Homework 1

Due date: Thursday, February 4^{th} 11:59 PM (Gradescope)

Question 1 (24 points)

Consider each of the the following encryption schemes and state whether the scheme is perfectly secret or not. Justify your answer by giving a detailed proof if your answer is *Yes*, a counterexample if your answer is *No*.

1. An encryption scheme whose plaintext space consists of the integers $\mathcal{M} = \{0, \ldots, 10\}$ and key generation algorithm chooses a uniform key from the key space $\mathcal{K} = \{0, \ldots, 11\}$. Suppose $\mathrm{Enc_k(m) = m + k \bmod 11}$ and $\mathrm{Dec_k(c) = c - k \bmod 11}$.

2. An encryption scheme whose plaintext space is $\mathcal{M}= \{\mathrm{m} \in \{0,1\}^{\ell} | \text{the last bit of m is } 0\}$ and key generation algorithm chooses a uniform key from the key space $\{0,1\}^{\ell-1}$. Suppose $\mathrm{Enc_k(m) = m \oplus (k \,||\, 1)}$ and $\mathrm{Dec_k(c) = c \oplus (k \,||\, 1)}$.

3. Consider a encryption scheme in which M={a,b}, $K = \{K_1, K_2, \ldots, K_4\}$, and $C = \{1, 2, 3, 4, 5, 6\}$. Suppose that Gen selects the secret key k according to the following probability distribution:

$$\Pr[k = K_1] = \Pr[k = K_4] = \frac{1}{6}, \Pr[k = K_2] = \Pr[k = K_3] = \frac{1}{3}.$$

and the encryption matrix is as follows

	a	b
K_1	1	4
K_2	2	3
K_3	3	2
K_4	4	1

4. Suppose that we have an encryption scheme whose plaintext space is $\mathcal{M} = \{0,1\}^{2n}$ and whose key space is $\mathcal{K} = \{0,1\}^n$. Suppose that $\mathrm{Enc_k}(m) = m \oplus G(k)$ where $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ is a secure PRG.

Question 2 (16 points)

Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ we have $\Pr[C = c_0] = Pr[C = c_1]$

Question 3 (20 points + 5 points bonus)

Let $\epsilon > 0$ be a constant. Say an encryption scheme, $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, is *$\epsilon$-perfectly secret* if for every adversary $\mathcal{A}$ it holds that:

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \epsilon$$

(See definition 2.5 page 31)

1. (20 points) Show that *ϵ-perfect secrecy* can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ **Hint:** Start with a well known perfectly secret encryption scheme and consider reducing the keyspace.
2. (5 bonus points) Prove a lower bound on the size of $\mathcal{K}$ in term of ϵ [Challenging]

Question 4 (20 points)

(a). Let G and H be a pseudorandom generator with expansion factor $\ell(n)$. In each of the for each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, find a counter example.

1. Suppose that $\ell(n) > 2n$ and define $G'(s_1, \cdots, s_{2n}) \overset{\mathsf{def}}{=} G(s_1 \cdots s_n)$ where $\ell(n) > 2n$. Note: Each $s_i \in \{0,1\}$ is just a single bit of input.
2. Suppose that $\ell(n) > 2n$ and $G'(s_1, \ldots, s_{\lceil n/2 \rceil}) \overset{\mathsf{def}}{=} G(0^{n-\lceil n/2 \rceil}||s)$.
3. Suppose that $\ell(n) = n + 2$ and define $G'(0s) \overset{\mathsf{def}}{=} G(s)$ and $G'(1s) = H(s)$.

(b). We say that a PRG $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is (t, ϵ)-secure if for all distinguishers $\mathcal{D}$ running in time at most t we have

$$\mathbf{Adv}_{\mathcal{D},G} = \left| Pr_{s \leftarrow \{0,1\}^n} [\mathcal{D}(G(s)) = 1] - Pr_{r \leftarrow \{0,1\}^{\ell(n)}} [\mathcal{D}(r) = 1] \right| \leq \epsilon \ .$$

Suppose that G and H are both $\left(t, \epsilon_t = \frac{1.5t}{2^n}\right)$-secure PRG for all $t \leq 2^t$.

For those schemes of part **(a)** which are secure PRG, determine (t', ϵ') for the resulting G'. Your bounds should be as tight as possible e.g., a bound of the form $(t, 1.5/2^n)$-secure would be better than the bound $(t - 100n, 1.5t/2^n)$-secure. Similarly, the bound$(t - 100n, 1.5t/2^n)$-secure would better than a bound of the form $(t - 100n, 3t/2^n)$-secure which in turn would be better than a bound of the form $(\sqrt{t}, 3t/2^n)$-secure.

Question 5 (20 points)

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

1. $F'_k \stackrel{\text{def}}{=} F_k(00||x)||F_k(01||x)$.

2. $F'_k \stackrel{\text{def}}{=} F_k(00||x_1 \cdots x_{n-3}||\bar{x}_{n-2})||F_k(00||x)$, where $x = x_1 \cdots x_{n-2} \in \{0,1\}^{n-2}$ and $\bar{x}_i = x_i + 1 \mod 2$.