List of Papers Presented

1. Rivest, R. L.; A. Shamir; and L. Adleman, "A method for obtaining digital signatures and public-key cryptography," *Communications of the ACM*, **21**:2 (February 1978), 120–126.

2. Cormen, Thomas H.; Charles E. Leiserson; and Ronald L. Rivest, "Chapter 33: Number-Theoretic Algorithms" in *Introduction to Algorithms*, MIT Press and McGraw-Hill (New York, 1990).
Note: We spent four lectures discussing the following topics: solving linear Diophantine equations, Chinese remainder theorem, quadratic residuosity, primality testing, and the security of Rabin's cryptosystem.

3. Elgamal, Tather, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, **IT-31**:4 (July 1985), 469–472.

4. Maurer, Ueli M., "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms," *Crypto 94*, Springer-Verlag (August 1994), 271–281.

5. Kent, Stephen T., "Internet privacy enhanced mail," *CACM*, **36**:8 (August 1993), 48–59.

6. Micali, Silvio, "Fair public-key cryptosystems," *Crypto 92 Abstracts* (August 1992), 3.11–3.24.

7. Kaliski, Burton S. Jr.; Ronald L. Rivest; and Alan T. Sherman, "Is the Data Encryption Standard a group? (Results of cycling experiments on DES)," *Journal of Cryptology*, **1**:1 (1988), 3–36.

8. *Special Lecture:* Dorothy Denning (Georgetown University), "The Clipper Chip" (October 6, 1994).

9. Blaze, Matt, "Protocol failure in the escrowed encryption standard," *2nd ACM Conference on Computer and Communications Security*, ACM Press (November 2–4, 1994), 59–67. [Presented by Paul Miller.]

10. Chaum, David, "Security without identification: Transaction systems to make big brother obsolete," CACM, **28** (October 1985), 1030–1044. [Presented by Mukund Mohan.]

11. *Special lecture:* Jack Ingram (Curator, National Cryptologic Museum), "Historical perspectives in communications security" (October 19, 1994).

12. Morris, Robert, "The Hagelin Cipher Machine (M-209): Reconstruction of the internal settings," *Cryptologia*, **2**:3 (July 1978), 267–289.

13. Baldwin and Sherman: "How we solved the $100,000 Decipher Puzzle (16 hours too late)," *Cryptologia*, **XXIV**:3 (July 1990), 258–284.

14. Sherman, Alan T., "When does a linear shift register attain the maximum possible period?" CMSC-652 lecture notes (spring 1992), 6 pages.

15. Cain, Thomas; and Alan T. Sherman, "How to break Gifford's Cipher," *Cryptologia* (June 2, 1994), accepted for publication. 49 pages. [Presented by Thomas Cain.]

16. Pomerance, Carl, "The quadratic sieve factoring algorithm," *Eurocrypt 84*, Springer-Verlag, 169–182. [Presented by Dave Helfrick.]

17. Lenstra, "Factoring by email." [Presented by Dave Helfrick.]

18. Hellman, Martin E., "A cryptanalytic time-memory trade-off," *IEEE Transactions on Information Theory*, **IT-26**: 4 (July 1980), 401–406. [Presented by Greg Urban.]

19. Shamir, Adi; Ronald L. Rivest; and Leonard Adleman, "Mental poker" in *The Mathematical Gardner*, edited by David A. Klarner, Wadsworth (Belmont, CA, 1981), 37–43.

20. Blum, Manuel, "Coin flipping by telephone," *Compcon*, IEEE Press (spring 1982), 133–137.

21. Ben-Or, Michael; Oded Goldreich; Silvio Micali; and Ronald L. Rivest, "A fair protocol for signing contracts," *ICALP 85*, Spring-Verlag (1985), 44–52.

22. Johnson, David S., "Interactive proof systems for fun and profit" in "The NP-completeness column: An ongoing guide," *Journal of Algorithms*, **9** (1988), 426–444.

23. Shannon, C. E., "Prediction and entropy of printed English," *Bell System Technical Journal*, **30**, (January 1951), 50–64.

24. Ganesan, Ravi; and Alan T. Sherman, "Statistical techniques for language recognition: An introduction and guide for cryptanalysts," *Cryptologia*, **XVII**:4 (October 1993), 321–366.

25. Shor, peter W., "Algorithms for quantum computation: Discrete log and factoring," extended abstract (August 1994), 14 pages. [Presented by Predrag Tosic.]