COS 433 — Cryptography — Homework 6.

Boaz Barak

Total of 140 points. Due March 24, 2010.

Note: In the following questions, you will often need to use a proof by reduction. When you write a proof by reduction it generally has two parts:

1. The description of the reduction— an algorithm B that uses a hypothetical algorithm A as a black box. The description should include the input, operation, and output of B, where the operation clearly states what are the inputs that B feeds into A. You should also explain why B will run in polynomial-time if A does.
2. Analysis of the reduction— proving that if A breaks the security of some crypto primitive X then B breaks the security of another crypto primitive Y.

Make sure you write both parts clearly and precisely.

Exercise 1 (20 points)**.** Recall that we say that a function $f : \{0,1\}^* \to \{0,1\}^*$ is a *one-way function* if it is efficiently computable and for every polynomial time A there is a negligible function $\epsilon : \mathbb{N} \to [0,1]$ such that for all $n \in \mathbb{N}$,

$$\Pr_{x \leftarrow_{\mathrm{R}} \{0,1\}^n}[A(f(x)) = x' \text{ s.t. } f(x') = f(x)] < \epsilon(n) .$$

1. Prove that if there exists a one way function f, then there exists a one-way function f' such that $|f'(x)| = |x|$ for every $x \in \{0,1\}^*$.
2. Prove the easy direction of the famous theorem of Hastad, Impagliazzo, Levin and Luby— if there exists a pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{2n}$ then there exists a one-way function.

Exercise 2 (20+20 points)**.** Recall that the Goldreich-Levin Theorem says that there is a poly$(n, 1/\epsilon)$-time algorithm that given oracle access to an oracle A that computes the function $r \mapsto \langle x, r\rangle$ with probability $1/2 + \epsilon$ over the choice of r, outputs a list of at most $\left(\frac{100n}{\epsilon}\right)^2$ strings one of which contains x. In this exercise we explore whether such a list is necessary and how large must it be. (Some of the questions may require a bit of thought— I suggest you try to think about the solution for a while on your own, before looking at the hint. In any case my hint is definitely not the only way to solve them.)

1. Show that there is a function $A : \{0,1\}^n \to \{0,1\}$ and two n-bit strings $x_1 \neq x_2$ such that for both $i = 1, 2$
$$\Pr_r[A(r) = \langle x_i, r\rangle] \geq 0.6 .$$
Deduce from this fact that for $\epsilon < 0.1$, there is no algorithm as above that outputs the string x with probability at least 0.99 instead of a list.

2. Show that for every small enough $\epsilon > 0$, there are at least $1/(10\epsilon)$ strings $x_1, \ldots, x_{1/(10\epsilon)}$ and function $A : \{0,1\}^n \to \{0,1\}$ such that for every i

$$\Pr_r[A(r) = \langle x_i, r \rangle] \geq 1/2 + \epsilon \ .$$

   For 10 extra points, show that there are $1/(100\epsilon^2)$ such strings.See footnote for hint[1]

3. (10 extra points) Show that there is some function $f(\epsilon)$ (independent of n), such that for every function $A : \{0,1\}^n \to \{0,1\}$ there are at most $f(\epsilon)$ strings $x_1, \ldots, x_i$ such that

$$\Pr_r[A(r) = \langle x_i, r \rangle] \geq 1/2 + \epsilon \ .$$

   (This can be shown for $f(\epsilon) = 100/\epsilon^2$.) See footnote for hint.[2]

Review of group and number theory

The following questions are meant to prepare you for the next lecture, when we'll start doing some very basic group and number theory to introduce *public key cryptography.* These questions are self contained, so you can solve them without reading outside sources. Nevertheless, I recommend you also take a look at some of the following resources: **(1)** The most recommended is Victor Shoup's book *"A Computational Introduction to Number Theory and Algebra"* (also available online at `http://www.shoup.net/ntb/`): pages 1–10 and pages 180–184 are particularly relevant, but look also in Chapter 2 up to and including Section 2.5, first 2 pages of Chapter 7, Chapter 10 up to and including 10.4.1, first two pages of Chapter 11, Chapter 12 and Chapter 13 (these page numbers are from Version 1, in Version 2 they may be a bit different) **(2)** Katz-Lindell book, Chapter 7 and Appendix B, and **(3)** The mathematical background appendix of book with Sanjeev Arora also contains some basic number theory background— see link on the course's website.

