Massachusetts Institute of Technology	Handout 20
6.857: Network and Computer Security	October 22, 1998
Professor Ronald L. Rivest	

Readings for Lecture 12

Attached is the following reading:

- readings from *Applied Cryptography, Second Edition*, pages 518–522. [3]

- readings from *Web Security and Commerce*, pages 417–427. [2]

- readings from *Designs, Codes, and Cryptography*, pages 107–125. [1]

References

[1] Whitfield Diffie, Paul C. Van Oorschot, and Michael J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes, and Cryptography*, 2(2):107–125, June 1992.

[2] Simson Garfinkel and Gene Spafford. *Web Security and Commerce*. O'Reilly and Associates, 1997.

[3] Bruce Schneier. *Applied Cryptography (Second Edition)*. John Wiley & Sons, 1996.