Last updated on November 24, 2016

Curriculum Vitae

Joshua Brandon Holden

Department of Mathematics
Rose-Hulman Institute of Technology
5500 Wabash Avenue
Terre Haute, IN 47803-3999

E-mail:
`holden@rose-hulman.edu`
Web page:
`http://www.rose-hulman.edu/~holden`

Education

- A.B., Harvard University, 1992
- A.M., Brown University, 1994
- Ph.D., Brown University, 1998 (requirements completed Sept. 1997)

Employment

Brown University Research Assistant / Departmental Computer Coordinator, 1992–1994.
Teaching Assistant / Research Assistant, 1994–1997.

University of Massachusetts at Amherst Visiting Assistant Professor (Postdoctoral), 1997–1999.

Duke University Assistant Teaching Professor (Postdoctoral), 1999–2001.

Rose-Hulman Institute of Technology Assistant Professor, 2001–2007.
Associate Professor, 2007–2014.
Full Professor, 2014–present.

Professional Societies

Member of Mathematical Association of America (MAA), Association for Women in Mathematics (AWM).

Contents

Honors and Awards

- Honorary Member of Upsilon Pi Epsilon (International Honor Society for the Computing and Information Disciplines), inducted Fall 2008.
- Best Paper Submitted to the ME Division, American Society for Engineering Education Annual Conference and Exposition, 2005. (With Richard Layton, Tina Hudson and Laurence D. Merkle.)

Research Activities

Research Specialty

Number Theory and Cryptography, in particular computational and algebraic number theory and applications

Dissertation

"On the Fontaine-Mazur Conjecture for number fields and an analogue for function fields", advised by Michael Rosen

Research Publications

(Unpublished papers are available on the web at `<http://www.rose-hulman.edu/~holden/Preprints>` or at the `<http://arXiv.org>` preprint archive.)

- Irregularity of prime numbers over real quadratic fields. In: *Algorithmic number theory: third international symposium; proceedings*, no. 1423 in Springer Lecture Notes in Computer Science, Springer-Verlag, 1998.
- Comparison of Algorithms to Calculate "Quadratic Irregularity" of Prime Numbers. In: *Proceedings of the Conference on The Mathematics of Public-Key Cryptography*, June 12–17, 1999, Fields Institute, Toronto.
- On the Fontaine-Mazur Conjecture for number fields and an analogue for function fields. *Journal of Number Theory*, 81:16–47, 2000.
- Comparison of algorithms to calculate quadratic irregularity of prime numbers. *Mathematics of Computation*, 71:863–871, 2002.
- Fixed Points and Two-Cycles of the Discrete Logarithm. In: *Algorithmic number theory: fifth international symposium; proceedings*, 405–415, no. 2369 in Springer Lecture Notes in Computer Science, Springer-Verlag, 2002.
- Notes on an analogue of the Fontaine-Mazur conjecture. With Jeffrey D. Achter. *Journal de Théorie des Nombres de Bordeaux*, 15:627–637, 2003.
- Distribution of Values of Real Quadratic Zeta Functions. In: *Unusual Applications of Number Theory*, no. 64 in DIMACS: Series in Discrete Mathematics and Theoretical Computer Science, AMS, 2004.

- Abelian varieties over finite fields with a specified characteristic polynomial modulo ℓ. *Journal de Théorie des Nombres de Bordeaux*, 16:173–178, 2004.
- First-hit analysis of algorithms for computing quadratic irregularity. *Mathematics of Computation*, 73:939–948, 2004.
- New Conjectures and Results for Small Cycles of the Discrete Logarithm. With Pieter Moree. In: *High Primes and Misdemeanours: Lectures in honour of the 60th birthday of Hugh Cowie Williams*, 245–254, no. 41 in Fields Institute Communications, AMS, 2004.
- Distribution of the Error in Estimated Numbers of Fixed Points of the Discrete Logarithm. *Communications in Computer Algebra*, 38:111–118, 2004.
- Some Heuristics and Results for Small Cycles of the Discrete Logarithm. With Pieter Moree. *Mathematics of Computation*, 75:419–449, 2006.
- Mapping the Discrete Logarithm. With Daniel R. Cloutier. *Involve*, 3:197–213, 2010.
- Counting Fixed Points, Two-Cycles, and Collisions of the Discrete Exponential Function using p-adic Methods. With Margaret M. Robinson. *Journal of the Australian Mathematical Society*, 92: 163–178, 2012. (Special issue in memory of Alf van der Poorten)

Research Talks

Slides for some of these talks may be found at `<http://www.rose-hulman.edu/~holden/Preprints>`.

- "Arithmetic Duality Theorems and the Birch and Swynnerton-Dyer Conjecture", Topic Examination, Brown University, March 15, 1995.
- "On the Fontaine-Mazur Conjecture", Algebra Seminar, Brown University, October 21, 1996.
- "On the Fontaine-Mazur Conjecture", Five College Number Theory Seminar, Amherst College, September 23, 1997.
- "On the Fontaine-Mazur Conjecture", Algebra Seminar, Boston University, October 6, 1997.
- "Calculation of Bernoulli Numbers and Values of Zeta Functions", Theory Seminar, Department of Computer Science, University of Massachusetts, April 28, 1998.
- "Irregularity of Prime Numbers over Real Quadratic Fields", Algorithmic Number Theory Symposium III, Reed College, June 21, 1998.
- "Comparison of Algorithms to Calculate 'Quadratic Irregularity' of Prime Numbers", Conference on the Mathematics of Public Key Cryptography, Fields Institute, June 13, 1999.
- "Online Analysis of Algorithms for Computing Quadratic Irregularity", DIMACS Workshop on Unusual Applications of Number Theory, DIMACS Center, January 14, 2000.
- "First-hit Analysis of Algorithms for Computing Quadratic Irregularity", AMS Special Session on Number Theory, Algorithms, and Cryptography, University of Notre Dame, April 8, 2000.
- "First-hit Analysis of Algorithms for Computing Quadratic Irregularity", Algorithmic Number Theory Symposium IV (poster session), Universiteit Leiden, July 4, 2000.

