Math 408, Spring 2024
David Singer
Course Information

Office My office is at 2145 Adelbert Road, room 113. I will be available on Monday and Wednesday at 10:30AM and after class. I will also be available at other times by appointment; contact me to schedule. On Tuesdays I will be available for Zoom appointments.

Text *An Introduction to Mathematical Cryptography, 2nd Edition 2014*, by Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman, Springer, New York, ISBN 978-1493939381. We will also use references available over the internet: in particular, the Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.

Plan of the Course We will be covering chapters 1, 2, and 3, and 5, some of chapter 4, several sections of chapter 6, some of chapter 7, and a bit more. There are quite a few mathematical topics that need to be looked at; a list of them can be found on page xv. I intend to cover the needed mathematics in detail, on the assumption that you will not have ever seen some of it (e.g., number theory, information theory, elliptic curves, or finite fields) before. The final part of the course will consist of short presentations (15-20 minutes in length) on topics chosen by individual students. These will take place beginning on or about April 3, with three presentations per class period and the remaining presentations during the final exam slot (May 6 from 8AM to 11AM). Attendance is **required** on May 13; there will not be a final exam.

Grading There are homework assignments, due roughly once a week; homework represents 25% of the grade. There will be two "in class" exams, tentatively scheduled for **Friday, March 1, 2024** and **Monday, April 10, 2024**, which will count for 25% each. Individual projects and presentations will count for the remaining 25%.

Homework All homework should be submitted through Canvas. If at all possible, please convert your documents to pdf before submitting. If you are scanning or photographing your handwritten solutions, this may be difficult or impossible. So make sure your submissions are readable. For instance, dark ink on white paper is easier to read than light ink on tan paper. Because I do all the grading myself and it is quite time-consuming, please abide by the following rules. On the **top** of the front page of each assignment, please put your name in the upper left corner, followed by the assignment number and date. Put your initials on other pages. If I need to download the file, this will guarantee that I can keep track of whose paper is yours.

Midterm Each exam has two parts. The first part is in class; you will have 50–55 minutes. After you have submitted your exam and I have graded it, I will notify you

about problems you did incorrectly. You will then have an opportunity to resubmit answers to these parts; I may ask for additional information for each part. This will allow you to receive half credit for work done incorrectly the first time. So if your exam score was 70%, you can potentially improve to 85% by fixing your mistakes.

The usual rules of academic integrity apply: you may consult books or notes but not other people or the internet.

Projects Each student will make a 15-minute presentation on the chosen topic. If two students wish to coordinate on a single topic, you can make consecutive presentations; material in one presentation should not be repeated in the follow-up. Slides are the best way to do the presentations. If you do not want to use slides, you may use typed or hand-written notes, which you should project using the document camera. Only very small amounts of material should be written on the whiteboard.

A summary of the project, to be submitted electronically in PDF format, should be organized as follows: 1: Title page, including title of project, author(s) and date of final submission. 2: Abstract - one or two paragraphs, suitable as a stand-alone document appearing, for instance, in a conference announcement. 3: Statement of the problem. 4: A summary of the main ideas developed about the topic. 5: References used (preferably with hyperlinks). These references must be fully and correctly cited. 6: The body of your project may consist of power-point or other slides that you used in your presentation. Or you can scan your hand-written materials used in your presentation.

You should let me know in writing your choice of topic and a brief outline (one page plus references) by **February 12, 2024**. If you choose a topic not listed below, you need to clear it with me in advance. First to request a topic gets preference. A draft of your report is due on **Wednesday, March 6, 2024**. This should indicate significant progress toward completion of the project. The final report is due no later than **11:59PM on April 29**. Failure to meet this deadline will result in the **loss of at least one grade**.

The list below includes references to help get you started, many of them **seriously out of date**. I will be happy to help you find other references! Note: Quantum Crypto and Quantum Computing are not part of this course. Likewise, hardware issues, or algorithms for private-key cryptosystems (e.g., AES, DES, etc.) are not part of this course.

(1) Blind Signature schemes. See Blind Signatures Based on the Discrete Logarithm Problem, by J. Camenisch, J.-M. Piveteau, and M. Stadler, Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science v. 950, Springer Verlag, 1995, pp. 428-432. A recent article is Security of Blind Signatures Revisited, by Dominique Schroder and Dominique Unruh.

(2) Braid Group Cryptography. This has not been successful in the past; however, see a recent article, A Strong Blind Signature Scheme over Braid Groups, by WEI Yun, XIONG Guo-Hua, BAO Wan-Su and ZHANG Xing-Kai.

(3) Code-based cryptosystems. See A public key cryptosystem based on algebraic coding theory and Semantically SecureMcEliece Public-Key Cryptosystems–Conversions for McEliece PKC–.

(4) Coin Tossing. A recent article is Unfair Coin Tossing, by Demay and Maurer. In 2013 IEEE International Symposium on Information Theory Proceedings (ISIT), pp. 1556–1560, Jul 2013.

(5) Computer Poker. See C. Crépeau, A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face; In Advances in Cryptology: Proceedings of Crypto '86, volume 263 of Lecture Notes in Computer Science, pages 239-247. Springer, 1987; an elementary article: The Mathematical Gardner, by D. Klarner, pp. 37-43. From 2009, A fast Mental Poker Protocol, by Wei and Wang. Warning: while this is a popular topic, it should only be chosen if you focus on recent results, as illustrated by this link.

(6) Digital Cash (See, e.g., T. Okamoto and K. Ohta, Universal Electronic Cash, Advances in Cryptology – CRYPTO 91, Springer Notes in Computer Science 576, Springer-Verlag 1992, pp. 324-337.) [There are interesting mathematical issues here. But let's not get into the economics and politics of Bitcoin and other e-currencies!] On recent reference is Cryptanalysis on "Secure untraceable off-line electronic cash system", by Chen and Chou.