A *group* $(S, \star)$ is a set S with a binary operation $\star$ defined on S for which the following properties hold:

1. **Closure**: For all $a, b \in S$ it holds that $a \star b \in S$.

2. **Identity**: There is an element $e \in S$ such that $e \star a = a \star e = a$ for all $a \in S$.

3. **Associativity**: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$.

4. **Inverses**: For each $a \in S$ there exists an element $b \in S$ such that $a \star b = b \star a = e$.

The *order* of a group, denoted by $|S|$, is the number of elements in S. If the order of a group is a finite number, the group is said to be a *finite group.* If a group $(S, \star)$ satisfies the *commutative law* $a \star b = b \star a$ for all $a, b \in S$ then it is called an *Abelian group.*

[1] **Hint:** For $x_1, \ldots, x_i$, with $i = 1/(100\epsilon^2)$, a natural candidate for A is the function that on input r outputs the majority value among the bits $\langle x_1, r \rangle, \ldots, \langle x_i, r \rangle$. Thus, if we think of an i by 2^n matrix in which for every $j \in \{1..i\}$, the j^{th} row consists of the 2^n values of the function $r \mapsto \langle x_i, r \rangle$, then we look at the majority value in each column. Since for i independent (or even pairwise independent) 0/1 variables, the variance of the sum is the sum of the variances (each of which is about 1/4), if the x_i's were chosen at random then each column is expected to have $i/2$ ones and $i/2$ zeroes, with a standard deviation of at least $\sqrt{i}/5$. So we expect the majority value on a typical column to agree with roughly $i/2 + \sqrt{i}$ of the rows. Since in our case $\sqrt{i} \sim \epsilon i$, we get that we expect roughly $1/2 + \epsilon$ agreement on average.

[2] **Hint:** For every function $f : \{0,1\}^n \to \{0,1\}$, let v_f be the 2^n-dimensional real vector (i.e. $v \in \mathbb{R}^{2^n}$) such that for every $r \in \{0,1\}^n$ (identified in some way with a number in $\{1..2^n\}$) the r^{th} coordinate of v_f is -1 if $f(r) = 1$ and $+1$ if $f(r) = 0$. For every $x \in \{0,1\}^n$, let v_x denote the vector corresponding to the function $r \mapsto \langle x, r \rangle$. Then if $x \neq x'$, one can check that $\langle v_x, v_{x'} \rangle = 0$ where this time we're talking about inner product over the reals (i.e. $\langle v, w \rangle = \sum_{r \in \{0,1\}^n} v(r)w(r)$). This means that the 2^n vectors $\{v_x\}_{x \in \{0,1\}^n}$ are an *orthogonal basis* for the space $\mathbb{R}^{2^n}$. Now normalize the basis to be orthonormal, and use the fact that the norm of a vector is invariant under a change of orthonormal basis. That is, for every vector $a \in \mathbb{R}^N$ and orthonormal basis $\{v_1, \ldots, v_N\}$, $\sum_{i=1}^N a_i^2 = \sum_{i=1}^n \langle a, v_i \rangle^2$.

Exercise 3 (10 points)**.** Let $+_n$ denote addition modulo n (e.g., $5 +_3 6 = (5+6) \mod 3 = 2$). Let $Z_n = \{0, 1, 2, \dots, n-1\}$. Prove that $(Z_n, +_n)$ is a finite Abelian group for every natural number n.