- “Finiteness Conjectures for Unramified Extensions of Global Fields”, Algebraic Geometry Seminar, Duke University, October 10, 2000.
- “Cryptography and Society: Report on a new course”, MAA Session on Integrating Mathematics and Other Disciplines, Joint Mathematics Meetings, New Orleans, January 12, 2001.
- “Recent results on the computation of zeta values at negative integers”, AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, AMS Central Section Meeting, The Ohio State University, September 22, 2001.
- “Counting Fontaine-Mazur-like function fields”, Algebraic Number Theory Seminar, University of Illinois at Urbana-Champaign, March 14, 2002.
- “Calculation of Bernoulli Numbers and Values of Zeta Functions”, RHIT Math Seminar, May 15, 2002.
- “Fixed points and Two-cycles of the Discrete Logarithm”, Algorithmic Number Theory Symposium V, University of Sydney, Australia, July 9, 2002.
- “Counting Fontaine-Mazur-like function fields”, AMS Special Session on Number Theory and Arithmetic Geometry, AMS Eastern Section Meeting, Northeastern University, October 5, 2002.
- “Parallel Computing in Number Theory”, RHIT Parallel Computing Seminar, October 23, 2002.
- “New Conjectures and Results for Small Cycles of the Discrete Logarithm”, Conference in Number Theory in Honour of Professor H.C. Williams, The Banff Centre, Banff, Alberta, Canada, May 26, 2003.
- “New Conjectures and Results for Small Cycles of the Discrete Logarithm”, RHIT Math Seminar, October 22 and 29, 2003.
- “Mapping the Discrete Logarithm”, Algorithmic Number Theory Symposium VII (poster session), Technische Universität Berlin, July 25, 2006. Joint work with Daniel R. Cloutier.
- “Mapping the Discrete Logarithm”, ISU Math & CS Research Seminar, February 19, 2007. Also given at Illinois Number Theory Fest, University of Illinois at Urbana-Champaign, May 20, 2007. Joint work with Daniel R. Cloutier.
- “A statistical look at maps of the discrete logarithm”, Algorithmic Number Theory Symposium VIII (poster session), Banff Centre, Banff, Alberta, May 18–22, 2008. Joint work with Nathaniel W. Lindle. Abstract published in *Communications in Computer Algebra*, 42:57–59, 2008.
- “Mapping the Discrete Logarithm”, University of Wisconsin at Madison Number Theory Seminar, March 4, 2010. Joint work with Daniel Cloutier, Nathan Lindle, Max Brugger, Christina Frederick, Andrew Hoffman, and Marcus Mace. Also given as three-talk series, Mount Holyoke College Mathematics Department Seminar, March 31, April 4, April 14, 2010.
- “Fixed points and small cycles of the discrete logarithm using p-adic methods”, Illinois Number Theory Conference, University of Illinois at Urbana-Champaign, May 21, 2010. Joint work with Margaret Robinson.
- “Mapping the Discrete Logarithm” MAA Session on Open and Accessible Problems in Number Theory and Algebra, MathFest, Pittsburgh, PA, August 6, 2010. Joint work with Daniel Cloutier, Nathan Lindle, Max Brugger, Christina Frederick, Andrew Hoffman, Marcus Mace, Aaron Blumenfeld, Matthew Friedrichsen, Brian Larson, and Emily McDowell. Also given at Southern Illinois University Carbondale Mathematics Colloquium, February 24, 2011, and RHIT Math Colloquium, March 30, 2011.

- “Exponential Equations and p-adic Numbers”, RHIT Mathematics Department Seminar, September 28, 2011.
- “Fixed points and two-cycles of the self-power map”, Algorithmic Number Theory Symposium X (poster session), University of California, San Diego, July 10, 2012.
- “Variations on a Theme of DLP”, MAA Session on Open and Accessible Problems in Number Theory, MathFest, Madison, WI, August 2, 2012. Joint work with JingJing Chen, Matthew Friedrichsen, Brian Larson, Mark Lotts, Emily McDowell, and Alex Wood.
- “Counting solutions to exponential congruences using p-adic methods”, Session on Experimental Methods in Number Theory, Canadian Mathematical Society Summer Meeting, Halifax, NS, June 7, 2013.
- “Statistics for fixed points of the self-power map”, Algorithmic Number Theory Symposium XII (poster session), GyeongJu, Korea, August 8, 2014. Joint work with Matthew Friedrichsen.
- “Counting fixed points of the singular map $x \mapsto x^{x^n}$ modulo powers of a prime”, Canadian Number Theory Association Conference, Calgary, AB, June 23, 2016.

Educational, Expository, and Artistic Activities

Educational, Expository, and Artistic Publications

- A Comparison of Cryptography Courses. *Cryptologia*, 28 (2), 2004.
- Underwater Model Rockets: An Innovative Design Problem and Competition for Undergraduate Students in Engineering, Math and Science. With Richard Layton, Tina Hudson and Laurence D. Merkle. In: *Proceedings of the 2005 American Society for Engineering Education Annual Conference and Exposition*, 2005. Chosen Best Paper Submitted to the ME Division.
- Underwater Hacker Missile Wars: A Cryptography and Engineering Contest. With Richard Layton, Laurence Merkle, and Tina Hudson. *Cryptologia*, 30:69–77, 2006.
- The graph theory of blackwork embroidery. In: *Making Mathematics with Needlework: Ten Papers and Ten Projects*, AK Peters, 2007.
- Review of *Complexity and Cryptography: An Introduction* by John Talbot and Dominic Welsh. *Cryptologia*, 32:92–97, 2008.
- Math in Your Hands: Integrating the Use of Maple with the Collaborative Use of Wireless Tablet PCs. With Shannon Sexton and Julia Williams. In: *The Impact of Tablet PCs and Pen-based Technology: New Horizons*, Purdue University Press, 2009.
- A Good Hash Function is Hard to Find, and Vice Versa. *Cryptologia*, 37:107-119, 2013.
- Demitasse: A "Small" Version of the Tiny Encryption Algorithm and its Use in a Classroom Setting. *Cryptologia*, 37:74-83, 2013.
- Hyperbolic Tilings with Truly Hyperbolic Crochet Motifs. With Lana Holden. In: *Proceedings of Bridges 2014: Mathematics, Music, Art, Architecture, Culture*, Tessellations Publishing, 2014.
- Modeling Braids, Cables, and Weaves with Stranded Cellular Automata. With Lana Holden. In: *Proceedings of Bridges 2016: Mathematics, Music, Art, Architecture, Culture*, Tessellations Publishing, 2016.

Educational, Expository, and Artistic Talks

Slides for some of these talks may be found at `<http://www.rose-hulman.edu/~holden/Preprints>`.

- "A Tour of Public Key Cryptography (and of Number Theory)", Colloquium, Miami University, October 11, 2001.
- "Modular Arithmetic and Trap Door Ciphers", Mathematics and Computer Science Colloquium, Wabash College, March 27, 2003. Also given as Math Club Invited Speaker, Benedictine University, April 11, 2006, Manchester College Science Seminar, January 11, 2010, Illinois Wesleyan Natural Sciences Colloquium, March 26, 2010.

