Proceedings of Symposia in APPLIED MATHEMATICS

Volume 62

Public-Key Cryptography

American Mathematical Society Short Course January 13–14, 2003 Baltimore, Maryland

Paul Garrett Daniel Lieman Editors



American Mathematical Society

AMS SHORT COURSE LECTURE NOTES Introductory Survey Lectures published as a subseries of Proceedings of Symposia in Applied Mathematics

Proceedings of Symposia in APPLIED MATHEMATICS

Volume 62

Public-Key Cryptography

American Mathematical Society Short Course January 13–14, 2003 Baltimore, Maryland

Paul Garrett Daniel Lieman Editors



Editorial Board

Mary Pugh Lenya Ryzhik Eitan Tadmor (Chair)

LECTURE NOTES PREPARED FOR THE AMERICAN MATHEMATICAL SOCIETY SHORT COURSE PUBLIC-KEY CRYPTOGRAPHY HELD IN BALTIMORE, MARYLAND JANUARY 13–14, 2003

The AMS Short Course Series is sponsored by the Society's Program Committee for National Meetings. The series is under the direction of the Short Course Subcommittee of the Program Committee for National Meetings.

2000 Mathematics Subject Classification. Primary 54C40, 14E20, 14G50, 11G20, 11T71, 11Yxx, 94Axx, 46E25, 20C20.

Library of Congress Cataloging-in-Publication Data

Public-key cryptography / Paul Garrett, Daniel Lieman, editors.

p. cm. — (Proceedings of symposia in applied mathematics ; v. 62)

Papers from a conference held at the 2003 Baltimore meeting of the American Mathematical Society.

Includes bibliographical references and index.

ISBN 0-8218-3365-0 (alk. paper)

1. Computers—Access control—Congresses. 2. Public key cryptography—Congresses. I. Garrett, Paul, 1952– II. Lieman, Daniel, 1965– III. American Mathematical Society. IV. Series.

2005048178

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2005 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights

except those granted to the United States Government.

Copyright of individual articles may revert to the public domain 28 years

after publication. Contact the AMS for copyright status of individual articles.

Printed in the United States of America.

The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability. Visit the AMS home page at http://www.ams.org/

 $10 \ 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1 \qquad 10 \ 09 \ 08 \ 07 \ 06 \ 05$

Contents

Preface	vii
Cryptographic primitives PAUL GARRETT	1
Cryptography in the real world today DANIEL LIEMAN	63
Public-key cryptography and proofs of security NICK HOWGRAVE-GRAHAM	73
Elliptic curves and cryptography JOSEPH H. SILVERMAN	91
Towards faster cryptosystems, I WILLIAM WHYTE	113
Towards faster cryptosystems, II WILLIAM D. BANKS	139
Playing "hide-and-seek" with numbers: the hidden number problem, lattices, and exponential sums	
Igor E. Shparlinski	153
Index	179

Preface

For the Baltimore 2003 meeting of the A.M.S. Daniel Lieman organized an expository and tutorial conference on public-key cryptography for mathematicians. This volume is the collection of papers that grew out of that conference.

By contrast to a number of lower-level introductory texts aimed at undergraduates, and which therefore necessarily dilute discussion of specific cryptographic issues with discussion of elementary mathematics, the aim here was to provide a survey and introduction to public-key cryptography assuming considerable mathematical maturity and considerable general mathematical knowledge. Thus, we hoped to make clearer the cryptographic issues that fall outside the scope of standard or typical mathematics.

The papers are mostly expository, with the mathematical level of the exposition meant to be palatable to experienced mathematicians not already too much acquainted with this subject.

An important part of the context is the extra-mathematical aspect. That is, many motivations and crucial issues for genuine cryptography are difficult or impossible to understood purely in terms of formal algorithmic or other mathematical notions. (And the very validity of that last assertion is a subject of debate.) It is necessary to have some idea of the complications entailed by real-life implementations of cryptographic systems. In particular, and in considerable contrast to formal mathematics, we cannot assume that everyone plays by the rules. Further, indeed, by contrast to most mathematical and scientific research contexts wherein there is no antagonist other than a merely disinterested Nature, the presence of an *active antagonist* is a singular aspect of the practice of cryptography.