Exercise 4 (10 points)**.** Prove that for every group:

1. The identity element e in the group is **unique**.
2. Every element a has a **single** inverse.

Exercise 5 (10 points)**.** Let a be an element in a group and let a^{-1} denote the (unique) inverse of a. Then, for every integer k we define:

$$a^k \overset{\text{def}}{=} \begin{cases} \underbrace{a \star a \star \dots \star a}_{k}, & \text{if } k > 0; \\ e, & \text{if } k = 0; \\ (a^{-1})^{-k}, & \text{if } k < 0. \end{cases}$$

Prove that for any integers m, n (not necessarily positive) it holds that:

1. $a^m \star a^n = a^{m+n}$.
2. $(a^m)^n = a^{nm}$.

Exercise 6 (10 points+10 points)**.** Let $(S, \star)$ be a group and let $S' \subseteq S$. If $(S', \star)$ is also a group, then $(S', \star)$ is called a *subgroup* of $(S, \star)$. Prove that:

1. If $(S, \star)$ is a finite group and $a \in S$ then there exists $m \geq 1$ such that $a^m = a^{-1}$.
2. If $(S, \star)$ is a finite group and S' is a subset of S such that $a \star b \in S'$ for every $a, b \in S'$, then $(S', \star)$ is a subgroup of $(S, \star)$.
3. (10 extra points.) Prove that if S' is a set corresponding to a subgroup of S, then for every $a \in S$ and $b \in S$, the sets $a \star S'$ and $b \star S'$ are either identical or disjoint, where we denote $x \star S' \overset{\text{def}}{=} \{x \star y : y \in S'\}$. Conclude that if S is finite and S' is a subgroup of S then $|S|/|S'|$ is an integer.

Exercise 7 (10 points)**.** Let a and b be two positive integers. We denote by $\gcd(a, b)$ the greatest common divisor of a and b; i.e, $d = \gcd(a, b)$ if d is the largest integer that divides both a and b. The extended Euclidean algorithm computes the gcd as follows:

```
input: $a > b > 0$
$r_{-1} \leftarrow a$
$r_0 \leftarrow b$
for $i = 1, 2, \dots$ till $r_i = 0$
    $r_i \leftarrow r_{i-2} \mod r_{i-1}$
output $r_{i-1}$
```

1. Prove that this algorithm indeed outputs the gcd of a and b.

2. Prove that if d is the gcd of a and b, then there exist (not necessarily positive) integers x, y such that $d = xa + yb$. Can you compute these numbers?

Exercise 8 (10 points)**.** Let $\times_n$ denote multiplication modulo n (i.e., $5 \times_7 3 = 15 \pmod 7 = 1$).

1. Prove that for every n, the set $\mathbb{Z}_n^* = \{k : 1 \leq k < n, gcd(k, n) = 1\}$ with the operation $\times_n$ is an Abelian group.

2. Give an algorithm that on input $a \in \mathbb{Z}_n^*$, computes a^{-1} (w.r.t. the group operation $\times_n$).

3. If n is a *prime* number, how many elements exist in $\mathbb{Z}_n^*$?

Exercise 9 (10+10 points)**.** A group S is *cyclic* if there exists an element $g \in S$ that "generates" the group; that is, $S = \langle g \rangle$, where $\langle g \rangle \overset{\text{def}}{=} \{g^k : k \geq 1\}$. (Such an element is referred to as a *generator* of the group.)

1. Give an example of a cyclic group.

2. Give an example of a finite group that is not cyclic.

3. (10 extra points) Prove that for every finite group S, if $a \in S$ then the size of the set $\langle a \rangle = \{a^k : k \geq 1\}$ divides $|S|$. Conclude that for every finite group S and $a \in S$, $a^{|S|} = 1$ (where 1 denotes the identity element in S).

In both cases you should prove that the given group is indeed cyclic (resp. non-cyclic).