Macintosh HD:Users:ers:Dropbox:ACTIVE:JHU-logos:WSE:small:PDF:whiting.small.horizontal.black.pdf

**Applied Mathematics and Statistics 550.371**

**Cryptology and Coding**

**Spring 2017 (4 credits, EQ)**

**Instructor**

Professor Donniell Fishkind, [def@jhu.edu](mailto:def@jhu.edu), http://www.ams.jhu.edu/~fishkind

Office: Whitehead Hall 304B, 410-516-7828

Office hours: Monday, Wednesday, Friday noon to 1pm, and by appointment.

**Teaching Assistants**

Julian Gould [jgould15@jhu.edu](mailto:jgould15@jhu.edu) and Andrew Hawkins [ahawki14@jhu.edu](mailto:ahawki14@jhu.edu) . Office hours for the TAs are all held in the Whitehead Hall help room on the second floor.

Office hours for TAs are dynamically updated on course webpage as changes are made.

**Meetings**

Monday, Wednesday, Friday, 1:30–2:20 pm, Shaffer Hall, Room 303.

**Textbook**

None required. Useful textbooks are listed on the course webpage.

**Online Resources**

Course website is at <http://www.ams.jhu.edu/~fishkind/550_371.html>

**Course Information**

An introduction to cryptology. We will begin with an overview of the classical and modern symmetric cryptosystems; Caesar, substitution, affine, and Vigenere ciphers, Vernam one-time-pad, DES, and Rijndael. We will also discuss cryptanalysis of the above. We introduce and develop relevant number theory, abstract algebra, and computer science, and then move on to asymmetric "public key" cryptosystems, including RSA, Rabin, Diffie-Hellman key exchange, Elgamal. We explore factoring integers and generating large prime numbers. Error correcting codes. Additional topics as time permits.

* **Prerequisites**

Discrete Mathematics (EN.550.171 or the equivalent)

Linear Algebra (AS.110.201 or the equivalent)

Computing experience

* **Required**

**Course Goals**

Specific Outcomes for this course are that

* Students will learn classical and modern methods of cryptology, cryptanalysis, making digital signatures (and similar such) in a mathematical framework.
* Students will learn how to execute these methods computationally.
* Students will understand the theory behind these methods.

This course will address the following Criterion 3 Student Outcomes

* An ability to apply knowledge of mathematics, science and engineering (Criteria 3(a))
* An ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability – the design process (Criteria 3(c))
* An ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability – recognition of constraints within design (Criteria 3(c))
* An ability to identify, formulate and solve engineering problems (Criteria 3(e))
* An understanding of professional and ethical responsibility (Criteria 3(f))
* An ability to communicate effectively (writing) (Criteria 3(g))
* The broad education necessary to understand the impact of engineering solutions in a global, economic, environmental and societal context (Criteria 3(h))
* A recognition of the need for and an ability to engage in life-long learning (Criteria 3(i))
* An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (Criteria 3(k))

**Course Topics**

* Classical and modern symmetric cryptosystems; Caesar, substitution, affine, Vigenere ciphers, Vernam one-time-pad, DES, Rijndael.
* Cryptanalysis of the above.
* Relevant background in number theory
* Relevant background in abstract algebra
* Relevant background in computational complexity
* Asymmetric, Public key cryptosystems; RSA, Rabin, Diffie-Hellman key exchange, Elgamal cryptosystems.
* Factoring integers; exponent factorization, p-1 method, quadratic sieve.
* Discrete logarithms
* Generating large prime numbers, primality testing.
* Secret sharing.
* Error correcting codes.
* Other topics as time permits

**Course Expectations & Grading**

Weekly homework assignments, two midterms, one final. Weekly homework is worth 15% of your grade, and the three exams are each worth a third of 85% of your grade. On the semester, percentages above 90, 80, 70, 60% are respectively guaranteed the grades A, B, C, D, but I reserve the right to lower these thresholds to reflect the difficulty of the exams and assignments. The top few points of each letter grade get a “+” appended to the letter, and the bottom few points of each letter grade get a “-“ appended to the letter.

**Key Dates**

Homework will be assigned as the associated material is covered, and exam dates will be decided by class vote on several options for exam dates that I will offer for consideration. The final exam date is scheduled by the registrar’s office.

**Ethics**

The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful. Ethical violations include cheating on exams, plagiarism, reuse of assignments, improper use of the Internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition.

[In addition, some specific ethics guidelines for this course are:

You may discuss homework problems with other students in the class up until the time you begin your writeup; your writeup must be your own and must reflect your understanding and effort.]

Report any violations you witness to the instructor.

You can find more information about university misconduct policies on the web at these sites:

* For undergraduates: <http://e-catalog.jhu.edu/undergrad-students/student-life-policies/>
* For graduate students: <http://e-catalog.jhu.edu/grad-students/graduate-specific-policies/>

**Students with Disabilities**

Any student with a disability who may need accommodations in this class must obtain an accommodation letter from Student Disability Services, 385 Garland, (410) 516-4720, [studentdisabilityservices@jhu.edu](mailto:studentdisabilityservices@jhu.edu) .

If you are allotted extra time on exams then the exam will begin at the same time as the rest of the class, and extend for as long as the time that you are allotted.

**Additional Policies**

There will be no makeup exams, nor early or late exams for any reason. If an exam is missed due to a medical emergency or another similar excused reason then I must be notified as soon as possible, and the exam will be made up for by averaging other exams in its place.