(7) Digital pseudonyms. (See Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM, 24 (February, 1981), 84-88. From 2007, there is Unique User-generated Digital Pseudonyms, by Peter Schartner and Martin Schaffer.

(8) The discrete log problem in Z_p or F_2^n : index calculus methods, Pollard's method, or generally methods based on random permutations. (See, e.g., B. LaMacchia and A. Odlyzko, Computation of discrete logarithms in prime fields, Designs, Codes, and Cryptography 1 (1991), pp. 46-62;or A.M. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance. [Avoid repeating the part of this topic covered in class!]

(9) New Representations for Elliptic Curves. See A NORMAL FORM FOR ELLIPTIC CURVES, by Harold Edwards.

(10) Hash-based digital signature schemes. See,e.g., Hash Based Digital Signature Schemes, by C. Dods, N.P. Smart, M. Stam, in Cryptography and Coding, LNCS 5299 (2005), 109-123.

(11) Information hiding. See Information Hiding - A Survey by F. Petitcolas, R. Anderson, and M. Kuhn, Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062-1078.

(12) Lattice-based Cryptography. [NOTE: This topic will be covered in class. If you wish to present on this, you will either have to do it early in April or on material not covered in class.] See D. Boneh and R. Venkatesan, Rounding in lattices and its cryptographic applications, Proceedings of SODA 1997, pp. 675-681. There are more recent sources, such as Post-quantum cryptography: lattice signatures, by J. Buchmann, R. Lindner, and M. Schneider, Computing, June 2009, 85, 105-125.[Avoid repeating material covered in class!]

(13) Multivariate Quadratic Encryption. See A "Medium-Field" Multivariate Public-Key Encryption Scheme, by Lih-Chung Wang; Bo-Yin Yang; Yuh-Hua Hu; Feipei Lai. A public key cryptosystem based on polynomial transformations, which may be resistent to quantum computing attacks. For an early paper, see Analysis of a Public Key Approach Based on Polynomial Substitutions, by Harriet Fell and Whitfield Diffie.

(14) Dragon Cryptosystems. Also a Multivariate encryption system, like the previous item. A recent update can be found at Poly-Dragon: An efficient Multivariate Public Key Cryptosystem, by Rajesh P. Singh, A. Saikia and B.K. Sarma

(15) The NTRU Cryptosystem. [This is a topic in Lattice Crypto]. See The Mathematics of the NTRUPublic Key Cryptosystem, By Nitaj.

(16) One-Time Signatures. See One-Time Signatures Revisited: Have They Become Practical?, by Dalit Naor and Amir Shenhav and Avishai Wool.

(17) Private passwords. See, for instance, C. Ellison, C. Hall, R. Milbert, and B. Schneier, Protecting Secret Keys with Personal Entropy, Future Generation Computer Systems. A 2007 paper is Secure Secret Recovery by using Weighted Personal Entropy, by leau, Dinna, Habeeb, and Jetol.

(18) Cryptographically secure Random Number generators, or Prime Number generators. See, for instance, U. Maurer, Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters; Institute for Theoretical Computer Science, ETH Zürich. 1995. Journal of Cryptology. Vol. 8. Nr. 3. Pages: 123-156. For an attack, see When Private Keys are Public: Results

from the 2008 Debian OpenSSL Vulnerability by By Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, and Stefan Savage. In Proceedings of IMC 2009, pages 15–27. ACM Press, Nov. 2009.

(19) Secret Sharing. See, e.g., Rational secret sharing and multiparty computation, by Joseph Y. Halpern and Vanessa Teague. In Proceedings of 36th ACM Symposium on Theory of Computing, 2004, pp. 623-632.

(20) Steganography (Visual cryptography). See R. Anderson and F. Peticolas, On the Limits of Steganography, IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection, vol. 16 no. 4, pp. 474-481, May 1998. Lots of literature out there!

(21) Timing cryptanalysis of RSA and other public key cryptosystems. (See, e.g., Paul C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Proc. CRYPTO'96, pp.104-113.) A more recent paper is Brumley and Boneh, Remote Timing Attacks are Practical In Proc. 12th USENIX Security Symposium, 2003.

(22) Tracing Traitors. See Tracing traitors., by Benny Chor, Amos Fiat, Moni Naor, and Benny Pinkas. IEEE Transactions on Information Theory, 46(3):893–910, 2000. A recent article, from 2013, is Multiparty Key Ecxchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation, by Dan Boneh and Mark Zhandry.

(23) Voting. (See Cohen and Fischer, A robust and verifiable cryptographically secure election scheme, Proceedings of the 26th IEEE symposium on Foundations of Computer Science (1985), pp. 372-382.) It is tough to find good current work on this. One possible reference is Every Vote Counts: Ensuring Integrity in Large-Scale Electronic Voting, by Hao et al. Another is Election Verifiability: Cryptographic Definitions and an Analysis of Helios and JCJ, by Smyth, Frink, and Clarkson.

(24) Weak Passwords. See Katz, Ostrovsky and Ung,Efficient and Secure Authenticated Key Exchange Using Weak Passwords,Journal of the ACM 57(1): 78-116, 2009.

(25) Zero Knowledge proofs. See, for instance, O. Goldreich and E. Kushilevitz, A Perfect Zero-Knowledge Proof System for a Problem Equivalent to the Discrete Logarithm, J. Cryptology 6(2), 1993, pp. 97-116. Early version: Crypto 88.