Introduction to Modern Cryptography, Exercise # 2

University of Amsterdam, Master of Logic
Lecturer: Christian Schaffner
TA: Joachim Schipper

13 September 2011
(to be handed in by Tuesday, 20 September 2011, 9:00)

1. Exercise 2.3 from [KL].
2. Exercise 2.4 from [KL]. **Hint:** Use part (a) in part (c).
3. Exercise 2.13. from [KL]. **Clarification:** Prove that the *same* lower bound $|\mathcal{K}| \geq |\mathcal{M}|$ as in Theorem 2.7 holds also for almost perfectly secret encryption schemes. **Hint:** Ignore the hint in the book, but follow the original proof of Theorem 2.7 instead.
4. Exercises 2.7 and 2.8 from [KL]. You do *not* need to prove Exercise 2.6. You can just use the result.

Figure 1: The "Red Phone" at the Jimmy Carter Library and Museum.
Image credit: `www.wikipedia.org`.