- “Understanding the Magic: Teaching Cryptography with Just the Right Amount of Mathematics”, MAA Session on Applications of Mathematics in Computer Science, Joint Mathematics Meetings, Phoenix, January 9, 2004.
- “Cryptography and Computer Security for Undergraduates”, Panelist, SIGCSE Technical Symposium on Computer Science Education, Norfolk, Virginia, March 4, 2004.
- “The Graph Theory of Blackwork Embroidery”, Mathematics and Statistics Conference on “Mathematics and Symmetry”, Miami University, October 2, 2004. Also given at AMS Special Session on Mathematics and Mathematics Education in Fiber Arts, Joint Mathematics Meetings, Atlanta, January 7, 2005, and Indiana MAA Section Meeting, Indiana University-Purdue University Fort Wayne, April 1, 2005. Joint work with Lana Holden. Featured talk, AMS “Highlights of the 2005 Joint Mathematics Meetings” web page.
- “Picking up Stitches”, AMS Special Session on Mathematics and Mathematics Education in Fiber Arts, Joint Mathematics Meetings, Atlanta, January 7, 2005. Joint work with Lana Holden.
- “Blackwork Embroidery and Algorithms for Maze Traversals”, Indiana MAA Section Meeting, DePauw University, November 5, 2005. Also given at MAA Session on Mathematics and the Arts, Joint Mathematics Meetings, San Diego, January 9, 2008.
- “Number Theory, Polynomials, and the Advanced Encryption Standard”, MAA Session on Number-Theoretic Applications, Joint Mathematics Meetings, San Antonio, January 12, 2006. Also given at Mathematics and Statistics Conference on “Number Theory”, Miami University, September 29, 2007.
- “How to Paint Your Way out of a Maze”, RHIT Math Seminar, October 18, 2006.
- “Where Does it Hurt? A Teaching Clinic for New and Slightly Used Faculty”, Panelist, RHIT (sponsored by an RHIT Faculty Success Grant), September 13, 2006.
- “Writing Projects and Rubrics in Foundational Mathematics Courses”, MAA Session on Getting Students to Discuss and to Write about Mathematics, Joint Mathematics Meetings, New Orleans, January 6, 2007.
- “Writing Learning Objectives”, with Rich House, August Teaching Workshop, RHIT (sponsored by the RHIT Center for the Practice and Scholarship of Education and an RHIT Faculty Success Grant), August 16, 2007. Also given with Richard Layton, August Teaching Workshop, RHIT (sponsored by the RHIT Center for the Practice and Scholarship of Education), August 21, 2008, and given alone, August Teaching Workshop, RHIT (sponsored by the RHIT Center for the Practice and Scholarship of Education), August 20, 2009, August 20, 2015, and August 18, 2016.
- “The Pohlig-Hellman Exponentiation Cipher as a Bridge between Classical and Modern Cryptography”, Indiana MAA Section Meeting, Manchester College, October 27, 2007. Also given at MAA Session on Cryptology for Undergraduates, Joint Mathematics Meetings, San Diego, January 8, 2008, MAA Session on Fascinating Examples from Combinatorics, Discrete Mathematics, and Graph Theory, MathFest, Madison, WI, August 2, 2008.
- “Braids, Cables, and Cells: An Interesting Intersection of Mathematics, Computer Science, and Art”, Illinois State MAA Section Meeting, Eastern Illinois University, April 4, 2008. Also given at RHIT Math Seminar, March 11, 2009, Indiana MAA Section Meeting, IUPUI, March 21, 2009, Manchester College Computer Science Club, January 18, 2010, Mount Holyoke College Math/Stat Club, April 14, 2010, Notre Dame Math for Everyone Series, November 18, 2010, Valparaiso University Mathematics Colloquium, February 21, 2011. Joint work with Lana Holden.

- Interview on cryptography with Namrita Nandakumar, Jason Bosco, David Appleyard, Rajesh D'monte, and Laura Velez, participants in ThinkQuest International website competition, 2008 (second place in "19 and under" division). Interview available on the web at `http://library.thinkquest.org/07aug/01676/interact`
- "Math in Your Hands: Integrating the Use of Maple with the Collaborative Use of Wireless Tablet PCs", Workshop on the Impact of Pen-Based Technology on Education (poster session), Purdue University, October 16, 2008.
- "Math in Your Hands: Integrating the Use of Maple with the Collaborative Use of Wireless Tablet PCs", Indiana MAA Section Meeting, Rose-Hulman Institute of Technology, October 25, 2008.
- "Teaching the Group Theory of Permutation Ciphers", MAA Session on Cryptology for Undergraduates, Joint Mathematics Meetings, Washington, DC, January 5, 2009.
- "Math in Your Hands: The Use of Tablet PCs and Computer Algebra Systems in a Calculus Classroom", MAA Session on Demos and Strategies with Technology that Enhance Teaching and Learning Mathematics, Joint Mathematics Meetings, Washington, DC, January 6, 2009.
- "Braids, Cables, and Cells: An Intersection of Mathematics, Computer Science, and Fiber Arts", AMS Special Session on Mathematics and Mathematics Education in Fiber Arts, Joint Mathematics Meetings, Washington, DC, January 7, 2009. Joint work with Lana Holden.
- (with Shannon Sexton and Julia Williams) "Math in Your Hands: The Use of Tablet PCs and Computer Algebra Systems in a Calculus Classroom", DyKnow Virtual User Conference, online presentation, July 30, 2009.
- ' "How Do You Say 'Cryptography' in Romanian?" Learning About Integers from Ciphers in Different Languages', MAA Session on Fascinating Examples from Combinatorics, Number Theory, and Discrete Mathematics, MathFest, Portland, OR, August 6, 2009.
- (with Shannon Sexton and Julia Williams) "Math in Your Hands: The Use of Tablet PCs and Computer Algebra Systems in a Calculus Classroom", ICI IT Summit, Taylor University, August 14, 2009.
- (with Shannon Sexton and Julia Williams) "Math in Your Hands: Integrating the Use of Maple with the Collaborative Use of Wireless Tablet PCs", Workshop on the Impact of Pen-Based Technology on Education, Virginia Tech, October 12, 2009.
- "Cognitive taxonomies applied to learning", August Teaching Workshop, RHIT (sponsored by the RHIT Center for the Practice and Scholarship of Education), August 19, 2010.
- "A Good Hash Function is Hard to Find, and Vice Versa", Indiana MAA Section Meeting, Indiana Wesleyan University, April 9, 2011. Extended version given as Math Club Invited Speaker, Benedictine University, April 26, 2013.
- "Laboratory-based writing activities in an Engineering Statistics course", MAA Session on Novel Ways to Incorporate Writing Into Mathematics Classes, MathFest, Lexington, KY, August 6, 2011.
- "Supporting Faculty Projects: Grant Funding on Campus", Panelist, RHIT Learning and Assessment Forum, September 15, 2011.
- "Braids, Cables, and Cells: Modeling Art and Craft with Mathematics and Computer Science", MAA Session on Arts and Mathematics, Together Again, Joint Mathematics Meetings, Boston, MA, January 5, 2012. Also given as Invited Plenary Talk, Illinois MAA Section Meeting, Illinois State University,

March 30, 2012, at Grand Valley State University Mathematics Seminar, April 4, 2012, and as INMAA College Visitors Program Invited Speaker, Purdue University, April 7, 2016. Joint work with Lana Holden.

