*Last updated April 1, 2009*

# Midterm

This midterm exam is due by email to luca@cs.berkeley.edu at noon, on Thursday, April 9, 2009. Put the word "midterm" in the subject line.

Some notes that apply to various problems:

- We use $||$ to denote string concatenation. For example if $a = 011$ and $b = 101$, then $a||b = 011101$.
- If $a$ and $b$ are bit strings, then $a + b$ is the bitwise xor of $a$ and $b$. For example if $a = 011$ and $b = 101$, then $a + b = 110$.
- About the use of $O()$ notation: When we ask to prove that "If $X$ is $(t, \epsilon)$-secure then $Y$ is $(t - O(r), \epsilon)$-secure," we mean "Prove that there is a $c$ such that, for all $t \geq 2$, $r \geq 2$ and $0 < \epsilon \leq 1$, it holds that if $X$ is $(t, \epsilon)$-secure then $Y$ is $(t - c \cdot r, \epsilon)$-secure." That is, the constant in the $O()$ notation must be independent of all other parameters $t, r, \epsilon$, and be entirely determined by the details of your reduction and the specific definition of the model of computation. (That is, what precisely can be computed in one step of computation.)
- Solve the problems individually, do not collaborate with your classmates or others.
- If in doubt, do not hesitate to ask for clarifications. Maybe that there is a typo that make a problem unsolvable as stated.

Solve the following problems:

1. **Using a pseudorandom generator to reduce key length [20 points]**

   Let $G : \{0,1\}^{256} \to \{0,1\}^{1024}$ be a $(2^{90}, 2^{-40})$-secure pseudorandom generator, and $F : \{0,1\}^{1024} \times \{0,1\}^{128} \to \{0,1\}^{128}$ be a $(2^{80}, 2^{-40})$-secure pseudorandom function which is computable with complexity $\leq 1,000,000$. (That is, $F$ has a 1024-bit key, a 128-bit input and a 128-bit output.)

   Consider the function $F' : \{0,1\}^{256} \times \{0,1\}^{128} \to \{0,1\}^{128}$ defined as

   $$F'_K(x) := F_{G(K)}(x)$$

   Prove that $F'$ is a $(2^{70}, 2^{-39})$-secure pseudorandom function.

2. **Encryption using a Pseudorandom Permutation [30 points].**

   Suppose $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m$ is a $(t, \epsilon)$-secure pseudorandom permutation computable in time $\leq r$ and $I : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m$ is its inverse, also computable in time $\leq r$.

   Consider the following scheme encryption scheme $(E, D)$ to encrypt blocks of $m/2$ bits.

   - $E(K, M)$: pick a random $R \in \{0,1\}^{m/2}$, output $F(K, (M||R))$.
   - $D(K, C)$: compute $M' := I(K, C)$, output the first $m/2$ bits of $M'$

   Show that $(E, D)$ is $(t/O(r), 2\epsilon + 2 \cdot t \cdot 2^{-m/2})$ CCA-secure.

3. **MACs from cryptographic hash functions. [15 points]**

   Suppose that $H : \{0,1\}^k \times \{0,1\}^{2m} \to \{0,1\}^m$ is a family of $(t, \epsilon)$-secure collision-resistant hash functions. Consider the following candidate MAC scheme for signing $m$-bit messages:

   - Secret key: a random $m$-bit string $K$;
   - $Tag(K, M)$ : pick a random $s \in \{0,1\}^k$, and output the tag $s||H_s(K||M)$
   - $Verify(K, M, (s||h))$ check that $h = H_s(K||M)$

   Show that, just from the assumption that $H$ is $(t, \epsilon)$-secure, it is not possible to deduce the security of the above scheme.

   In more detail: show that if a family of $(t, \epsilon)$-secure collision-resistant hash functions $H : \{0,1\}^k \times \{0,1\}^{2m} \to \{0,1\}^{m-1}$ exists, then there is a family $H' : \{0,1\}^k \times \{0,1\}^{2m} \to \{0,1\}^m$ that is still $(t, \epsilon)$-secure but is such that if $H'$ is used in the above construction, then there is an attack that runs in linear time $O(k + m)$ and produces a forged tag with probability 1 after seeing only one message-tag pair.

4. **One-way functions and function composition. [20 points]**

   Let $f : \{0,1\}^n \to \{0,1\}^n$ a $(t, \epsilon)$ one-way function and $g : \{0,1\}^n \to \{0,1\}^n$ be a bijection computable in time $\leq r$.

   (a) Show that $h_1(x) := g(f(x))$ is $(t - r, \epsilon)$-one way.

   (b) Show that $h_2(x) := f(g(x))$ is $(t - r, \epsilon)$-one way.

5. **Composition of Pseudorandom Generators. [15 points]**

   Suppose that $H, G : \{0,1\}^n \to \{0,1\}^{2n}$ are $(t, \epsilon)$-secure pseudorandom generators computable in time $\leq r$.

Prove that the mapping $B : \{0,1\}^{2n} \to \{0,1\}^{4n}$ defined as

$$B(x, y) := G(x)||H(y)$$

is a $(t - O(r + n), 2\epsilon)$-secure pseudorandom generator.