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

Handout 15
October 22, 1997

Readings for Lecture 14

Attached are the following papers

- *Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks* [1].
- *Tamper Resistance – a Cautionary Note* [**?**].

References

[1] Paul C. Kocher. Cryptanalysis of diffie-hellman, RSA, DSS, and other systems using timing attacks. Unpublished Manuscript, December 1995.