Cryptology I (spring 2015)	Dominique Unruh
Exercise Sheet 6	
Out: 2015-05-27	Due: 2015-06-02

Problem 1: Negligible functions

Which of the following facts are true and which are false? Prove your answers.

(a) If f and g are negligible, then $f+g$ is negligible.

(b) If f and g are negligible, then fg is negligible.

(c) If f is negligible and g is an arbitrary positive function, then $f+g$ is negligible.

(d) If f is negligible and c is a positive constant, then cf is negligible.

(e) $f(n) := 1/n^{10}$. f is negligible.

(f) $f(n) := 2^{-n}$. f is negligible.

(g) If $\lim_{n\to\infty} f(n) = 0$, then f is negligible.

(h) If f is negligible, then $\lim_{n\to\infty} f(n) = 0$.

(i) $f(n) := 2^{-n}$ for even n and $f(n) := 1$ for odd n. f is negligible.

Problem 2: One-way functions

Which of the following are one-way functions? Why (short argument, no proof)? (You may assume that the RSA assumption holds. And that E_{AES} is a PRF.)

Remember that to break a one-way function, it is sufficient to find some preimage, not necessarily the "true" one that was fed into the one-way function.

(a) $f(x) := 0$ for all $x \in \{0,1\}^\eta$.

(b) $f(x) := x_1 \dots x_{\eta/2}$ for $x \in \{0,1\}^\eta$.

(c) $f(N,e,x) := (N,e,x^e \bmod N)$ where the domain of f is the set of all (N,e,x) where N is an RSA modulus, e is relatively prime to N, and $x \in \{0,\dots,N-1\}$.

(d) $f(N,e,x) := x^e \bmod N$ where the domain of f is the set of all (N,e,x) where N is an RSA modulus, e is relatively prime to N, and $x \in \{0,\dots,N-1\}$.

(e) $f(k,x) := E_{AES}(k,x)$.

(f) $f(x) := g(x)\|g(x)$ where g is a one-way function.

Note: Here (and in (g)), the question is whether f would be a one-way function for *every* one-way function g.

(g) $f(x) := g(g(x))$ where g is a one-way function.

Hint: The first thought here might be wrong. Remember that a one-way function g might not be surjective. E.g., the first half of $g(x)$ might always consist of zeroes.

Problem 3: Merkle-Damgård and the ROM

In the lecture, I explained the random oracle heuristic which suggests to model a hash function as a random oracle. It should be added that a (preferable) refinement of this heuristic is to model the compression function itself as a random oracle, and to model the hash function as some function constructed based on that compression function (using, e.g., Merkle-Damgård). The reason behind this is that constructions like Merkle-Damgård do not produce functions that behave like random functions (even if the underlying compression function is a random function).

Give an example why a hash function H constructed using the Merkle-Damgård construction should not be modeled as a random oracle. More precisely, find a cryptographic scheme which is secure when H is a random oracle (no security proof needed), but which is insecure when H is a Merkle-Damgård construction (even if the compression function is a random oracle).

Hint: Consider the construction of MACs from hash functions that is insecure when the hash function is constructed with Merkle-Damgård.