- "An Interactive Tour of Public Key Cryptography (and of Number Theory)", Invited Workshop, Illinois MAA Section Meeting, Illinois State University, March 30, 2012. Also given as Invited Workshop at Indiana MAA Section Meeting, Indiana University-Purdue University Fort Wayne, April 5, 2014.
- "Stitching Graphs and Painting Mazes: Problems in Generalizations of Eulerian Walks", MAA Session on Open and Accessible Problems in Combinatorics and Graph Theory, MathFest, Madison, WI, August 3, 2012. Joint work with Lana Holden.
- "Rose-Hulman Institute of Technology Uses Maple to Improve Learning for Two Thousand Students", User Case Study in *Bring Learning to Life*, Maplesoft, January 2013.
- "Granny's Not So Square, After All: Hyperbolic Tilings with Truly Hyperbolic Crochet Motifs", AMS Special Session on Mathematics and Mathematics Education in Fiber Arts, Joint Mathematics Meetings, Baltimore, MD, January 15, 2014. Also given at Bridges Conference on Mathematics, Music, Art, Architecture, Culture, Gwacheon National Science Museum, Seoul, Korea, August 17, 2014. Joint work with Lana Holden.
- "Why Induction Is Like Ice Cream: Writing About Analogies in Discrete Mathematics Courses", Themed Contributed Paper Session on Improving Undergraduate Math Writing, MathFest, Washington, DC, August 5, 2015.
- "Reflective activities in Calculus: Using short writing exercises to improve metacognition and self-assessment", MAA Session on Contemplative Pedagogy and Mathematics, Joint Mathematics Meetings, Seattle, WA, January 8, 2016.
- "A Short Tour of Public-Key Cryptography from the 1970's to Today", Kappa Mu Epsilon Induction Ceremony Invited Speaker, Dominican University, April 17, 2016.
- "Modeling Braids, Cables, and Weaves with Stranded Cellular Automata", Bridges Conference on Mathematics, Music, Art, Architecture, Education, Culture, University of Jyväskylä, Jyväskylä, Finland, August 8, 2016. Joint work with Lana Holden.

Curriculum Development

Summer 1996; Spring 1997 Obtained grants for, developed curriculum for, and team-taught new course in "Calculus and Its History" at Brown University in cooperation with Prof. Kim Plofker of the Brown History of Mathematics Department. Used "historically informed" pedagogy to teach calculus.

Summer and Fall 2000 Obtained grants for, developed curriculum for, and taught new course in "Cryptography and Society" at Duke University. Seminar-style introduction to the techniques of modern cryptography and the impact on society of their widespread use.

Summer 2000–present Designed web-based learning modules for the Connected Curriculum Project including:

- Mathematica Tutor (with Lang Moore, David Smith, and Jim Tomberg). Available on the web at `<http://www.math.duke.edu/education/ccp/materials/linalg/mmatutor/index.html>`.

- Maple Tutor (Maple 10 and higher) (with Lang Moore, David Smith, and Jim Tomberg). Available on the web at <http://www.math.duke.edu/education/ccp/materials/mvcalc/javamaptutor/index.html>.
- Linear Filters. Available on the web at <http://www.math.duke.edu/education/ccp/materials/linalg/linfilters/index.html>.
- Introduction to the Mathematics of Ciphers. In review.
- Damping and Resonance Investigations Using Laplace Transforms. In review.
- Using Riemann Sums to Estimate Areas, Volumes, and Lengths of Arc. In preparation.

Spring 2002, Spring 2003, Spring 2004 Developed curriculum for and taught course in "Cryptography" at RHIT. (Team-taught in 2002 and 2003 in cooperation with Prof. David Mutchler of the RHIT Computer Science Department.)

Spring 2004 Developed curriculum for and taught course in "Abstract Algebra" at RHIT.

Spring 2005 Developed curriculum for and taught course in "Topics in Discrete Mathematics: p-adic numbers" at RHIT.

Winter 2005–2006 Developed curriculum for and taught course in "Topics in Mathematics: Galois Theory" at RHIT.

Fall 2008 Developed new technology for integrating the use of Maple with the use of wireless Tablet PCs and DyKnow Vision software and implemented it in Calculus III, revising course as appropriate.

Spring 2009 Developed curriculum for and taught course in "Topics in Discrete Mathematics: Quantum Computing" at RHIT.

January 2010 Developed curriculum for and taught new course on "Codes, Ciphers and Society", Manchester College.

May 2010 Developed curriculum for and taught new course on "Mathematical World: Mathematics of Secret Messages", Goshen College.

Spring 2011 Developed computer laboratory modules for Engineering Statistics I.

Winter 2011–2012 Developed curriculum for and taught course in "Topics in Number Theory: Quadratic Field Cryptography" at RHIT.

Grants

- Wayland Collegium Course Development Grant for "Calculus and Its History", Brown University (joint application with Kim Plofker), Summer 1996.
- Curricular Development Grant for "Calculus and Its History", Brown University (joint application with Kim Plofker), Spring 1997.
- Recognition Award for the Integration of Research and Education (RAIRE) Grant for curriculum development for "Cryptography and Society", Duke University, Summer 2000.
- Undergraduate Mathematics Conference Grant for the RHIT Undergraduate Mathematics Conference, administered by the Mathematical Association of America, supported by grant DMS-0241090 from the National Science Foundation, 2005–2006.

