

Advanced Cryptology Syllabus

Instructor: Wesley Pegden

July 15, 2006

Week 1

Day 1: Substitution ciphers

Morning: Caesar cipher

- Description of the Caesar cipher.
- Groups send messages to each other with Caesar cipher.
- Working in groups to break Caesar-ciphertexts in which word lengths are preserved.
- Using frequency analysis to break the cipher when word lengths aren't preserved.

Afternoon: substitution cipher

- Discussion of frequency analysis (for general substitution ciphers).
- Working as a class to break substitution ciphers with frequency analysis.

Day 2: Crash course in number theory/The affine cipher

Morning: number theory

- Basic Proofs.
- Divisibility.
- gcd's.
- Modular arithmetic.
- Multiplicative inverses (mod n).

Students work in groups on their proofs and problems.

Afternoon: application: affine cipher

- The affine cipher and multiplicative inverses.
- Groups send messages with affine cipher.
- Breaking the affine cipher: frequency analysis and solving systems of equations to a modulus.

Day 3: The Vigenère cipher

Morning

- Description of the Vigenère cipher.
- Groups send messages with Vigenère cipher.
- Discussion: Cracking the Vigenère cipher?
- Using the Kasiki Test and frequency analysis to crack the Vigenère cipher.

Afternoon

Class works together to break a long Vigenère cipher.

Day 4: Permutations

Morning: the permutation cipher

- What is a permutation?
- Discussion: multiplication of permutations?
- The permutation cipher: encryption, decryption, and cracking.

Afternoon: more on permutations

- Generating S_n from transpositions.
- Definition of the sign of a permutation.

Day 5: 2×2 matrices and the Hill cipher

Morning

- 2×2 Matrices:
 - Multiplication.
 - Inverses/Determinant (deriving).
 - Matrix multiplication and inverses mod 26.
- The Hill cipher with 2×2 matrices: groups send messages.

Afternoon

- Discussion: cracking the 2×2 Hill cipher with frequency analysis on digrams and by setting up the correct matrix equations.
- Class works together to crack 2×2 hill ciphers.

Week 2

Day 1: $n \times n$ matrices

Morning: the determinant

- Definition of the determinant for general matrices (definition is based on the sign of permutations).
- Group work: finding the determinant of some 3×3 , 4×4 , and sparse 5×5 matrices.

Afternoon: Gaussian elimination

- Elementary row operations, effect on determinant.
- Elementary matrices.
- Proof of correctness of Gaussian elimination to find determinants and inverses of matrices (both over \mathbb{R} and mod 26.)

Day 2: the Hill cipher

Morning

- Encrypting and decrypting with the Hill cipher (involves finding inverses of large matrices).

Afternoon

- Discussion: Cracking larger Hill ciphers with frequency analysis on blocks and by solving the associated matrix equations.
- Class breaks a 3×3 Hill cipher (wow!).

Day 3: Merkle's Puzzles

Morning

- Discussion: Public-channel cryptography.
- Description of Merkle's idea.
- Discussion: How can we implement Merkle's Puzzles?

Afternoon

- Class implements Merkle's Puzzles by using sentences encrypted with the Caesar cipher as 'puzzles'.
- Groups send messages to each other, while other groups 'eavesdrop' and try to break the codes by solving all (or most) of the puzzles.
- Discussion: weaknesses in our implementation of Merkle's Puzzles? Ways to improve?

Day 4: The perfect code system

Morning

- Basic concepts in graph theory.
- Definition of a perfect code in a graph.
- Description of the perfect code cryptography scheme.

Afternoon

- Class splits into groups. Each group makes graphs with perfect codes. The graphs are their public keys, the codes their private keys. They exchange messages with other groups, while 'eavesdropping' groups try to break their messages (usually by trying to find a perfect code in their graph).

Day 5: Kid-RSA and FLT

Morning: Kid-RSA

- Description of Kid-RSA
- Students send 'messages' (just a small number) to each other with Kid-RSA.
- Discussion: is Kid-RSA secure?

Fermat's Little Theorem

- Statement of Fermat's Little Theorem.
- Proving Fermat's Little Theorem by counting 'bracelets'.
- Proving Fermat's Little Theorem with graphs.

Week 3

Day 1: RSA

Morning: machinery

- Fast modular exponentiation algorithm.
- Extended Euclidean algorithm for finding modular inverses.
- Description of the RSA algorithm.

Afternoon

- Proving the correctness of the RSA algorithm (i.e., that decryption reverses encryption).
- Groups send each other 'messages' (small numbers) with RSA, using primes 2 or 3 digit primes for p and q .

Day 2: RSA

Morning

- The Fermat primality test.
- Students implement the Fermat primality test by hand to test for primality of 4 and 5 digit numbers.

Afternoon

- Students break into groups and generate RSA public/private key pairs to exchange 'messages' with other groups.

Day 3: More RSA/Diffie-Hellman

Morning: more RSA

- Discussion: given the inefficiencies of RSA (especially when implementing it by hand!) how can we use RSA to send long messages?
- Students break into groups, and exchange messages encrypted with the Hill cipher, and send the 'key' with RSA by generating public/private key pairs (this is a LOT of work by hand).

Afternoon: Diffie-Hellman

- The Diffie-Hellman key agreement protocol.
- Groups use Diffie-Hellman key-agreement to exchange messages without eavesdroppers cracking their code.

Day 4

Morning

- Introduction to Complexity theory (Why do we think factoring and the discrete logarithm problems are hard?)
- Showing of *Sneakers*

Afternoon: Oral Exams

One on one oral exams. Other students practice Diffie-Hellman.

Day 5

Wrap-up and goodbye.