CS6111: Foundations of Cryptography

Assignment 2 - CS16B107

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 $\{1\} \cup \{2, 4, 6, 8 \cdots\} \subset \mathbb{R}$.

   Solution: Consider the set $\mathbb{G} = \mathbb{R} - \{0\}$. This is a group for the associated operation of multiplication of real numbers. 1 is the identity of the set. Now consider the set $\mathbb{H} = \{1\} \cup \{2, 4, 6, 8 \cdots\} \subset \mathbb{G}$. This subset satisfies both conditions in the proposition. However, it is not a subgroup because inverse of element 2 under the multiplication operation does not exist within $\mathbb{H}$. Hence The proposition is false.

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?

   Solution:

Closure

For all g^i, g^j in $< g >$, $g^i.g^j = g^{i+j}$ also belongs to $< g >$.

Existence of Identity

$g^0 = 1$ exists in $< g >$.

Existence of Inverse

Let $m = |G|$ be the order of the set. Therefore, for any element $g \in G$, we have

$$g^m = 1$$

$$\implies g^i.g^{m-i} = 1 \ , \ \forall i \in \{0, 1, 2, .., m-1\}$$

$$\implies g^i.g^{m-(i \mod m)} = 1 \ , \ \forall i \geq 0$$

$$\implies (g^i)^{-1} = g^{m-(i \mod m)} \ , \ \forall i \geq 0$$

Thus for all $g^i \in < g >$, its inverse also belongs to $< g >$.

Associativity

Property maintained from the original group G.

Hence $< g >$ is a subgroup. If G were infinite, then the Existence of Inverse cannot be proven and hence it need not be a subgroup. For instance, let G be the set of non-zero real numbers for the multiplication operation. Let the subset be $< g > = \{1, 2, 4, 8, 16, ..\}$. $< g >$ does not contain the inverse of element 2 and is hence not a subgroup.

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.

Solution: Since we already know that the property holds for any $x \in \mathbb{Z}_N^*$, we only need to additionally show that it also holds for all $x \in \mathbb{Z}_N - \mathbb{Z}_N^*$. These x are either of form $x = ap$ where $a < q$ or of form $x = bq$ where $b < p$. We prove for the latter case and the proof for the former is similar.

Since $q \neq p$ and $b < p$, we have that $p \nmid bq$. Thus, by Fermatt's Little Theorem, we have

$$(bq)^{p-1} \equiv 1 \mod p$$

Raising both sides of the modulo equation by power $k(q-1)$, for some non-negative integer k, we have

$$(bq)^{k(p-1)(q-1)} \equiv 1^{k(q-1)} \mod p \implies (bq)^{k(p-1)(q-1)} \equiv 1 \mod p$$

$$\implies (bq)^{k(p-1)(q-1)+1} \equiv bq \mod p$$

$$\implies p \mid ((bq)^{k(p-1)(q-1)+1} - bq)$$

Since $\phi(N) = (p-1)(q-1)$ and k can be any non-negative integer, the above equation can be rewritten for any e,d with $ed = 1 \mod \phi(N)$ as follows.

$$\implies p \mid ((bq)^{ed} - bq)$$

Also, since $q|(bq)$, we also have

$$\implies q \mid ((bq)^{ed} - bq)$$

Since p and q are primes and $p \neq q$, p and q are coprime. Thus we can combine the above two statements as

$$\implies (pq) \mid ((bq)^{ed} - bq)$$

$$\implies N \mid ((bq)^{ed} - bq)$$

$$\implies (bq)^{ed} \equiv bq \mod N$$

Similarly, we can prove for the case when $x = ap$ where $a < q$. Thus the property is true for all $x \in \mathbb{Z}_N$

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.

Solution:

$$pq = N$$

$$p + q = -(pq - p - q + 1) + pq + 1 = -(p-1)(q-1) + pq + 1 = -\phi(N) + N + 1$$

We have the sum and product of p and q. Therefore, we can construct a quadratic polynomial whose roots are p and q.

$$x^2 - (p+q)x + pq = 0$$

That is,

$$x^2 + (\phi(N) - N - 1)x + N = 0$$

The roots of the above quadratic polynomial are p and q and they can be computed in polynomial time using the quadratic formula.

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 $\phi(n)$.)

