

EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 5
20 February 2020

Professor Dunham
Due: 27 February 2020

Review Paar Text: Chapter 3 & 4.
Review FIPS 46, 46-3 and 197.

1. Paar & Pelz 3.1.
2. Paar & Pelz 3.3.
3. Paar & Pelz 3.5.
4. Paar & Pelz 4.9.
5. Paar & Pelz 4.11.
6. Paar & Pelz 4.13.
7. Paar & Pelz 4.17 Hardcopy or 4.16 Online copy. Refer to p. 12 for Moore's Law.