Introduction to Cryptography
Exercise Week 5

Dr. Patrick Struck
patrick.struck@uni.kn

Leon Weingarten
leon.weingarten@uni.kn

Jonah Herr
jonah.herr@uni.kn

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

(a) $F'_k(x) := F_k(0||x) \,||\, F_k(0||x)$.

(b) $F'_k(x) := F_k(0||x) \,||\, F_k(x||0)$.

Exercise 2.
Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Consider the following encryption scheme:

1. Gen: On input 1^n, choose uniform $k \in \{0,1\}^n$ and output it as the key.
2. Enc: Given a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, output the ciphertext
$$c := F_k(0^n) \oplus m.$$
3. Dec: Given a key $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^n$, output the message
$$m := F_k(0^n) \oplus c.$$

Prove that this scheme is not secure in the sense of

(a) EAV-security for multiple encryptions.

(b) CPA-security.

(c) CPA-security for multiple encryptions.

(d) CPA-security for multiple encryptions, with the additional requirement that the adversary can never query a message twice.

Hint: Compare this scheme to Construction 3.28. What is different here and what consequences does this have?

Exercise 3.

Say CBC-mode encryption is used with a block cipher having a 256-bit key and 128-bit block length to encrypt to a 1024-bit message. What is the length of the resulting ciphertext?

Exercise 4.

Prove that chained CBC mode is not CPA-secure.