- Senior Investigator, Research Experiences for Undergraduates (REU) Site Grant from National Science Foundation in the research area of "Discrete Logarithms" (joint application with Kurt Bryan and David Finn, Co-PI's), National Science Foundation grant DMS-0352940, 2007–2009 funding cycle.
- Principal Investigator, National Science Foundation group travel grant for the Eighth Algorithmic Number Theory Symposium ANTS-VIII, (joint application with Jonathan Sorenson, Co-PI), DMS-0801165, 2008–2009.
- Investigator, Project to Implement Tablet PCs and DyKnow Vision Software into a Course, RHIT, Summer 2008.
- Rose-Hulman Summer Professional Development Grant, Summer 2009.
- Mount Holyoke College Hutchcroft Fund Visiting Scholar, April 2010.
- Principal Investigator, Research Experiences for Undergraduates (REU) Site Grant from National Science Foundation, DMS-1003924, 2010–2012 funding cycle.
- Rose-Hulman Summer Professional Development Grant, Summer 2015.
- Investigator, Faulty Learning Community for Consortium to Promote Reflection in Engineering Education, RHIT, Summer 2015.

Workshops Attended

- Project NExT-IN (New Experiences in Teaching — Indiana) Workshop, MAA Indiana Section Meeting, Butler University, March 28, 2003.
- Rethinking the Design of Presentation Slides, conducted by Michael Alley, RHIT (sponsored by the RHIT Center for the Practice and Scholarship of Education), March 19, 2011.
- Midwest Moodle Moot, Goshen College, July 25–27, 2012.
- Enhancing Intercultural Sensitivity in the Classroom and on Campus, conducted by Kay Coder, RHIT (sponsored by the RHIT Center for Diversity), March 23, 2013.
- New Directions for Mathematics Research Experiences for Undergraduates, Mount Holyoke College, June 21-22, 2013.
- Intercultural Competence Workshop I, RHIT (sponsored by the RHIT Center for Diversity), October 4, 2013.
- Intercultural Competence Workshop II, RHIT (sponsored by the RHIT Center for Diversity), January 26, 2015.
- Intercultural Competence Workshop III, RHIT (sponsored by the RHIT Center for Diversity), January 22, 2015.
- Attracting and Retaining Women in Science, Engineering, and Mathematics, RHIT (sponsored by the RHIT Center for Diversity), March 18, 2015.

Teaching Experience

Syllabi and materials used in many of these courses may be found on my web site.

Pre-calculus and Introductory Calculus Brown University, Rose-Hulman Institute of Technology

Used Eric Mazur's "Peer Instruction" and other collaborative learning techniques.

Calculus I–III Brown University, University of Massachusetts, Duke University, Rose-Hulman Institute of Technology

Teaching techniques used include "Peer Instruction", collaborative techniques, computer algebra system labs, graphing calculator labs, written projects, computer algebra system demonstrations, and reflective activities.

Differential Equations I–II Rose-Hulman Institute of Technology

Teaching techniques used include "Peer Instruction", collaborative techniques, computer algebra system labs, and computer algebra system demonstrations.

Discrete and Combinatorial Algebra I–II Rose-Hulman Institute of Technology

Teaching techniques used include "Peer Instruction", collaborative learning techniques, written projects, computer demonstrations, and reflective activities.

Engineering Statistics I Rose-Hulman Institute of Technology

Teaching techniques used include "Peer Instruction", collaborative learning techniques, computer labs, and computer demonstrations.

Introduction to Probability Rose-Hulman Institute of Technology

Teaching techniques used include "Peer Instruction", collaborative learning techniques, computer labs, and computer demonstrations.

Linear Algebra Duke University, Rose-Hulman Institute of Technology

Used Maple labs and demonstrations, and writing, programming, and student research projects.

Undergraduate Number Theory University of Massachusetts, Rose-Hulman Institute of Technology

Integrated writing, computer programming, and student research projects (written and/or oral) into the syllabus, as well as discussions of current research.

Undergraduate Number Theory Seminar Duke University

Roughly half the course lecture-based, half based on student presentations on various topics. Student written projects included answers to questions from other students.

Undergraduate Abstract Algebra I University of Massachusetts

Integrated writing, computer programming, and student research projects into the syllabus, as well as discussions of current research.

Undergraduate Abstract Algebra Rose-Hulman Institute of Technology

Developed curriculum for and taught new course.

Integrated student research projects (written and oral) into the syllabus, as well as discussions of current research.

Cryptography Rose-Hulman Institute of Technology

Developed curriculum for and team-taught course in cooperation with Prof. David Mutchler of the RHIT Computer Science Department.

Integrated writing, computer programming, and student research projects and presentations into the syllabus, as well as discussions of current research.

Theory of Computation Rose-Hulman Institute of Technology

Design and Analysis of Algorithms Rose-Hulman Institute of Technology

Topics in Discrete Mathematics Rose-Hulman Institute in Technology

Topic for Spring 2005 was p-adic numbers. Developed curriculum for and taught course.

Topic for Spring 2009 and Spring 2014 was quantum computing. Developed curriculum for and taught course.

Integrated discussions of current research into the syllabus.

Topics in Number Theory Rose-Hulman Institute in Technology

Topic for Winter 2005–2006 was Galois Theory. Developed curriculum for and taught course. Also taught Winter 2010–2011.

Topic for Winter 2011–2012 was Quadratic Field Cryptography. Developed curriculum for and taught course.

Integrated frequent student presentations of material into the syllabus, as well as discussions of current research.

Contemporary Mathematical Problems Rose-Hulman Institute in Technology

Centered syllabus around classroom discussions, oral presentations, and written papers.

"Calculus and Its History" Brown University

Developed curriculum for and team-taught new course in cooperation with Prof. Kim Plofker of the Brown History of Mathematics Department.

Used "historically informed" pedagogy to teach calculus. Included student term papers as well as problem sets.

History of Mathematics University of Massachusetts

Supervised independent study.

"Cryptography and Society" Duke University

Developed curriculum for and taught new course.

Seminar-style introduction to the techniques of modern cryptography and the impact on society of their widespread use. Included student short essays and term papers as well as problem sets and computer experience. Guest lecturers also used.

Mathematics Seminar Rose-Hulman Institute of Technology

Responsible for coordinating student attendance and talks at department seminar. Worked with students to develop 50 minute-long mathematical talks and supervised their presentation.

Problem Solving Seminar Rose-Hulman Institute of Technology

Student-driven presentation of solutions to contest-type problems. Incorporated written and oral presentations and team contests.

Senior Thesis Rose-Hulman Institute of Technology

Supervised senior theses in number theory for Mathematics and Computer Science and Software Engineering Departments.

Topics in Combinatorics Rose-Hulman Institute of Technology

Supervised independent study.

Number Fields I and II Rose-Hulman Institute of Technology

Supervised independent study.

"Codes, Ciphers and Society" Manchester College

Developed curriculum for and taught new course.

An intensive three-week, 45-hour interdisciplinary course introducing students to the techniques of modern cryptography and the impact on society of their widespread use. Included student short essays and class discussion as well as problem sets and computer experience.

