University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Practice Problems

Numbered exercises are from the *first edition* of the book.

1. Exercise 10.1.
2. Exercise 10.4.
3. Exercise 10.11.
4. Exercise 10.12.
5. Exercise 10.13.
6. Exercise 10.17.
7. Consider textbook RSA encryption with public key 55 and public exponent $e = 3$.
   (a) How many elements are in $\mathbb{Z}_{55}^*$?
   (b) Compute the private exponent d.
   (c) Compute the encryption of the message $m = 6$.
   (d) Compute the decryption of the ciphertext $c = 2$.
8. Consider El Gamal encryption using the cyclic group $\mathbb{Z}_{19}^*$. (Note: this is not a prime-order group, but El Gamal encryption can be defined in any cyclic group—even though it can only secure in prime-order groups.)
   (a) How many elements are in this group?
   (b) Find a generator of this group.
   (c) Find an element in this group that is not a generator.
   (d) Say a receiver uses your generator from part (b) and chooses private exponent 7. What is the receiver's public key?
   (e) Using the public key from part (d), what is the encrption of $m = 2$ using randomness $r = 4$?