elliptic curves and long standing conjectures

Optional Material

5. Hidden monomial cryptosystems
6. Hyperelliptic curves
7. Algebraic-combinatorial cryptosystems
8. Cryptocurrency

Grading procedure

• Two midterm exams (15% each)
• Homework assignments (40% total)
• Comprehensive final exam (30%)

Important dates

1 September 2017 | Last day to drop without a grade, with full reimbursement
15 September 2017 | Last day for partial refunds
20–26 November 2017 | Thanksgiving break
27 October 2017 | Last day to withdraw without permission for W
17 November 2017 | Last day to withdraw from a class or from school with permission
Makeups

If an emergency arises which requires you to miss an exam, I must be made aware at least two hours prior to the start time of your exam. Note: proper documentation will be required before a makeup arrangement is considered.

Academic dishonesty/misconduct

Academic misconduct includes, but is not limited to, cheating, plagiarism and forgery, and soliciting, aiding, abetting, concealing, or attempting such acts. Plagiarism may consist of copying, paraphrasing, or otherwise using written or oral work of another without proper acknowledgment of the source or presenting oral or written material prepared by another as one’s own. At minimum, cheating will result in that assignment receiving a grade of zero.

Official communication

Your SIUE student e-mail account is the official method to communicate between you and your instructor. Official communication will not be sent to your personal e-mail (yahoo, wildblue, gmail etc.).

Disability Support Services

If you have a documented disability that requires academic accommodations, please go to Disability Support Services for coordination of your academic accommodations. DSS is located in the Student Success Center, Room 1270; you may contact them to make an appointment by calling (618) 650-3726 or sending an email to disabilitysupport@siue.edu. Additional information is located online at www.siue.edu/dss.

Disclaimer

This syllabus is subject to change by the instructor if deemed necessary for the benefit of student learning or to correct errors and omissions.