MATHFEST 2002

BURLINGTON, VERMONT AUGUST 1–3, 2002

THE ANNUAL SUMMER MEETING OF THE MATHEMATICAL ASSOCIATION OF AMERICA

THE TWO-DAY SHORT COURSE THE MATHEMATICS OF CRYPTOLOGY

For millennia cryptology and mathematics followed separate paths. Now they are intimately entwined, with cryptology influencing the development of mathematics and vice versa. In this short course we shall visit some of the mathematics that has been stimulated by cryptology, some of the cryptology that has arisen out of mathematical problems, and some of the real-world issues that arise when cryptosystems are actually implemented. Most talks will supplement what is usually found in an undergraduate text on cryptology. The listed talks will be given at the short course. They are listed in alphabetical order by speaker. The actual order will be different. To sign up for this course, go to `www.maa.org` and download the MathFest registration form.

ORGANIZED BY

Carl Pomerance, *Lucent Technologies, Bell Labs*

PART I: TUESDAY, JULY 30, 9:00 AM – 5:00 PM

PART II: WEDNESDAY, JULY 31, 9:00 AM – 5:00 PM

IMPLEMENTING PUBLIC KEY CRYPTOLOGY: THE DEVIL IS IN THE DETAILS
Daniel Bleichenbacher, *Lucent Technologies, Bell Labs*

HOW HARD IS FACTORING?
Carl Pomerance, *Lucent Technologies, Bell Labs*

HOW HARD ARE DISCRETE LOGARITHMS?
Carl Pomerance, *Lucent Technologies, Bell Labs*

ELLIPTIC CURVES AND CRYPTOLOGY
Joe Silverman, *Brown University and NTRU Cryptosystems, Inc.*

LATTICES AND CRYPTOLOGY
Joe Silverman, *Brown University and NTRU Cryptosystems, Inc.*

THE GIVE AND TAKE OF MAKING AND BREAKING CRYPTOSYSTEMS
Mike Szydlo, *RSA Security, Inc.*

TEXTBOOK CRYPTOGRAPHY AND THE REAL WORLD
Mike Szydlo, *RSA Security, Inc.*

COMBINATORIAL CRYPTOGRAPHY AND THE 'TWO SHERIFFS PROBLEM'
Peter Winkler, *Lucent Technologies, Bell Labs*

COMPARISON WITHOUT DISCLOSURE (OR AVOIDING CRYPTOGRAPHY FOR FUN AND PROFIT)
Peter Winkler, *Lucent Technologies, Bell Labs*