Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 17
October 20, 1998

Readings for Lecture 11

Attached is the following reading:

- readings from *Handbook of Applied Cryptography*, pages 474-481. [1]

- *How to Share a Secret* [2]

References

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[2] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, November 1979.