Introduction to Cryptography – LMAT2450
Practical Lesson 3

Clément Hoffmann (clement.hoffmann@uclouvain.be)
Yaobin Shen (yaobin.shen@uclouvain.be)

October 19, 2022

Exercise 1 *(Pseudo-random Function)*

Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a (length-preserving) pseudorandom function, that is, if k is selected uniformly at random in $\{0,1\}^n$, then $F_k(\cdot)$ is computationally indistinguishable from a function f selected randomly in the set of functions from $\{0,1\}^n$ to $\{0,1\}^n$. More formally, $\forall$ PPT D, $\exists$ negl. ϵ:

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

Show that no length-preserving function F can offer the same guarantees in front of an adversary who has an unbounded computational power, that is, for every length-preserving function F, there is a (possibly unbounded) distinguisher D such that the difference of probabilities in the equation above is not negligible.

Exercise 2 *(Pseudo-random Permutation, Katz & Lindell 3.18)*

Let F be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ as follows: On input $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a random string $r \leftarrow \{0,1\}^{n/2}$ 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 $n/2$. (If you are looking for a real challenge, prove that this scheme is *CCA-secure* if F is a *strong* pseudorandom permutation.)

Exercise 3 *(CBC, Katz & Lindell 3.20)*

Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

Exercise 4 (*Reduction and/or attacks*)

Let $\Pi_1 = \langle \mathrm{Gen}^1, \mathrm{Enc}^1, \mathrm{Dec}^1 \rangle$ and $\Pi^2 = \langle \mathrm{Gen}^2, \mathrm{Enc}^2, \mathrm{Dec}^2 \rangle$ be an encryption scheme with $\mathrm{Enc}^1 : \mathcal{K} \times \mathcal{M}^1 \longmapsto \mathcal{C}^1$ and $\mathrm{Enc}^2 : \mathcal{K} \times \mathcal{M}^2 \longmapsto \mathcal{C}^2$

1. If $\mathcal{C}^1 = \mathcal{M}^2$, let $\Pi = \langle \mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec} \rangle$ with
   - $\mathrm{Gen} := (\mathrm{Gen}_1, \mathrm{Gen}_2)$ (that is, we obtain two different keys (k_1, k_2)
   - $\mathrm{Enc}_{(k_1,k_2)}(m) := \mathrm{Enc}^2_{k_2}(\mathrm{Enc}^1_{k_1}(m))$
   - $\mathrm{Dec}_{(k_1,k_2)}(c) := \mathrm{Dec}^1_{k_1}(\mathrm{Dec}^2_{k_2}(c))$

(a) If Π^1 is CPA secure, is Π CPA secure?

(b) If Π^2 is CPA secure, is Π CPA secure?

(c) If Π is CPA secure, is Π^1 CPA secure?

(d) If Π is CPA secure, is Π^2 CPA secure?

2. If $\mathcal{M}^1 = \mathcal{M}^2$ and $\mathcal{C}^1 = \mathcal{C}^2$. let $\Pi' = \langle \text{Gen}', \text{Enc}', \text{Dec}' \rangle$ with

- $\text{Gen}' := (\text{Gen}^1, \text{Gen}^2)$ (that is, we obtain two different keys (k_1, k_2)
- $\text{Enc}'_{(k_1,k_2)}(m) := (c_1, c_2)$ with $c_1 = \text{Enc}^1_{k_1}(m),\ c_2 = \text{Enc}^2_{k_2}(m))$
- $\text{Dec}'_{(k_1,k_2)}(c) := \text{Dec}_{k_1}(c_1)$ with $c = c_1 \| c_2$ (c_1 is the first half of c)

(a) If Π^1 is CPA secure, is Π' CPA secure?

(b) If Π^2 is CPA secure, is Π' CPA secure?

(c) If Π' is CPA secure, is Π^1 CPA secure?

(d) If Π' is CPA secure, is Π^2 CPA secure?