Solution:

$$3d = 1 \mod \phi(N)$$

$$\implies 3d - 1 = k\phi(n) \; for \; some \; k \in \mathbb{N}$$

Thus $\phi(N)$ is a factor of $3d-1$. If p and q are large primes, then $\phi(N) = (p-1)(q-1)$ is relatively closer to $N = pq$. Thus, in order to efficiently get possible values of $\phi(N)$, we do the following

- find $x_0 = \lfloor \frac{3d-1}{N} \rfloor$
- We choose natural number values of x close to x_0. For each of these, we see if $\frac{3d-1}{x}$ is an integer. If so, it is a possible value for $\phi(N)$.

For each of these possibilities, we can apply the polynomial time method described in the previous solution. Thus the overall method still takes polynomial time.

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.

Solution: $\mu(.)$ and $\nu(.)$ are negligible functions. Thus, for all $c \in \mathbb{N}$, we have m_c and n_c such that

$$\mu(m) \leq \frac{1}{m^c} \;\; \forall m \geq m_c$$

$$\nu(n) \leq \frac{1}{n^c} \;\; \forall n \geq n_c$$

Now consider the function $\mu(.) \cdot \nu(.)$. For any $c \in \mathbb{N}$, let $k_c = max(m_{\lfloor c/2 \rfloor}, n_{\lfloor c/2 \rfloor})$. Thus for all $k \geq k_c$, we have

$$\mu(k).\nu(k) \leq \frac{1}{k^{\lfloor c/2 \rfloor}} . \frac{1}{k^{\lfloor c/2 \rfloor}}$$

$$\implies \mu(k).\nu(k) \leq \frac{1}{k^c}$$

Thus $\mu(.) \cdot \nu(.)$ is also 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.

Solution: $\mu()$ is a negligible function. By replacing c by $c+1$ in the definition of negligible functions, we have

$$\forall c \in \mathbb{N}, \;\; \exists n_0 \in \mathbb{N} \;\; such \; that \; \mu(x) \leq \frac{1}{x^{c+1}} \;\; \forall x \geq n_0$$

Assume that $f()$ has a positive degree and that the leading coefficient of $f()$ is positive. Then,

$$\forall n_0 \in \mathbb{N},\ \ \exists n_1 \in \mathbb{N}\ \ \textit{such that } f(n) \geq n_0\ \ \forall n \geq n_1$$

Combining the above two equations that share the value of n_0 (by replacing x with $f(n)$, we have

$$\forall c \in \mathbb{N},\ \ \exists n_1 \in \mathbb{N}\ \ \textit{such that } \mu(f(n)) \leq \frac{1}{f(n)^{c+1}}\ \ \forall n \geq n_1$$

Since $f()$ has degree ≥ 1 ,

$$\forall c \in \mathbb{N},\ \ \exists n_2 \in \mathbb{N}\ \ \textit{such that } (f(n))^{c+1} \geq n^c\ \ \forall n \geq n_2$$

Combining the above two equations with $n_c = max(n_1, n_2)$, we have

$$\forall c \in \mathbb{N},\ \ \exists n_c \in \mathbb{N}\ \ \textit{such that } \mu(f(n)) \leq \frac{1}{n^c}\ \ \forall n \geq n_c$$

Thus $\mu(f())$ is also negligible.

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

Solution: Assume that one-way functions exist. Let f(x)=y be one such one-way functions. Consider the corresponding computational problem $\mathcal{C}$.

- Given a problem instance (y, x), we can compute f(x) in polynomial time (as f is one-way). Thus we can verify $y = f(x)$ in polynomial time. Hence $\mathcal{C} \in NP$.
- Given an instance y, we cannot find a $x_0 \in domain(f)$ in polynomial time such that $y = f(x_0)$ (as f is one-way). Thus we cannot find a valid inverse of y (if it exists) in polynomial time. Hence $\mathcal{C} \notin P$.

Thus we have an element which belongs to NP but not to P. Hence, $P \neq NP$.

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

Solution: $f : A \rightarrow B$, where, $A = \{0,1\}^n$ and $B = \{0,1\}^{\lfloor \log_2 n \rfloor}$. $|A| = 2^n$ and $|B| = 2^{\lfloor \log_2 n \rfloor} = n$. Since f is a mapping from A to B, there exists a $y_0 \in B$ and $S \subseteq A$ such that $|S| \geq \frac{|A|}{|B|} = \frac{2^n}{n}$ and

$$f(x) = y_0\ \forall\ x \in S$$

Let us choose an $x_0 \in S$. We consider the inverter I that has the property that $I(y) = x_0\ \forall\ y \in B$

$$
\begin{aligned}
Pr[f(I(f(x))) = f(x)] &= Pr[f(I(f(x))) = f(x)|x \in S].Pr[x \in S] + Pr[f(I(f(x))) = f(x)|x \notin S].Pr[x \notin S] \\
&\geq Pr[f(I(f(x))) = f(x)|x \in S].Pr[x \in S] \\
&= Pr[f(x_0) = f(x)|x \in S].Pr[x \in S] \\
&= Pr[x \in S] \\
&= \frac{|S|}{|A|} \\
&\geq \frac{2^n/n}{2^n} \\
&= \frac{1}{n} = non - negligible
\end{aligned}
$$

Thus, the inverter I has non-negligible success probability. Thus, f is not one-way.

