| **Cryptography** | **Question Set** |
|---|---|
| Tutorial | |
| *Instructor: Arpita Patra* | *Jul 31, 2018* |

## Question 1

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 2

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 $K_1, K_2 \in \{0,1\}^k$.

## Question 3

Let $G$ be a pseudorandom generator and define $G'(s)$ to be the output of $G$ truncated to $n$ bits (where $|s| = n$). Prove that the function $F_k(x) = G'(k) \oplus x$ is not pseudorandom.

## Question 4

Suppose an algorithm $G$ is a pseudorandom generator. Let $\overline{G}$ be the following algorithm, on input seed $s$, run $G(s)$ to get $w$, then negate every bit of $w$ to get $\overline{w}$ (i.e., for bit $i$, $\overline{w_i} = 1 - w_i$), and output the result. Prove $\overline{G}$ is a pseudorandom generator.

## Question 5

Suppose algorithms $G_1$ and $G_2$ are pseudorandom generators. Let $G_3$ be the following algorithm: on input $s$, $G_3$ runs $G_1(s)$ to get $w_1$, runs $G_2(s)$ to get $w_2$, and outputs the concatenation of the two strings: $w_3 = w_1 \mid\mid w_2$. Show that $G_3$ is not necessarily a pseudorandom generator. (Hint: Use what you proved in Question 1.)

# Exercise Questions

## Question 1

Let $F$ be a length-preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether $F'$ is a pseudorandom function. If yes, prove it; if not, show an attack.

(a) $F'_k(x) \stackrel{def}{=} F_k(0||x)||F_k(1||x)$

(b) $F'_k(x) \stackrel{def}{=} F_k(0||x)||F_k(x||1)$

## Question 2

Let $F$ be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows: On input $m \in \{0,1\}n/2$ and key $k \in \{0,1\}^n$, algorithm $\mathsf{Enc}$ 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 $n/2$.

# References


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