"Mathematical World" Goshen College

Topic was the Mathematics of Secret Messages. Developed curriculum for and taught new course.

An intensive three-week, 45-hour general education course introducing students to the mathematics behind classical and modern cryptography. Also included some discussion on the impact on society of the use of cryptography and digital communications. Included class discussions and a term paper as well as problem sets and computer experience.

Number Theory and Fractals Supervised independent study.

Advising and Student Projects

- Committee member, Master's Thesis on high-speed digital multiplierless FIR filters, Himanshu Narayana, Electrical and Computer Engineering department, 2003–2004.
- Advisor, Senior Thesis on "Mapping the Discrete Logarithm", Daniel Cloutier, Computer Science and Software Engineering department, 2004–2005.
- "Mapping the Discrete Logarithm", presented by Daniel Cloutier at AMS Special Session on Number Theory, AMS Central Section Meeting, Notre Dame University, April 9, 2006.
- Mathematics major advisor, graduating class of 2008.
- Group director, Rose-Hulman Research Experience for Undergraduates (REU) in Mathematics, Summer 2007. Supervised the following projects, which were presented at the Indiana Summer Undergraduate Mathematics Conference, Wabash College, July 26, 2007, and are also available as RHIT Technical Reports:

  - "The Discrete Logarithm Problem and Ternary Functional Graphs", Max F. Brugger and Christina A. Frederick. Also presented at MAA Undergraduate Poster Session, Joint Mathematics Meetings, San Diego, January 8, 2008, and published in the *Rose-Hulman Undergraduate Mathematics Journal*, Vol. 8, No. 2, 2007.
  - "Isomorphisms of Elliptic Curves over Extensions of Finite Fields", Matthew Niemerg. Also presented at the Illinois State MAA Section Meeting, Eastern Illinois University, April 5, 2008, and at the Rose-Hulman Undergraduate Mathematics Conference, April 11, 2008.
  - "Structural Properties of the Mapping $g^x \to g^{x^2}$", Philip Brunetti.

- Advisor, Senior Thesis on "A Statistical Look at Maps of the Discrete Logarithm", Nathaniel W. Lindle, Computer Science and Software Engineering department, 2007–2008.
- "A Statistical Look at Maps of the Discrete Logarithm", presented by Nathaniel W. Lindle at the Rose-Hulman Undergraduate Mathematics Conference, April 12, 2008.
- Committee member, Senior Thesis, Max Brugger, Mathematics Department, Oregon State University, 2007–2008.
- Committee member, Senior Thesis, Robert Lemke-Oliver, Mathematics Department, RHIT, 2007–2008.
- Committee member, Senior Thesis, Ian Rogers, Mathematics Department, RHIT, 2007–2008.
- Advisor, Senior Thesis on "The Collatz Conjecture", Amanda Vessey, Mathematics Department, RHIT, 2008–2009.
- Committee member, Senior Thesis, Jordan Phegley, Mathematics Department, RHIT, 2008–2009.
- Committee member, Senior Thesis, Jeremy Schendel, Mathematics Department, RHIT, 2008–2009.
- Group director, Rose-Hulman Research Experience for Undergraduates (REU) in Mathematics, Summer 2009. Supervised the following projects, which were presented at the Indiana Undergraduate Research Conference, Indiana University, July 23, 2009 and are also available as RHIT Technical Reports:
  - "The Digraph of the Square Mapping on Elliptic Curves", Katrina Glaeser.
  - " Statistical Investigation of Structure in the Discrete Logarithm", Andrew Hoffman. Also published in the *Rose-Hulman Undergraduate Mathematics Journal*, Vol. 10, No. 2, 2009.
  - "Symmetries and Automorphisms in Power Digraphs Modulo n", Joseph Kramer-Miller.
  - "Mapping the Discrete Logarithm Problem over Composite Moduli", Marc Mace.
- Group director, Rose-Hulman Research Experience for Undergraduates (REU) in Mathematics, Summer 2010. Supervised the following projects, which were presented at the Indiana Undergraduate Research Conference, Indiana University, July 29, 2010 and are also available as RHIT Technical Reports:
  - "Discrete Logarithms on Elliptic Curves", Aaron Blumenfeld. Also Also published in the *Rose-Hulman Undergraduate Mathematics Journal*, Vol. 12, No. 1, 2011.
  - "Structure and Statistics of the Self-Power Map", Matthew Friedrichsen, Brian Larson, and Emily McDowell. Also published in the *Rose-Hulman Undergraduate Mathematics Journal*, Vol. 11, No. 2, 2010.

- Advisor, Senior Thesis on "Algebraic Solutions to Overdefined Systems and Applications to Cryptanalysis", Eric Crockett, Computer Science and Software Engineering department, 2010–2011.
- "Algebraic Solutions to Overdefined Systems and Applications to Cryptanalysis", presented by Eric Crockett at the Rose-Hulman Undergraduate Mathematics Conference, March 26, 2011.
- Mathematics major advisor, graduating class of 2014.
- Advisor, Senior Thesis on "Counting Solutions to Discrete Non-Algebraic Equations Modulo Prime Powers", Abigail Mann, Mathematics Department, 2015-2016.
- "Counting Solutions to Discrete Non-Algebraic Equations Modulo Prime Powers", presented by Abigail Mann at the Rose-Hulman Undergraduate Mathematics Conference, April 23, 2016.
- Advisor, Senior Thesis on "Statistical Analysis of Binary Functional Graphs of the Discrete Logarithm", Mitchell Orzech, Mathematics Department, 2015-2016.
- "Statistical Analysis of Binary Functional Graphs of the Discrete Logarithm", presented by Mitchell Orzech at the Rose-Hulman Undergraduate Mathematics Conference, April 23, 2016.
- Group director, Rose-Hulman Research Experience for Undergraduates (REU) in Mathematics, Summer 2011. Supervised the following projects, which were presented at the Indiana Undergraduate Research Conference, Indiana University, July 27, 2011 and are also available as RHIT Technical Reports:
  - "Structure and Randomness of the Discrete Lambert Map", JingJing Chen and Mark Lotts.
  - "The Elliptic Curve Discrete Logarithm and Functional Graphs", Christopher Evans.
  - "The Square Discrete Exponentiation Map", Alex Wood.
- Committee chair, Master's Thesis in Cryptography, Jay Dial, Program in Systems Engineering and Management, International, Spring–Summer 2013.
- Group co-director, Mount Holyoke College and Rose-Hulman joint summer undergraduate research program in Mathematics, Summer 2014. Co-supervised the following projects, which were presented at the REU Mini-Conference, Yale University, July 25, 2014 and are also available as Mount Holyoke College and/or RHIT Technical Reports:
  - "Collisions of the discrete Lambert map", Yu Liu.
  - "Deconstructing the Welch equation using p-adic methods", Abigail Mann and Adelyn Yeoh. Also published in the *Rose-Hulman Undergraduate Mathematics Journal*, Vol. 16, Issue 1, 2015.
  - "The discrete Lambert map", Anne Waldo and Caiyun Zhu, also published in the *Rose-Hulman Undergraduate Mathematics Journal*, Vol. 16, Issue 2, 2015.