Some of the authors of the papers are academic mathematicians, some are professional cryptographers outside academe, and some have been in both situations. All the papers were reviewed for literal correctness and for aptness for our espoused purposes.

Paul Garrett

Index

"academic" constructions, 65 active attacker, 84 AddKey, 19 Adleman, 1 advantage of the algorithm, 80 AES, 16, 18 alphabet, 54 anagrams, 15 anonymity, 63, 68 Arazi's cryptosystem, 170 Arithmetica key exchange, 35 Artin group, 36 asymmetric cipher, 1 Atlantic City algorithm, 10 atmospheric noise, 58 attacks, 171 authentication, 1, 37, 69 authenticity, 63 avalanche effect, 18 avoiding inversions, 132

Bell's theorem, 13 big primes, 26 big random primes, 27 binary symmetric channel, 55 binding an identity, 68 bit commitment schemes, 41 bit operations, 8 bit security, 79, 169, 171 bit security problem, 153 blinded, 143 Blum, 53 Blum-Blum-Shub pRNG, 57 Blum integers, 4 braid group, 36 brute force attacks, 142 ByteSub, 19

canonical height, 103 Carmichael number, 21 CCA1-security, 86 CCA2-secure, 85 CCA2-security, 86 certifiable large primes, 41 certificate, 67 certificate chains, 68 channel, 55, 73 channel capacity, 56 character values HNP, 164 Chinese Remainder Theorem, 20 chord-and-tangent rule, 126 chosen ciphertext security, 84 chosen ciphertext security (CCA1), 85 ciphertext space, 74 class NP, 9 class P, 9 classical efficient algorithms, 75 closest vector problem (CVP), 164 cofactor multiplication, 123 coin flipping over the phone, 41 collision, 168 collision search, 107 common modulus, 5 complexity, 8 compression, 55 compression permutation, 17 computability, 9 computational Diffie-Hellman assumption, 76computing roots, 5 confidentiality, 63 conjugacy problem, 36 continued fractions, 27, 47 Coppersmith's short pad attack, 7 coupon collector's test, 57 Coxeter groups, 36 **CR-HNP**, 163 Cramer-Shoup CCA2-secure encryption scheme, 85 cryptograms, 15 CryptoLib, 170

decay of radioactive isotopes, 58 decisional Diffie-Hellman assumption, 76 decryption, 74 decryption exponent, 3 decryption oracle, 76 decryption step, 4

Deligne, 159 Δ -homogeneously distributed modulo m, 157DES. 16 deterministic pRNGs, 57 /dev/random, 58 /dev/urandom. 58 dictionary attack, 53, 67, 77 differential cryptanalysis, 17 difficulty of factoring, 6 Diffie-Hellman, 1, 114 Diffie-Hellman key exchange, 3, 8, 76, 92 Diffie-Hellman problem, 93 Diffie-Hellman secret key, 153 Digital Signature Scheme, 155 Digital Signature Standard, 38 Diophantine equation, 101 Dirichlet's Theorem, 24 discrepancy, 166 discrete logarithm, 3, 22, 82 discrete logarithm attacks, 147 discrete logarithm problem, 76, 91, 92, 114 discrete logs, 31 discriminant, 94 distillation. 57 Dixon's algorithm, 48 DSA, 116 E-box. 18 eavesdropper, 3 EC-HNP, 161 efficient, 74 Einstein-Podolsky-Rosen, 13 El Gamal, 83 electronic money, 41 electronic voting, 41 ElGamal ciphers, 31 ElGamal encryption, 115 ElGamal signature, 38 elliptic curve, 91, 93, 124 elliptic curve algorithms, 53 Elliptic Curve Discrete Logarithm Problem, 94, 128 elliptic curve DSA, 157 elliptic curves in characteristic 2, 105 Ellis-Cocks-Williamson, 1 encoding step, 4 encryption, 74 encryption exponent, 3 Enigma, 15 ENROOT, 139, 148 entropy, 53, 54 equidistribution, 57 equivalence, 3 Euclidean algorithm, 20 Euler totient function, 4 Euler's criterion, 22 Euler's theorem, 4, 21

