Introduction to Cryptography
Exercise Week 4

Dr. Patrick Struck
patrick.struck@uni.kn

Leon Weingarten
leon.weingarten@uni.kn

Jonah Herr
jonah.herr@uni.kn

Exercise 1.
Prove Proposition 3.6 from the lecture:

Let negl_1 and negl_2 be negligible functions. Then,

1. $\mathsf{negl}_3(n) := \mathsf{negl}_1(n) + \mathsf{negl}_2(n)$ is negligible.
2. For any polynomial p, the function $\mathsf{negl}_4(n) := p(n) \cdot \mathsf{negl}_1(n)$ is negligible.

Exercise 2.
Prove that Definition 3.8 cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is *not* restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

Hint: Let p be a polynomial. Why is it very likely that the resulting ciphertext from encrypting a string of length greater than $p(u)$? is of length $u + p(u)$?

Exercise 3.
Prove or disprove whether each G_i is a pseudorandom generator for the following constructions:

(a) $G_1 : \{0,1\}^n \to \{0,1\}^{2n}, G_1(s) := s_1||s_1|| \dots ||s_n||s_n$.

(b) $G_2 : \{0,1\}^n \to \{0,1\}^{2n}, G_2(s) := s||s$.

(c) Let G be a pseudorandom generator. Define $G_3(s) := G(\overline{s})$ where $\overline{s}$ is the complement of s.

(d) Again let G be a PRG and define $G_4(s) := \overline{G(s)}$, i.e. the complement of $G(s)$.