University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 6

Due at the *beginning* of class on Nov. 14

1. Exercise 7.1.
2. Exercise 7.3.
3. Exercise 7.5.
4. Exercise 7.6.
5. (You can use a calculator that handles modular arithmetic [e.g., bc on unix systems], or write a program for this question. I don't care what method you use.)

   Let $N = 23701 = 137 \cdot 173$.

   - What is $\varphi(N)$?
   - What is the smallest value of $e > 1$ that is relatively prime to $\varphi(N)$?
   - Fix e as in the previous question. Find d such that $ed = 1 \bmod \varphi(N)$. (*Hint*: If you think about it, you can find this by simple trial-and-error using a calculator, without having to write a program.)
   - Fix e, d as in the previous question. Take $x = 201$ and compute $y = [201^e \bmod N]$. What is $[y^d \bmod N]$?
6. Exercise 7.15.
7. Exercise 7.18.
8. Assume you overhear the following conversation between Alice and Bob:

   - Alice says "$p = 347$, $g = 4$, $h_1 = 236$"
   - Bob says "$h_2 = 167$"

   Determine their shared secret. (*Note*: You can do this by hand using a calculator that does modular arithmetic [e.g., bc on unix systems], or write a short program to solve it. I don't care what method you use.)
9. Exercise 9.2.
10. Exercise 9.3.