Exercises E4: DES and AES

August 16, 2006

1 From *Making, Breaking Codes* by Paul Garrett

Answer either of these two questions.

1. Is there any good argument *against* Kerckhoff and Shannon's principle that only the key should be secret, not the larger mechanism (or algorithm) of a cipher? (6.1.01)

2. Why is resistance to known and adaptive plaintext attacks really necessary, rather than merely resistance to ciphertext-only attacks? (6.1.02)

2 From Trappe and Washington

Section 4.9
Exercises: 1, 2, 3, 4, 6, 11.

Section 5.5
Exercises: 1, 3, 4.