FINAL – MATH 5405
SPRING 2016

The final will be on Monday, May 2nd, 10:30am-12:30pm.
There will be 4 pages.

(1) The first page will be short answers. 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. Miller-Rabin could show up. There could be short answer questions on various factoring methods ($p-1, p+1$, Pollard's rho, quadratic sieve, Lenstra's elliptic curve method, etc.). We could also have short answer questions on elliptic curve group (either the size or just general facts). Additionally, things like Diffie-Hellman, ElGamal and RSA are fair game. AES could also appear here. We will have questions on error detecting and correcting codes.

(2) There will be a page on ciphers. Some could be classical (Caesar shift, Vigenére, Columnar tranposition), or modern (RSA, ElGamal, Diffie-Hellman etc.).

(3) There will be a page on modular arithmetic and elliptic curves (we could also include things like Lenstra's factoring method or Miller-Rabin here).

(4) There will be a page on coding theory. You should be familiar with the bounds on codes we have/will discuss. You should also be familiar with Hamming codes, and if we are able to cover them, with Golay codes and Reed-Solomon codes. For instance, I could send a message with a certain code and you could be responsible for correcting the errors.