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?

Solution: Let $g : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Let us construct function $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ as follows.

$$f(x) = f(x_0||x_1) = 0^n||g(x_0)$$

where, x_0 is the first n bits of x. By construction, this function f is also one-way, since finding preimages for hf(x) is at least as hard as finding preimages for $g(x_0)$. (Note that the size of input is only changed as $n \to 2n$ and a polynomial in 2n is also a polynomial in n.)

Now, let $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be constructed as $f'(x) = f(x) \oplus x$. Thus, when x_0 is the first n bits of x, we have

$$
\begin{aligned}
f'(x) = f'(x_0||x_1) = f(x_0||x_1) \oplus (x_0||x_1) = (0^n||g(x_0)) \oplus (x_0||x_1) = (0^n \oplus x_0)||(g(x_0) \oplus x_1) \\
= x_0||(g(x_0) \oplus x_1)
\end{aligned}
$$

For any $x \in \{0,1\}^{2n}$, we can find a valid inverse of $y = f'(x)$ in polynomial time using these steps.

- get x_0 = first n bits of y.
- compute $g(x_0)$ in polynomial time (as g is one-way).
- Let y_1 be the last n bits of y. Then, $x_1 = (g(x_0) \oplus x_1) \oplus g(x_0) = y_1 \oplus g(x_0)$ and can be computed in polynomial time.
- $x' = x_0||x_1$ is one valid inverse of y.

Thus, we see that $f(x) \oplus x$ need not always be one-way, even though f(x) is.

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 $f(x)$.

Solution: $g(x)$ denotes the $n - \log n$ higher order bits of $f(x)$. Let $f_1(x)$ denote the remaining $\log n$ bits.

Proof by contradiction. Assume that g is not one-way. Thus, there exists a polynomial $p(n)$ for an inverter I such that

$$Pr[g(I(g(x))) = g(x)] \geq \frac{1}{p(n)}$$

Let us consider the same inverter for f. This inverter only requires the first $n - \log n$ bits of f(x). Thus we have

$$\begin{aligned} Pr[f(I(f(x))) = f(x)] &= Pr[f(I(g(x))) = f(x)] \\ &= Pr[g(I(g(x))) = g(x)].Pr[f_1(I(g(x))) = f_1(x)] \\ &\geq \frac{1}{p(n)}.Pr[f_1(I(g(x))) = f_1(x)] \end{aligned}$$

Since a bit string with $\log n$ bits has at most n possibilities, we have

$$Pr[f_1(I(g(x))) = f_1(x)] = \frac{1}{n}$$

Using this in the above inequality, we have

$$Pr[f(I(f(x))) = f(x)] \geq \frac{1}{np(n)} = \frac{1}{polynomial(n)}$$

Thus, we get that f() is not one-way, which is a contradiction. Hence, our assumption is wrong. Hence, g() is also a one-way function.

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

Solution: Let $g : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Let us construct function $h : \{0,1\}^{2n} \to \{0,1\}^{2n}$ as follows.

$$h(x) = h(x_0||x_1) = 0^n||g(x_0)$$

where, x_0 is the first n bits of x. By construction, this function h is also one-way, since finding preimages for h(x) is at least as hard as finding preimages for $g(x_0)$. (Note that the size of input is only changed as $n \to 2n$ and a polynomial in 2n is also a polynomial in n.)

However, by construction, for any $x \in \{0,1\}^{2n}$

$$h(h(x)) = h(h(x_0||x_1)) = h(0^n||g(x_0)) = 0^n||g(0^n) = constant$$

Thus, for any $y \in \{0,1\}^{2n}$, we can choose any random $x \in \{0,1\}^{2n}$ such that $h(h(x)) = z$. Hence, h(h(x)) is not one-way even though h(x) is.

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 $x = x_1(\circ)x_2$.

