Course Syllabus

SM486A, Cryptography and Information Security

Text: Making and Breaking Codes: An Introduction to Cryptology,

by Paul Garrett

Topics

1 Simple Ciphers

1.1 The Shift Cipher
1.2 Reduction/Division Algorithm.
1.3 The One-Time Pad
1.4 The Affine Cipher

2 Probability

2.1 Counting
2.2 Basic Ideas
2.3 Statistics of English
2.4 Attack on the Affine Cipher

3 Permutations

3.1 Cryptograms: Substitutions
3.2 Anagrams: Transpositions
3.3 Permutations
3.4 Shuffles
3.5 Block Interleavers

4 A Serious Cipher

4.1 The Vigenere Cipher
4.2 LCMs and GCDs
4.3 Kasiski Attack
4.4 Expected Values
4.5 Friedman Attack

5 More Probability

5.1 Generating Functions
5.2 Variance, Standard Deviation

5.3 Chebycheff's Inequality
5.4 Law of Large Numbers

6 Modern Symmetric Ciphers

6.1 Design Goals
6.2 Data Encryption Standard
6.3 Advanced Encryption Standard

7 The Integers

7.1 Divisibility
7.2 Unique Factorization
7.3 Euclidean Algorithm
7.4 Multiplicative Inverses
7.5 Computing Inverses
7.6 Equivalence Relation
7.7 The Integers mod m
7.8 Primitive Roots, Discrete Logarithms

8 The Hill Cipher

8.1 Hill Cipher Operation
8.2 Hill Cipher Attacks

9 Complexity

9.1 Big-Oh-Little-Oh Notation
9.2 Bit Operations
9.3 Probabilistic Algorithm
9.4 Complexity
9.5 Subexponential Algorithm
9.6 Kolmogorov Complexity
9.7 Linear Complexity
9.8 Worst-Case versus Expected

10 Public-Key Ciphers

10.1 Trapdoors
10.2 The RSA Cipher
10.3 Diffie-Hellman Key Exchange
10.4 ElGamal Cipher
10.5 Knapsack Cipher
10.6 NTRU Cipher
10.7 Arithmetica Key Exchange
10.8 Quantum Cryptography

11 Prime Numbers

11.1 Euclid's Theorem
11.2 Prime Number Theorem
11.3 Primes in Sequences
11.4 Chebycheff's Theorem
11.5 Sharpest Asymptotics
11.6 Riemann Hypothesis

12 Roots mod p

12.1 Fermat's Little Theorem
12.2 Factoring Special Expressions
12.3 Mersenne Numbers
12.4 More Examples
12.5 Exponentiation Algorithm
12.6 Square Roots mod p
12.7 Higher Roots mod p

13 Roots Mod Composites

13.1 Sun Ze's Theorem
13.2 Special Systems
13.3 Composite Moduli
13.4 Hensel's Lemma
13.5 Square-Root Oracles
13.6 Euler's Theorem
13.7 Facts about Primitive Roots
13.8 Euler's Criterion

Selected Exercises are to be assigned in class.