Mathematical Cryptography

Joshua Holden

http://www.rose-hulman.edu/~holden

Rose-Hulman Institute of Technology

Goals

- “Cool” way of introducing mathematics and CS theory
- Practical knowledge
- Societal impact
- Coordinate the goals!

MA/CSSE 479

- Cross-listed; sometimes team-taught
- Most students CS (SE?) majors
- Prerequisites
  - One quarter Discrete Mathematics
  - Two quarters Computer Science
- Elective
  - Frequently used by CS majors as math elective

Coordinating Theory and Practice

Theory	Algorithms
modular arithmetic	shift ciphers
modular inverses	affine ciphers
ciphertext cryptanalysis	letter-frequency attacks
block ciphers	Hill cipher
known-plaintext attacks	Hill cipher attacks
perfect secrecy	one-time pad

Coordinating Theory and Practice 2

Theory	Algorithms
confusion and diffusion	S-DES and DES
chosen-text attacks	differential cryptanalysis
finite fields	S-AES and AES
public key systems	Merkle's Puzzles
Fermat's Little Theorem	Pohlig-Hellman
Euler's Theorem	RSA
key exchange	Diffie-Hellman
"hard problems"	factoring and DL

Coordinating Theory and Practice 3

Theory	Algorithms
digital signatures	RSADS
masking and nonces	ElGamal, DSS
elliptic curves	ECCDH, ECCEG

Philosophy

- Fast-moving field
- Broad principles more important than technical details
- Serious mathematical and theoretical content
  - Some proofs but not too many
- Overview of many topics

Materials

- Mathematical and technical aspects
  - Need extra mathematical background
  - William Stallings. *Cryptography and Network Security: Theory and Practice*. Prentice Hall, 2002.
  - Handouts and websites

More Materials

- Cryptography and society
  - Readings and discussions
  - Two-minute essays
  - Steven Levy. *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age*. Penguin Books, 2002.
  - Rather provocative tone!

Other features of the course

- Lectures balanced with in-class exercises
- “Inspired by math” and “inspired by CS” homework
- Choice of homework on “point system”
- Simplified algorithms
- Student presentations on current literature
- Student research proposal
- Extra topics