University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 4

Due at the *beginning* of class on Nov. 4

1. Compute $7^{120007} \bmod 143$ *by hand*. (Note that $143 = 11 * 13$.) Use the Chinese remainder theorem, Fermat's little theorem, and the fast modular exponentiation algorithm discussed in class, as needed.

2. Show that $\mathbb{Z}_{56}$ is not a group under multiplication by showing an element of $\mathbb{Z}_{56}$ which does not have a multiplicative inverse. Can you *prove* that this element does not have an inverse?

3. How many elements are in $\mathbb{Z}_{17}^*$? Is this group cyclic? If so, determine how many generators it has and list them. If not, find the subgroup of $\mathbb{Z}_{17}^*$ of largest order.

4. Since 101 is prime, $\mathbb{Z}_{101}^*$ is a cyclic group. What is its order? Use Prop. 7.13 of Bellare-Rogaway to determine whether 8 is a generator of this group. How many generators does $\mathbb{Z}_{101}^*$ have? If you chose an element of $\mathbb{Z}_{101}^*$ at random, what is the probability that it will be a generator?

5. Prove that if G is a commutative group, then the set of quadratic residues in G forms a subgroup of G.

6. Consider the group $\mathbb{Z}_{35}^*$ (of course, $35 = 5 * 7$). Answer the following questions about this group:

   - How many elements are in this group? List them.
   - (Note: The Chinese Remainder Theorem will make the next two problems much less tedious.) For each element of the group, determine whether it has Jacobi symbol $+1$ or -1. How many elements have Jacobi symbol $+1$?
   - For each element which has Jacobi symbol $+1$, state whether it is a quadratic residue or not. How many of the elements with Jacobi symbol $+1$ are quadratic residues?
   - For each element which is a quadratic residue, find all of its square roots.
   - Say we fix our RSA public exponent e to 5. What is the value of d, the private exponent?

7. Fix an RSA modulus N and public exponent e. Say we have an efficient algorithm A that can invert RSA for these parameters but which works only 1% of the time. Specifically, let $S \subset \mathbb{Z}_N^*$ be the set of elements such that $C \in S \Rightarrow A(C) = C^{1/e} \bmod N$ (i.e., S is the set of elements for which A can compute the inverse). Then since A works 1% of the time, $|S|/|\mathbb{Z}_N^*| = 0.01$.

(a) Show that if one can compute the inverses of C_1 and C_2, then one can also efficiently compute the inverse of their product $C_1C_2 \bmod N$.

(b) Show that if one can compute the inverse of $C' \stackrel{\text{def}}{=} Cr^e \bmod N$, then one can also efficiently compute the inverse of C.

(c) Suggest how to use A to compute the inverse of *any* element $C \in \mathbb{Z}_N^*$ with high probability. *Hint:* you will need to use randomization.