University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 7

Due at the *beginning* of class on Dec. 7

1. Exercise 10.2.
2. Exercise 10.4. (Give a construction and a proof.)
3. Exercise 10.12. (A proof is not needed.)
4. Exercise 10.13.
5. Exercise 10.14. (*Hint*: consider what happens when you multiple $\bar{m}$ by 2.)
6. Exercise 10.17. (In part (b), assume that encryption of a single bit using El Gamal is done by using the encoding $0 \mapsto g^0$ and $1 \mapsto g^1$. No proof is needed for part (c).)