Discrete Mathematics for Cryptographic Applications

CSC 85031 Spring, 2011 CUNY Graduate Center, Department of Computer Science
Prof. Kent D. Boklan
Class Time: Thursdays, 2:00 – 4:00

Ten year old boys and girls run and jump about, they play video games, they accidentally download computer viruses and they invent secret codes, their very own private algorithms to disguise their communications from both parent and peer. On their own, children quickly learn the rules: their approaches must be efficient and their methods must be able to be undone, too. (Children who spend their efforts breaking the systems of their classmates are scarcer; budding cryptanalysts, it seems, are tougher to come by than young cryptographers.) It’s the bread and butter of cryptography, the encrypting. And there’s a popular mythology to Top Secret ciphers and to spy intrigue - with those television shows with the strong encryption that always manages to get broken. We are inundated by media pronouncements of strong (or strongest!) protections with such ubiquitous phrases as, “128 bit encryption.” It seems that everyone does it or claims they do it. Even I can do it, with my Captain Midnight decoder badge that I bought off eBAY. But exactly how does it all work? Cryptography is not just the latest trend like hula hoops, betamax and the Spice Girls. It’s here and it’s not going away and someone needs to know how it really works - and if it’s really strong.

Ah, but a man's reach should exceed his grasp, or what's an SSL for?

For as long as mankind has had the ability to communicate, there has been a need, a desire for privacy. This is a necessity of our species: to be able to conduct our conversations and our business, professional and intimate, in such a way that they are not public, for all to view. Cryptography, the art and science of keeping messages secure, has been practiced since languages first evolved.

This course serves as an introduction to cryptographic practices and the Mathematics behind it all. We will learn many classical protocols and some of the attacks against them (the cryptanalysis) – and some will be implemented (by you). And we will learn the Mathematics needed to gain a firm foothold on how information and communication security is accomplished today. And then we will address, in the immortal words of Buffy, “Where do we go from here?”


Course grades will be determined by five factors: performance on three or four problem sets (10% each), score on a take home midterm examination (15 or 20%), work on a project where you will be tasked with breaking a cipher (15%) and class attendance and participation (10%). An optional final examination (20 or 25%) will be offered. (If you do not choose to take the exam, your course grades will be rescaled accordingly.) You will need to program (well). Late problem sets will not be accepted.

Course topics will include

...
Number theory for cryptography:

Applications: discrete logarithms, Knapsack, RSA, DSA, El Gamal, digital signatures, (trapdoor) one-way
functions, data integrity, linear congruential generators, index calculus, the quadratic sieve

Finite field theory for cryptography

Applications: Rijndael, linear feedback shift registers, A5, primitive tap polynomials, RC4, stream ciphers

Elementary Combinatorics and Probability

Applications: mono and polyalphabetic ciphers, language recognition, the Enigma machine, random number
generators, one-time pads, DES, 3DES and other block ciphers and modes, Feistel networks,
Vigenère, multiple encryption, collisions, data integrity, Pollard’s kangaroo, certificates

Basic group theory for cryptography

Applications: RSA, Diffie-Hellman and elliptic curve methods