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

Handout 21
October 27, 1998

Paper for Lecture 13

Attached is the following reading:

- Paper: *SKIPJACK and KEA Algorithm Specifications* [1]

NOTE: The description of the Skipjack block cipher is left in here for completeness, although for this class the purpose of this handout is the description of the KEA Key Exchange Algorithm.

References

[1] National Institute of Standards and Technology (NIST). SKIPJACK and KEA algorithm specifications, 1998. `http://csrc.nist.gov/encryption/skipjack-1.pdf`, `skipjack-2.pdf`.