CS6111: Foundations of Cryptography

Assignment 2

Instructions

- Deadline is September 9.
- We encourage submissions by Latex. Paper is also accepted.

References

- Introduction to Cryptography - Delfs and Knebl
- A Graduate Course in Applied Cryptography - Boneh and Shoup (link)
- Introduction to Modern Cryptography - Katz and Lindell
- Handout 3

1 Number Theory

1. (2 points)

   Proposition 1. *Let $\mathbb{G}$ be a finite group, and $\mathbb{H} \subseteq \mathbb{G}$. Assume that $\mathbb{H}$ contains the identity element of $\mathbb{G}$, and that for all $a, b \in \mathbb{H}$ it holds that $ab \in \mathbb{H}$. Then $\mathbb{H}$ is a subgroup of $\mathbb{G}$.*

   Show that the above proposition does not necessarily hold when $\mathbb{G}$ is infinite. **Hint:** Consider the set $\{1\} \cup \{2, 4, 6, 8 \cdots\} \subset \mathbb{R}$.

2. (2 points) Let $\mathbb{G}$ be a finite group and $g \in \mathbb{G}$. Show that $\langle g \rangle = \{g^i \mid i \geq 0\}$ is a subgroup of $\mathbb{G}$. Is the set $\{g^0, g^1, \cdots\}$ necessarily a subgroup of G when G is infinite?

3. (2 points) If $N = pq$ and $ed = 1 \mod \phi(N)$ then for any $x \in \mathbb{Z}_N^*$ we have $(x^e)^d = x \mod N$. Show that this holds for all $x \in \mathbb{Z}_N$. **Hint:** Use the Chinese remainder theorem.

4. (2 points) Let $N = pq$ be a product of two distinct primes. Show that if N and $\phi(N)$ are known, it is possible to compute p and q in polynomial time.

5. (2 points) Let $N = pq$ be a product of two distince primes. Show that if N and an integer d such that $3d \equiv 1 \mod \phi(n)$ are known, then it is possible to compute p and q in polynomial time. **Hint:** First obtain a small list of possible values of $\phi(n)$.)

2 One Way Functions and Negligible Functions

1. (2 points) If $\mu(.)$ and $\nu(.)$ are negligible functions then show that $\mu(.) \cdot \nu(.)$ is a negligible function.

2. (2 points) If $\mu()$ is a negligible function and $f()$ is a function polynomial in its input then show that $\mu(f())$ are negligible functions.

3. (2 points) Prove that the existence of one-way functions implies $\mathsf{P} \neq \mathsf{NP}$.

4. (2 points) Prove that there is no one-way function $f : \{0,1\}^n \to \{0,1\}^{\lfloor \log_2 n \rfloor}$.

5. (2 points) Let $f : \{0,1\}^n \to \{0,1\}^n$ be any one-way function then is $f'(x) \stackrel{def}{=} f(x) \oplus x$ necessarily one-way?

6. (2 points) Prove or disprove: If $f : \{0,1\}^n \to \{0,1\}^n$ is a one-way function, then $g : \{0,1\}^n \to \{0,1\}^{n-\log n}$ is a one-way function, where $g(x)$ outputs the $n - \log n$ higher order bits of $f(x)$.

7. (2 points) If f is a one-way function then is $f^2(x) = f(f(x))$ always a one-way function?

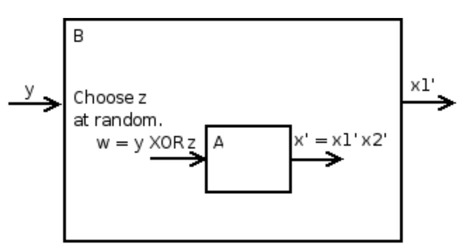
3 Fun With One Way Functions

Suppose that $f(x)$ is a one-way function. Let $|x|$ denote the length of the binary string x. We let $\circ$ denote the concatenation operator. Similarly, $(\circ)$ is the parse operator which we can use to represent a string x as $x = x_1(\circ)x_2$ where $|x_1| = |x_2|$. (Assume for simplicity that all strings to which this operator is applied are of even length; for example, this can be accomplished by appending a 0 to the end of an odd-length string prior to applying this operator.) Function f here is *length-preserving*, which means that $|f(x)| = |x|$, and also that we need not give the adversary 1^k as input.

1. (3 points) Prove that the following is not a one-way function:
   $f_a(x) = f(x_1) \oplus x_2$, where $x = x_1(\circ)x_2$.

2. (3 points) Find the fault in the following proof that f_a is one-way.

   $f_a(x)$ is a one-way function. Assume for the sake of contradiction that we have a PPT inverter $\mathcal{A}$ for $f_a(x)$ that, when given w, outputs some x' such that $f_a(x') = w$ with nonnegligible probability. We want to use this $\mathcal{A}$ to construct an inverter for the one-way function $f(x)$. Let $\mathcal{B}$ be a PPT that on input y picks a random string $z \leftarrow \{0,1\}^{|y|}$, runs $\mathcal{A}$ on $w = y \oplus z$ to get back some value $x' = x'_1(\circ)x'_2$, and then returns x'_1.



What happens when $\mathcal{A}$ succeeds? This means that the x' that $\mathcal{A}$ returns is such that $f(x'_1) \oplus x'_2 = f_1(x') = w = y \oplus z$. Because f is length preserving and y and z have the same length, we know that $f(x'_1) = y$ and $x'_2 = z$. Therefore, the x'_1 that $\mathcal{B}$ returns is a preimage of y.

This means that when $\mathcal{A}$ succeeds, so does $\mathcal{B}$, which further implies that the probability of $\mathcal{B}$ succeeding is at least the probability of $\mathcal{A}$ succeeding inside $\mathcal{B}$. Since the input to $\mathcal{A}$ inside $\mathcal{B}$ is distributed identically to the input to $\mathcal{A}$ in the wild, the probability of $\mathcal{A}$ succeeding inside $\mathcal{B}$ is equal to the probability of $\mathcal{A}$ succeeding in the wild, which is non-negligible by assumption. So the probability of $\mathcal{B}$ succeeding is also non-negligible. But this means that $\mathcal{B}$ is an inverter for the one-way function $f(x)$ that works with non-negligible probability, which is a contradiction. So $f_a(x)$ must be a one-way function.

3. (3 points) Prove that one-way functions cannot have polynomial-size ranges. More precisely, prove that if f is a one-way function, then for every polynomial $p()$ and all sufficiently large n's, $|\{f(x) : x \in \{0,1\}^n\}| > p(n)$

4. (3 points) Let f be a one-way function. Prove that $g(x) = f(x_1)$, where $x = x_1(\circ)x_2$, is a one-way function.