**MIDTERM 1 INFO – MATH 5405**
**SPRING 2016**

The first midterm will be on Thursday February 18th. The test will be about 45 minutes long. There will be no calculators or notes.

There will be 4 pages.

(1) The first page will be short answers. I will ask you about basic definitions. For instance, I could ask what you if what a field is, or whether the integers are a field. I could Ask what conditions on $g(x)$ imply that $(\mathbb{Z}/7[x])/g(x)$ is a field. For a fixed $g$ I could ask how many elements the field has. I could ask you to find the order of an element (of some group) or if some element is a primitive root / generator. I could give you some autocorrelation data and ask you what the likely key length of a Vigenére cipher is (or possibly with some frequency data). I could ask you to show that a certain low degree polynomial is irreducible. I could give you some data of a Diffie-Hellman key exchange and ask you what the common key is. Finally, I might ask you about some of the primality testing we learned on 2/11 or 2/16.

(2) There will be a page on classical ciphers. Things like Caesar shifts, Vigenére, Columnar Transposition. I could ask you to encrypt or decrypt something (or maybe even break some encryption).

(3) There will be a page on computations with polynomials with coefficients in $\mathbb{Z}/p$. For instance I could ask you to find the order of some element, to find the inverse of some element, to find whether an element is a primitive root/generator.

(4) There will be a page on Diffie-Hellman, ElGamal, and/or RSA. You might have to carry out some computation to encrypt something. I could also ask you to break some encryption by factoring something or computing a discrete logarithm.