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

Handout 6
September 26, 1995

Readings for Lecture 6

Attached are the following sections from Bruce Schneier's book *Applied Cryptography* [1]

13.3 The El Gamal public-key cryptosystem

13.5 The Digital Signature Algorithm (DSA)

14.1 One–way hash functions: background

14.5 The Message Digest 5 function (MD5)

References

[1] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, New York, 1993.