Euler-Fermat trick, 43 exhaustive search, 107 expansion permutation, 18 exponential sums, 153, 166 exponential time, 9 Extended Riemann Hypothesis, 25 factor base, 47 factoring, 5 factoring attacks, 1 factorization algorithms, 43 factorization attacks, 146 failure modes, 16 failure rate, 26 faking the key, 146 fast cryptosystems, 139 fast exponentiation, 6 Feistel network, 17 Fermat prime, 3 Fermat pseudoprime base, 21 Fermat's Little Theorem, 21 Fiege-Fiat-Shamir, 40 finite field, 94 Floyd's cycle-detection, 45 forward search attack, 7 futility of trial division, 22 Gaussian normal basis, 134 generic random squares, 47 generic-HNP, 154 genuine randomness, 58 GMP, 22 group law, 91 group law on an elliptic curve, 95 hard-core, 80 hard-core bit, 80 hash functions, 65, 66 hash-function, 167 Hasse, 104 Hastad's broadcast attack, 7 Hensel's lemma, 30 hidden Markov, 55 hidden number problem, 153 HNP. 154 HNP on elliptic curves, 161 HNP over unknown algebraic number fields, 162 "how hard is factoring?", 72 hybrid encryption, 83 identity, 64 i.i.d., 55 index, 22 index calculus, 117, 128 infeasibly large number, 76 information, 53 information leakage, 142 information rate, 56

180

information theory, 56 integrity, 63 introductory texts, 1 Jacobi symbol, 23 Katz, 159 key distribution, 16 key exchange, 1, 36 key generation, 6, 16, 74 key scheduling, 17 knapsack ciphers, 31 knapsack problem, 31 knapsack vector, 32 Koblitz curves, 106 Kolmogoroff complexity, 11 large multiples of a point, 100 Las Vegas algorithm, 10 lattice attacks, 143, 147 lattice basis reduction, 156, 164 lattice basis reduction algorithms, 153 lattice problems, 139 lattices, 164 lava lamps, 58 LCGs, 12 leakage of information, 6 Legendre symbol, 22 Lehmer, 42 Lehmer's continued fraction factorization attack 7 Lenstra, 164 LFSRs. 12 linear complexity, 12 linear congruential generators, 13 linear cryptanalysis, 17 linear feedback shift register, 12 Linux, 59 LLL, Lenstra-Lenstra-Lovasz algorithm, 33 Lovász, 164 low-level tests, 56 LUC cryptosystems, 155 Lucas, 42 Lucifer, 16 malleability, 142 Markov, 55 Mazur, 102 Merkle, 1 message (or plaintext) space, 74 Miller-Rabin, 3, 25 Miller-Rabin strong pseudoprime test, 6 Miller-Rabin test base b, 26 MixColumn, 19 models, 74 Monte Carlo algorithm, 10 multiple anagramming, 15 multiple transmission attacks, 142 mutual-authentication, 69