> **Solution:** Let $f : \{0,1\}^n \to \{0,1\}^n$ and $f_a : \{0,1\}^{2n} \to \{0,1\}^{2n}$.
>
> Consider the following inverter for f_a. For any $y \in \{0,1\}^n$, it returns $x' = 0^n||(y \oplus f(0^n))$. Since f is one-way, $f(0^n)$ and hence x' can be computed in polynomial time.
>
> $$f_a(x') = f_a(0^n||(y \oplus f(0^n))) = f(0^n) \oplus (y \oplus f(0^n)) = y$$
>
> Thus f_a is not a one-way function.

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.

   image.png

   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.

Solution: The fault lies in the statement "Because f is length preserving and y and z have the same length, we know that $f(x'_1) = y$ and $x'_2 = z$."

$$f(x'_1) \oplus x'_2 = y \oplus z \;\not\Longrightarrow\; f(x'_1) = y \;\; and \;\; x'_2 = z$$

Thus, even if $\mathcal{A}$ succeeds in getting x'_1 and x'_2, it might happen that $x'_2 \neq z$ and thus $f(x'_1) \neq y$. So, success probability of $\mathcal{B}$ cannot be proven to be greater than success probability of $\mathcal{A}$.

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, $|\{f(x) : x \in \{0,1\}^n\}| > p(n)$

Solution: Proof by contradiction. Assume $|\{f(x) : x \in \{0,1\}^n\}| \leq p(n)$ for some polynomial p() and sufficiently large n.

$f : A \rightarrow B$, where, $A = \{0,1\}^n$, $|A| = 2^n$ and $|B| = p(n)$. Since f is a mapping from A to B, there exists a $y_0 \in B$ and $S \subseteq A$ such that $|S| \geq \frac{|A|}{|B|} = \frac{2^n}{p(n)}$ and

$$f(x) = y_0 \; \forall \; x \in S$$

Let us choose an $x_0 \in S$. We consider the inverter I that has the property that $I(y) = x_0 \; \forall \; y \in B$

$$\begin{aligned}
Pr[f(I(f(x))) = f(x)] &= Pr[f(I(f(x))) = f(x)|x \in S].Pr[x \in S] + Pr[f(I(f(x))) = f(x)|x \notin S].Pr[x \notin S] \\
&\geq Pr[f(I(f(x))) = f(x)|x \in S].Pr[x \in S] \\
&= Pr[f(x_0) = f(x)|x \in S].Pr[x \in S] \\
&= Pr[x \in S] \\
&= \frac{|S|}{|A|} \\
&\geq \frac{2^n/p(n)}{2^n} \\
&= \frac{1}{p(n)} = non-negligible
\end{aligned}$$

Thus, the inverter I has non-negligible success probability. Thus, f is not one-way.

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.

Solution: Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ and $g : \{0,1\}^{2n} \rightarrow \{0,1\}^n$. We prove the contra-positive. Assuming g() is not one-way, we show that it implies f() is not one-way. Since we assume g() is not one-way, there exists a PPT inverter $\mathcal{A}$ and polynomial p() such that

$$\underset{x \in \{0,1\}^{2n}}{Pr}[g(A(g(x))) = g(x)] \geq \frac{1}{p(2n)}$$

Let $x = x_1(\circ)x_2$. Since $p(2n) = q(n)$ for some other polynomial q(), we have

$$\Pr_{x_1 \in \{0,1\}^n,\ x_2 \in \{0,1\}^n}[g(A(g(x_1||x_2))) = g(x_1||x_2)] \geq \frac{1}{q(n)}$$

$$\implies \Pr_{x_1 \in \{0,1\}^n,\ x_2 \in \{0,1\}^n}[g(A(f(x_1))) = f(x_1)] \geq \frac{1}{q(n)}$$

The probability becomes independent of x_2.

$$\implies \Pr_{x_1 \in \{0,1\}^n}[g(A(f(x_1))) = f(x_1)] \geq \frac{1}{q(n)}$$

Let $A(f(x_1)) = x_1'||x_2'$, where x_1' and x_2' are from $\{0,1\}^n$.

$$\implies \Pr_{x_1 \in \{0,1\}^n}[g(x_1'||x_2') = f(x_1)] \geq \frac{1}{q(n)}$$

$$\implies \Pr_{x_1 \in \{0,1\}^n}[f(x_1') = f(x_1)] \geq \frac{1}{q(n)}$$

The LHS of the above equation is the success probability of the following PPT inverter B defined for f() as follows. For any $y \in \{0,1\}^n$, B does the following

- get $A(y) = x_1'||x_2'$ in polynomial time.
- return x_1'

Since success probability of B is non-negligible, it implies f is not one-way. Hence proved.