Service Activities

Institutional Service

Institute Offices

- Faculty Champion for CMS Transition to Moodle, 2011–2014.

Departmental Offices

- Associate Department Head, 2015–2017.

Institute Committees

- Member, Visual and Performing Arts Committee, Rose-Hulman Institute of Technology, 2001–2002.
- Member, Quality of Education Committee, Rose-Hulman Institute of Technology, 2002–2003.
- Member, Academic Computing/Technology Committee, Rose-Hulman Institute of Technology, 2003–2007.
- Secretary, Academic Computing Committee, Rose-Hulman Institute of Technology, 2003–2004.
- Chair, Academic Technology Committee, Rose-Hulman Institute of Technology, 2004–2006.
- Member, Faculty Affairs Committee, Rose-Hulman Institute of Technology, 2007–2009.
- Member, Committee on Potential Academic Technologies, Rose-Hulman Institute of Technology, 2008–2009 and 2010–2017.
- Member, Course Management Software Faculty Team, Rose-Hulman Institute of Technology, 2003–2004.
- Member, Commission on the Assessment of Student Outcomes, Rose-Hulman Institute of Technology, 2005–2006.
- Member, High Performance Computing (formerly Parallel Computing) Steering Committee, Rose-Hulman Institute of Technology, 2005–2008 and 2010–2013.
- Member, Imaging Systems Faculty Cluster, 2005–2010.
- Member, High Performance Computing (formerly Parallel Computing) Faculty Cluster, 2005–2014.
- Member, Academic Computing Review Commission, 2006–2007.
- Member, Tablet and Lightweight PC Study Team, 2007–2008.

Departmental Committees

- Member, ad hoc subcommittee of the Undergraduate Affairs Committee to choose textbook for Calculus with Computers, University of Massachusetts Department of Mathematics, 1998.
- Member, Calculus Committee, Duke University Mathematics Department, 1999–2001.
- Member, Library and Publications (formerly Library) Committee, Rose-Hulman Institute of Technology Mathematics Department, 2001–2004, 2011–2014, 2015–2016.
- Member, RHIT High School Contest Committee, Rose-Hulman Institute of Technology Mathematics Department, 2002–2005.
- Co-chair, RHIT High School Contest Committee, Rose-Hulman Institute of Technology Mathematics Department, 2003–2004.
- Chair, Brochure Committee, Rose-Hulman Institute of Technology Mathematics Department, 2002–2004.
- Member, Computing Environment Committee, Rose-Hulman Institute of Technology Mathematics Department, 2003–2007, 2008–2009, 2011–2014.
- Member, Curriculum Committee, Rose-Hulman Institute of Technology Mathematics Department, 2003–2005, 2011–2012.
- Member, Mathematics Concentration Curriculum Development Group, Rose-Hulman Institute of Technology Mathematics Department, 2002–2017.
- Chair, Mathematics Concentration Curriculum Development Group, Rose-Hulman Institute of Technology Mathematics Department, 2004–2005, 2011–2012.
- Member, Discrete Applied Mathematics Concentration Curriculum Development Group, Rose-Hulman Institute of Technology Mathematics Department, 2002–2017.
- Member, Assessment and Testing Curriculum Development Group, Rose-Hulman Institute of Technology Mathematics Department, 2007–2009.
- Member, Four-day Calculus Committee, Rose-Hulman Institute of Technology Mathematics Department, 2004–2005.
- Member, Hiring Committee, Rose-Hulman Institute of Technology Mathematics Department, 2006–2007, 2015–2017.
- Member, Alfred R. Schmidt Freshman Mathematics Competition Committee, Rose-Hulman Institute of Technology Mathematics Department, 2006–2009, 2011–2013, 2014–2016.
- Member, Student Recruiting Committee, Rose-Hulman Institute of Technology Mathematics Department, 2008–2014.
- Chair, Department Honors and Awards Committee, Rose-Hulman Institute of Technology Mathematics Department, 2013–2014.
- Chair, Committee on the Rose-Hulman Undergraduate Mathematics Conference, 2015–2017.

Other

- Webmaster for Five College Number Theory Seminar, 1997–1999.
- Led session for student laptop orientation, Rose-Hulman Institute of Technology, each Fall, 2002–2013.
- Co-organizer, RHIT Undergraduate Mathematics Conference, 2005–2006.
- Advisor, Rose-Hulman Macintosh Interest Group, 2003–2006.
- Advisor, Unity, 2007–Fall 2009.
- Captain, RHIT Faculty/Staff Intramural Soccer Team ("The Dinosaurs"), 2005–2006. Co-captain, 2015.
- Speaker, RHIT Student Leaders' Luncheon on the theme "Diversity Matters", January 17, 2007.
- Photo Archivist, Rose-Hulman Institute of Technology Mathematics Department, 2007–2009.
- Faculty/Staff Representative to the RHIT Intramural Council, 2011–2014.
- Captain, RHIT Faculty/Staff Volleyball Team ("FAST"), 2011–12
- Maintainer, Mathematical Sciences Technical Report Series, Rose-Hulman Institute of Technology Mathematics Department, 2012–present.
- Captain, RHIT Faculty/Staff/Math/CSSE Intramural Ultimate Frisbee Team ("SECS y Dinosaurs"), 2009, 2011, and 2013–2016.
- Advisor, Juggling Club, 2012–present.
- Advisor, Jewish Culture Club, 2015–present.

Professional Service

Professional Organizations

- Member, Nominating Committee, Indiana MAA Section, 2009–2012.
- Chair, Nominating Committee, Indiana MAA Section, 2011–2012.
- Consultant for the 2010 Cohort, Project NExT, 2010–present
- Online Editor, Special Interest Group of the MAA on Mathematics and the Arts, 2012–present.
- Judge, AWM/MfA High School Essay Contest, 2012, 2013, 2016
- Public Information Officer, Indiana MAA Section, 2014–present.
- Mentor, MAA Early Career Mathematician Mentoring Network, 2015–present.