Naor, 53 Néron, 103 no-biased, 10 non-malleability, 84 non-repudiation, 63 nonce, 167 NP-complete, 9 NP-hard, 9 nth convergent, 27 NTRU, 33, 139 NTRU Public Key Cryptosystem, 139 number field sieve, 53 Nyberg-Rueppel, 155 **OAEP**, 143 Occam's razor, 75 1024-bit RSA, 141 one-time pads, 16 one-way function, 76, 78, 148 optimal extension fields, 134 oracle, 9, 40, 75 OTA, 64 padding, 6 padding schemes, 77, 78 Paillier's scheme, 81 partial disclosure. 7 patents, 124 Perl, 59 permutation ciphers, 15 Pocklington, 42 point at infinity, 94, 127 poker test, 57 Pollard's algorithms, 118 Pollard's p-1, 45Pollard's rho, 6, 44, 119 Pollard's ρ method, 108 Polya, 166 polyalphabetic ciphers, 15 polynomial HNP, 161 polynomial-time algorithms, 8 primality certificate, 41 primality testing, 1 Prime Number Theorem, 24 primitive roots, 22 principal square root, 40 privacy, 63 private key, 4, 65 private-key cipher, 1 pRNG, 57 probabilistic algorithms, 10 probable primes, 25 program (-length) complexity, 11 protocol sketches, 37 pseudoprimes, 25 pseudorandom bits, 164 pseudorandom generators, 171 pseudorandom number generators, 170 public key, 4, 65

public key infrastructure, 87 public key space, 74 public-key cipher, 1 public-key infrastructure (PKI), 68 purification, 57 Purple, 15 quadratic reciprocity, 22 quadratic sieve, 47, 49 quadratic symbol, 22 quantum algorithm, 7 quantum algorithms, 13, 161, 162, 172 quantum channels, 13 quantum computers, 7, 76 quantum particles, 76 quantum teleportation, 13 Rabin, 3, 25 random bits. 3 random numbers, 4 random oracle (model), 76 random oracle model, 76, 86 random primes, 4 randomness, 53 rank, 102 reduction, 3 reductionist view, 75 redundancy, 55 Reingold, 53 RFID security, 71 Riemann Hypothesis, 24 Rijndael, 16, 18 Rivest-Shamir-Adleman, 1 rounds, 17 RSA, 1, 3 RSA cryptosystem, 76 RSA decryption, 22 RSA moduli, 4 RSA modulus, 3 S-boxes, 18 secret key space, 74 secret-sharing schemes, 38 Secure Sockets Layer, 68 security failure, 64 security primitives, 65 semantic security, 7, 79 serial test, 57 server-only authentication, 69 set-up, 3 SHA-1, 86 Shamir, 40 Shamir message passing scheme, 157 Shamir's trick, 131 Shannon's noiseless coding, 55 Shannon's noisy coding theorem, 56 shared secret, 8 ShiftRow, 19 Shor's algorithm, 14

Shub, 53 side channel attacks, 87 Siegel, 103 sieving, 50 sign, 66 signature, 1, 37, 66 small decryption exponent attack, 7 small public exponent attacks, 7 small subgroup attacks, 130 small subgroups, 119 smooth, 45, 47 Solovay-Strassen test, 25 source, 54 sparse polynomial interpolation, 162 **SPIFI**, 139 SPIFI identification scheme, 143 spoofing, 64 square roots modulo primes, 28 square-and-multiply, 6, 21 SSL, 68 statistical randomness, 56 strong modular multiplication, 33 strong pseudoprime base b, 26 subexponential algorithms, 10 subexponential sieve methods, 6 subexponential time algorithm, 108 subkey, 17 substitution boxes, 18 substitution cipher, 15 Sun-Ze, 20 superincreasing, 32 symmetric cipher, 1, 14 T-Approx-HNP, 158 T-CTP-HNP, 159 T-HNP, 156 Tate, 103 Tate pairing, 109 τ -sparse, 144 testing, 162 thresh-hold schemes, 38 timed-release crypto, 158 timing, power attacks, 7 timing/power attacks, 170 TLS, 68 torsion subgroup, 102 trace of Frobenius, 105 Transport Layer Security, 68 trapdoor, 3 trapdoor one-way function, 76 trial division runtimes, 22 tripartite Diffie-Hellman, 110 trust, 68 Turing machines, 73 Vernam cipher, 16 Vigenère cyphers, 15 Vinogradov, 166

Vinogradov method, 157

182

Waring problem, 153 Weil bound, 157, 164 word, 35 word problem, 36

XTR, 155

yes-biased, 10

zero-knowledge proofs, 39

