E0 235 : Cryptography	**Question Set**
Tutorial 4	
Instructor: Arpita Patra	*Jan 27, 2017*

Question 1

Let f, g be length-preserving one-way functions (so, e.g., $|f(x)| = |x|$). For each of the following functions f', decide whether it is necessarily a one-way function (for arbitrary f, g) or not. If it is, prove it. If not, show a counterexample.

(a) $f'(x) = f(x) \oplus g(x)$

(b) $f'(x_1||x_2) = f(x_1) \;||\; g(x_2)$

Question 2

Let F be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ as follows: On input $m \in \{0,1\}n/2$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}n/2$ of length $n/2$ and computes $c := F_k(r||m)$. Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

Question 3

Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $l(n) = n+1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

(a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

(c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Question 4

Let $F' : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a length-preserving pseudorandom function. For the following constructions of a keyed function F', state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

(a) $F' : \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^n$ such that

$$F'_K(x_1||x_2) = F_K(x_1) \oplus F_K(x_2)$$

for all $x_1, x_2 \in \{0,1\}^n$ and $K \in \{0,1\}^k$.

(b) $F' : \{0,1\}^{2k} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ such that

$$F'_{K_1||K_2}(x_1||x_2) = F_{K_1}(x_1) \oplus F_{K_2}(x_2)$$

for all $x_1, x_2 \in \{0,1\}^n$ and $K_1, K_2 \in \{0,1\}^k$.

(c) $F' : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ such that

$$F'_K(x) = F_K(x) \oplus x$$

for all $x \in \{0,1\}^n$ and $K \in \{0,1\}^k$.

Question 5

For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}(\cdot)$ to be a probabilistic oracle that, on input 1^n, chooses uniform $r \in \{0,1\}^n$ and returns $\langle r, g(r)\rangle$. A keyed function F is a *weak pseudorandom* function if for all PPT algorithms D, there exists a negligible function $negl$ such that:

$$| \ \mathsf{Pr}\left[D^{F_k^{\$}(\cdot)}(1^n) = 1\right] - \mathsf{Pr}\left[D^{f_k^{\$}(\cdot)}(1^n) = 1\right] \ | \leq negl(n)$$

where $k \in \{0,1\}^n$ and $f \in Func_n$ are chosen uniformly.

(a) Prove that if F is pseudorandom then it is weakly pseudorandom.

(b) Let F' be a pseudorandom function, and define

$$F_k(x) \stackrel{def}{=} \begin{cases} F'_k(x) & \text{if } x \text{ is even} \\ F'_k(x+1) & \text{if } x \text{ is odd} \end{cases}$$

Prove that F is weakly pseudorandom, but not pseudorandom.

References

1. Jonathan Katz, Yehuda Lindell : Introduction to Modern Cryptography, Second Edition