Conferences

- Co-organizer, AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, AMS Central Section Meeting, Indiana University, April 4–6, 2003.
- Judge, Undergraduate Student Poster Session, Joint Mathematics Meetings, Phoenix, January 9, 2004.
- Member, Design Contest Planning Committee, Midwestern Undergraduate Private Engineering Colleges Student Conference, Rose-Hulman Institute of Technology, March 27, 2004.
- Co-organizer, Graduate Student Workshop, Indiana MAA Section Meeting, Indiana State University, April 3, 2004.
- Judge, Undergraduate Student Poster Session, Joint Mathematics Meetings, New Orleans, January 7, 2007.
- Conductor, Early Music Sing, Joint Mathematics Meetings, New Orleans, January 7, 2007.
- Member, Organizing Committee, Algorithmic Number Theory Symposium VIII, 2006–2008.
- Judge, MAA Student Paper Sessions, MathFest, Madison, WI, July 31, 2008.
- Judge, MAA Student Paper Sessions, MathFest, Portland, OR, August 6, 2009.
- Judge, MAA Student Paper Sessions, MathFest, Pittsburgh, PA, August 5, 2010.
- Judge, MAA Student Paper Sessions, MathFest, Lexington, KY, August 4, 2011.
- Judge, Undergraduate Student Poster Session, Joint Mathematics Meetings, Boston, January 6, 2012.
- Judge, MAA Student Paper Sessions, MathFest, Madison, WI, August 3, 2012.
- Panelist, Project NExT-IN Session on "Publishing Undergraduate Research", MAA Indiana Section Meeting, University of Southern Indiana, October 26, 2013.
- Member, Program Committee, Midstates Conference for Undergraduate Research in Computer Science and Mathematics, Ohio Wesleyan University, November 16, 2013.
- Judge, Undergraduate Student Poster Session, Joint Mathematics Meetings, Baltimore, MD, January 17, 2014.
- Member, Program Committee, Midstates Conference for Undergraduate Research in Computer Science and Mathematics, The College of Wooster, November 15, 2014.
- Judge, MAA Student Paper Sessions, MathFest, Washington, DC, August 7, 2015.
- Panelist, Project NExT-IN Session on "Effectively Incorporating Technology in the Classroom", Indiana MAA Section Meeting, Purdue University North Central, October 17, 2015.
- Judge, Undergraduate Student Poster Session, Joint Mathematics Meetings, Seattle, WA, January 8, 2016.
- Panel Moderator, Project NExT-IN Session on"Alternative Assessment Techniques", Indiana MAA Section Meeting, Franklin College, March 19, 2016.

Publications

- Referee for *Journal of Number Theory*, *Journal of Online Mathematics and its Applications*, *RHIT Undergraduate Mathematics Journal*, *Cryptologia*, *PRIMUS*, *Boletin de la Sociedad Matematica Mexicana*, *Integers*, *Mathematics Magazine*, *Electronic Commerce Research.*
- Editor, *Cryptologia* Editorial Board, Taylor and Francis, 2005–present.
- Editor, *Ball State Undergraduate Mathematics Exchange* Editorial Board, 2008–2014.
- Associate Editor, *Electronic Commerce Research* Editorial Board, Springer, 2015–present.
- Reviewer for *The Internet Encyclopedia*, Hossein Bidgoli, Editor-in-Chief, John Wiley and Sons, 2003.
- Pre-publication reviewer for *Calculus*, Taalman, Brazfield, and Kohn, Houghton Mifflin Company.
- Pre-publication reviewer for Princeton University Press.
- Pre-publication reviewer for Thomson Higher Education.
- Pre-publication reviewer for 12th edition of *Thomas' Calculus*, Pearson Addison-Wesley.
- Pre-publication reviewer for third edition of *Introduction to Computer Theory*, Cohen, John Wiley & Sons, Inc.
- Pre-publication reviewer for *Discrete Math*, by David Barrington, McGraw-Hill.
- Pre-publication reviewer for *Calculus*, Soo Tan, Cengage Learning.
- Pre-publication reviewer for 12th edition of *Thomas' Calculus: Early Transcendentals*, Pearson Addison-Wesley.
- Pre-publication reviewer for *NSDL Timely Teaching* web site.
- Pre-publication reviewer for *Introduction to Cryptography*, Klima and Sigmon, Taylor and Francis.
- Pre-publication reviewer for *Calculus*, Beyers, Pearson.
- Pre-publication reviewer for *Calculus*, Lutzer and Goodwill, Wiley.
- Reviewer for Proceedings of "Dynamics and Numbers", Max Planck Institute for Mathematics.
- Pre-publication reviewer for fourth edition of *Fundamentals of Probability with Stochastic Processes*, Gharamani, CRC Press.

Other

- Assistant Coach, American Regions Mathematics League Team from Indiana, Spring, 2002.
- Supervised Science Fair Project on "The Discrete Logarithm: Finding the trace of the non-primitive case" for Krishan Kumar, student at Vigo South H.S, Winter 2013–Spring 2014. Earned Intel ISEF Student Observer Award at the 2013 Hoosier Science and Engineering Fair. Earned Fourth Place, Indiana Junior Science and Humanities Symposium. Earned Intel ISEF Finalist Award at the 2014 Hoosier Science and Engineering Fair. Earned "Fourth Award" in Mathematical Sciences at the 2014 Intel International Science and Engineering Fair.

- "Mapping the Discrete Lambert", presented by Krishan Kumar at the Rose-Hulman IRC Undergraduate Student Research Symposium, October 25, 2013.
- Supervised Science Fair Project on "Exploring the Alternative El Gamal System" for Chaman Kumar, student at Vigo South H.S., Fall 2014–Spring 2016. Earned Second Place at the 2015 West Central Indiana Regional Region Science and Engineering Fair. Earned Fifth Place, Poster Competition, 2015 Indiana Junior Science and Humanities Symposium. Presented at 2016 Hoosier State Science and Engineering Fair.

Consulting Activities

Consulting Employment

- Cryptography consultant, Vadium Technology, Summer 2003.
- Reader, AP Calculus Exam, Summer 2005, Summer 2006, Summer 2008, Summer 2012, Summer 2013, Summer 2015, Summer 2016
- Contributed homework problems to *Cryptography and Network Security*, Fourth Edition, William Stallings, Prentice-Hall, 2006.
- Rater, RosEPortfolio, Rose-Hulman Institute of Technology, Summer 2007, Summer 2008, Summer 2009, Summer 2012, Summer 2013.

Consulting Publications

- “XOR Convert Phase of the AlphaCipher Key Distribution Protocol”, proprietary document prepared for Vadium Technology, July 24, 2003.