Problem 3.2. *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* $PrivK^{eav}_{\mathcal{A},\Pi}$.

Since the encoder of Π is PPT, there is some bound $q(n, |m|)$, polynomial in the security parameter n and the plaintext message m, on the length of its ciphertext. The idea of the proof is to have the adversary distinguish between a single-bit message and a message which is larger than the largest ciphertext the encoder may admin.

Because Π is correct, and so encryption is injective, by the pidgeonhold principle it must hold that with with all but negligible probability that the encryption of a message is at least as long as the message.

By abuse of notation, let $q(n) = q(n, 1)$. Construct the adversary $\mathcal{A}$ as follows:

1. Receive the security parameter n. Emit $m_0 \leftarrow \{0, 1\}$ and $m_1 \leftarrow \{0, 1\}^{q(n)+1}$, uniformly at random.
2. Receive the ciphertext c. Return 0 if $|c| \leq q(n)$ and 1 otherwise.

By construction of q, if the random bit is 0, $\mathcal{A}$ always succeedes. On the other hand, if the random bit is 1, and so with all but negligible probability the length of the ciphertext is at least than $q(n) + 1$, $\mathcal{A}$ succeedes with all but negligible probability. Hence Π is not secure.

Problem 3.7. *Prove the converse of Theorem 3.18. Namely, show that if* G *is not a pseudorandom generator then Construction 3.17 does not have indistinguishable encryptions in the presence of an eavesdropper.*

Let G fail to be a pseudorandom generator, such that there exists a (PPT) distinguisher D which distinguishes outputs of G with non-negligible probability, i.e.

$$|\Pr[D(G(s)) = 1] - \Pr[D(r) = 1]| \text{ is non-negligible,} \tag{1}$$

where the probability is taken over choice of s and r and over the randomness of D.

We need to construct an adversary to Construction 3.17. Let $\mathcal{A}$ act as follows:

1. Receive the security parameter n. Emit messages m_0 and m_1 uniformly at random.
2. Receive the challenge ciphertext c. Return $D(m_1 \oplus c)$.

Let b be the bit chosen by the experiment. If $b = 1$, then

$$m_1 \oplus c = m_1 \oplus (m_1 \oplus k) = k,$$

which is $G(s)$ for a uniform random s. If $b = 0$, then $r := m_1 \oplus c$ is uniform random, since m_1 was uniform random.

Now,

$$\begin{aligned}
\Pr[\mathcal{A} \text{ succeeds}] &= \frac{1}{2}(\Pr[\mathcal{A} \text{ succeeds} \mid b = 1] + \Pr[\mathcal{A} \text{ succeeds} \mid b = 0]) \\
&= \frac{1}{2}(\Pr[D(G(s)) = 1] + \Pr[D(r) = 0]) \\
&= \frac{1}{2}(1 + \Pr[D(G(s)) = 1] - \Pr[D(r) = 1]),
\end{aligned}$$

which is non-negligible by (1).