Recall the definitions of pseudorandom generators and polynomially secure shared-key encryption. The formulations below use the notation where \{S_1, S_2, \ldots, S_k : R\} represents the distribution of the random variable \(R\) following the sequence of sampling or computational steps \(S_1, S_2, \ldots, S_k\).

**Definition 1** A function \(g : \{0,1\}^* \rightarrow \{0,1\}^*\) is a pseudorandom generator with expansion factor \(t(n)\) if
\[
\{[k \leftarrow U_n : g(k)]\}_{n \in \mathbb{N}} \approx \{[k \leftarrow U_{n+t(n)} : k]\}_{n \in \mathbb{N}}
\]
where \(U_n\) is the uniform distribution over \(\{0,1\}^n\).

**Definition 2** A pair of algorithms \(\mathrm{Enc}, \mathrm{Dec}\), and ensembles \(K = \{K_n\}_{n \in \mathbb{N}}, M = \{M_n\}_{n \in \mathbb{N}}\) are a polynomially secure encryption scheme if:

**Correctness:** For any \(n \in \mathbb{N}\) and for any \(k \in K_n\) and \(m \in M_n\) we have \(m = \mathrm{Dec}(k, \mathrm{Enc}(k, m))\).

**Secrecy:** For any two sequences of messages \(m_1 = \{m_{1,n}\}_{n \in \mathbb{N}}, m_2 = \{m_{2,n}\}_{n \in \mathbb{N}}\), where \(m_{1,n}, m_{2,n} \in M_n\), we have:
\[
\{[k \leftarrow K_n : \mathrm{Enc}(k, m_{1,n})]\}_{n \in \mathbb{N}} \approx \{[k \leftarrow K_n : \mathrm{Enc}(k, m_{2,n})]\}_{n \in \mathbb{N}}.
\]

**Question 1 (80%)**: Let \(g\) be a pseudorandom generator with expansion factor \(t(n)\). Consider the following encryption scheme \(\mathrm{Enc}, \mathrm{Dec}, K = \{K_n\}_{n \in \mathbb{N}}, M = \{M_n\}_{n \in \mathbb{N}}\), where \(K_n = \{0,1\}^n\) and \(M_n = \{0,1\}^{n+t(n)}\):
Given key \(k \in \{0,1\}^n\) and message \(m \in \{0,1\}^{n+t(n)}\), output \(c = m \oplus g(k)\), where \(\oplus\) represents bitwise exclusive or. Similarly, \(\mathrm{Dec}(k, c) = c \oplus g(k)\). Prove that \(\mathrm{Enc}, \mathrm{Dec}, K, M\) is polynomially secure.

**Bonus (60%)**: Prove the converse. That is, assume the above scheme is using some unknown function \(g\) such that the scheme is polynomially secure. Show that \(g\) is a pseudorandom generator with expansion factor \(t(n)\). (Hint: First show that if the scheme is polynomially secure then an encryption of any single message sequence \(m = \{m_n\}_{n \in \mathbb{N}}\) is computationally indistinguishable from an encryption of a random message.)

Recall the definition of a pseudorandom function ensemble:

**Definition 3** Let \(F = \{F_n\}_{n \in \mathbb{N}}\) be an ensemble of function families, where for each \(n\), the family \(F_n = \{f_k\}_{k \in \{0,1\}^n}\) consists of functions \(f_k : \{0,1\}^{a_1(n)} \rightarrow \{0,1\}^{a_2(n)}\). (That is, each function \(f_k\) in the family \(F_n\) maps strings of length \(a_1(n)\) to strings of length \(a_2(n)\).) We say that \(F\) is a pseudorandom function family ensemble if (a) there exists a polynomial time algorithm \(M\) such that \(M(k, x) = f_k(x)\) for all \(k, x\), and (b) for all feasible adversary \(A_n\) there exists a negligible function \(\nu\) such that for all large enough \(n\) we have:
\[
\Pr[k \leftarrow \{0,1\}^n : A_n^f(1) = 1] - \Pr[R \leftarrow F^{a_1(n), a_2(n)} : A_n^R = 1] < \nu(n),
\]
where \(A^f\) denotes the output of algorithm \(A\) with oracle access to function \(f\), and \(F^{a_1(n), a_2(n)}\) denotes the set of all functions from \(\{0,1\}^{a_1(n)}\) to \(\{0,1\}^{a_2(n)}\).

**Question 2 (60%)**: An ensemble of pseudorandom function families is binary if all functions in the ensemble have domain \(\{0,1\}^n\) and range \(\{0,1\}\). That is, ensemble \(F = \{F_n\}_{n \in \mathbb{N}}\) is binary if for all \(n\), \(F_n = \{f_k\}_{k \in \{0,1\}^n}\) and \(f_k : \{0,1\}^n \rightarrow \{0,1\}\). An ensemble is doubly-binary if both the domain and the range of all functions in the ensemble is \(\{0,1\}\).

(30%) Assume one way functions do not exist. Can there exist binary pseudorandom function families?

(30%) Assume one way functions do not exist. Can there exist doubly binary pseudorandom function family ensembles?