DALHOUSIE UNIVERSITY
Inspiring Minds

Department of Mathematics & Statistics

Course Curriculum - Fall 2014

Course Number: MATH4116
Course Name: Cryptography
Instructor: Selinger
Textbook:

WEEK	DATES	TOPICS COVERED	BOOK SECTIONS
1	Sep. 5	Terminology: cryptoanalysis vs cryptography, cv. steganography, plaintext, ciphertext, Alice, Bob, Eve, symmetric and public key cryptography. Applications: confidentiality, data integrity, authentication, non-repudiation. Attacker goals: read the message, find the key, change the message, masquerade. Attack models: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext.	Trappe-Washington Ch. 1.
2	Sep. 8-12	Ceasar and shift ciphers, brute force attack. The sets Z and nZ. Intersection of nZ and mZ. Ideals of Z, Z is a principal ideal domain. Z/nZ. Divisibility, greatest common divisor and d=ax+by.	Trappe-Washington 2.1, 3.1-2.
3	Sep. 15-19	Euclid's algorithm. Invertibility in Z/nZ. Affine ciphers. Dot products and correlation of random variables; letter frequency attacks. Vigenere cipher and its cryptanalysis.	Trappe-Washington 3.2, 2.2-3.

4	Sep. 22-26	Vigenere cipher demo. Playfair cipher. Block ciphers and stream ciphers. Substitution permutation networks. Confusion and diffusion. Linear cryptanalysis: piling-up lemma. Linear relations.	Trappe-Washington 2.3, 2.6. Heys 1-2, 3.1-3.
5	Sep. 29-Oct. 3	Setting up a linear relation for the cipher; calculating overall bias from active S-boxes. Two methods for linear cryptanalysis.	Heys 3.4-5.
6	Oct. 6-10	Complexity analysis of linear attack. Design of better S-boxes. Differential cryptanalysis: difference tables, differential characteristic, attack on key bits.	Heys 3.6, 4.1-4.
7	Oct. 15-17	Complexity analysis of differential cryptanalysis. Chinese Remainder Theorem.	Heys 4.5. Trappe-Washington 3.4.
8	Oct. 20-24	Modular exponentiation by repeated squaring. p|ab => p|a or p|b; unique factorization into primes; definition of a group. a^n=1 in groups of size n; Fermat's Little Theorem, Euler's Theorem; 3-pass protocol.	Trappe-Washington 3.5-6.
9	Oct. 27-31	Midterm. Primality testing: Fermat pseudoprime test, Miller-Rabin test.	Handout 3.

10	Nov. 3-7	Euler's phi function, formula for phi(n) given a prime factorization of n. Proof that computing phi(n) is equivalent to factoring n. RSA cryptosystem. Factoring algorithms: trial division and Fermat's method.	Trappe-Washington 3.6, 6.1, 6.4.
11	Nov. 12-14	Factoring algorithms: quadratic sieve. Pitfalls to avoid with RSA. Definition of primitive root. Number of primitive roots in Z_p.	Trappe-Washington 6.4.1, 6.2, 3.7.
12	Nov. 17-21	Proof of existence of primitive roots. Discrete logarithms. The Diffie-Hellman key exchange protocol. The ElGamal cipher. Equivalence between ElGamal and the computational Diffie-Hellman problem. Elliptic curves: law of addition.	Trappe-Washington 3.7 + extra material. 7.1, 7.4-5, 16.1-2.
13	Nov. 24-28	Elliptic Diffie-Hellman key exchange and elliptic ElGamal cryptosystem. Computing square roots modulo p, when p=3 (mod 4), and for general p. Polynomial division, polynomial gcd.	Trappe-Washington 16.5 (excluding 16.5.3). 3.9 + extra material.
14	Dec. 1	Factoring: Pollard-Rho method; p-1 method; elliptic curve factoring.	6.4, 16.3 (excluding 16.3.1) + extra material.