University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 1

Due at *beginning* of class on Sept. 23

1. In class we discussed *perfect security* and gave the following definition: an encryption scheme for n-bit messages is perfectly secure if, for all distributions over message space $\{0,1\}^n$, for all $m \in \{0,1\}^n$, and for all ciphertexts c we have: $\Pr[m|c] = \Pr[m]$ (where c is an observed ciphertext). Note that this definition only covers security against *ciphertext only attacks*.

   - Formulate a definition of perfect security against known message attacks. You may consider an adversary who receives only a single (message, ciphertext) pair.
   - Prove that no *deterministic*, stateless encryption scheme can be perfectly secure against known message attacks. (A deterministic encryption scheme is one in which E is a deterministic function of the key and the message.)
   - **(Graduate students only.)** Prove that even a randomized, stateless encryption scheme cannot be perfectly secure against known message attacks. Suggest a way to relax the definition so that it might be attainable (you do not need to show a scheme that attains it).

2. Compute $101^{4,800,000,023} \bmod 35$ (without using a computer). Show all work. (Hint: use Chinese remaindering, among other tricks.)

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

   - How many elements are in this group?
   - List the elements of this group.
   - (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.
   - What is $\varphi(35)$?

4. Assume we have an algorithm A that runs in 5 seconds and can compute square roots over a composite 1% of the time. More precisely: fix modulus $N = pq$ where p, q are prime. Let S be the subset of $\mathcal{QR}_N$ such that $A(y) = x$ and $x^2 = y$ (i.e., S is that subset for which A can correctly compute a square root). Then since A is correct 1% of the time, we have $|S| = \frac{|\mathcal{QR}_N|}{100}$.

   (a) Show that if A can compute the square root of y_1 and also compute the square root of the product $y_1 \cdot y_2 \bmod N$, then we can use A to efficiently compute the square root of y_2.

   (b) Suggest how to use A to efficiently compute the square root of *any* element in $\mathcal{QR}_N$ (use randomization). How long will this take, on average?

5. Recall the definition of a pseudorandom generator (PRG) given in class: $G : \{0,1\}^* \to \{0,1\}^*$ is a PRG if its output is larger than its input and, for all efficient (probabilistic polynomial time) algorithms A we have:

$$\Pr[x \leftarrow \{0,1\}^n; y = G(x) : A(y) = 1] - \Pr[y \leftarrow \{0,1\}^m : A(y) = 1] < \epsilon(m). \qquad (1)$$

   Discuss whether the functions G which follow are secure under the above definition. When it is, prove it. When it is not, give an explicit (efficient) algorithm for which condition (1) does not hold.

   (a) G defined by $G(x) = x \circ b$ where b is the parity of x.

   (b) Let G_1, G_2 be secure PRGs. Define G by $G(x) = G_1(x) \circ G_2(x)$.

   (c) **(Graduate students only)** Let G_1, G_2 be secure PRGs. Define G by $G(x_1 \circ x_2) = G_1(x_1) \circ G_2(x_2)$. Note the difference between this and the previous problem.