Name:

Purdue E-mail:

I collaborated with (...). I affirm that I wrote the solutions in my own words and that I understand the solutions I am submitting.

Homework 1

Due date: Thursday, September 13^{th} 3:00 PM

Question 1 (20 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*.

- An encryption scheme whose plaintext space consists of the integers $\mathcal{M} = \{0, ..., 12\}$ and key generation algorithm chooses a uniform key from the key space $\mathcal{K} = \{0, ..., 13\}$. Suppose $\mathrm{Enc_k(m) = m + k \bmod 13}$ and $\mathrm{Dec_k(c) = c - k \bmod 13}$.

- 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 $\mathrm{Enc_k(m) = m \oplus (k \mid\mid 0)}$ and $\mathrm{Dec_k(c) = c \oplus (k \mid\mid 0)}$.

- 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

- Suppose that we have an encryption scheme whose plaintext space is $\mathcal{M}= \{\mathrm{m} \in \{0,1\}^{2n}\}$ and whose key space is $\mathcal{K}= \{\mathrm{k} \in \{0,1\}^{n}\}$. Suppose that $\mathrm{Enc_k}(m) = m \oplus (k||F(k))$ where F is a secure length-preserving pseudorandom generator.

Question 2 (10 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 $|\mathcal{K}| < |\mathcal{M}|$
2. (5 bonus points) Prove a lower bound on the size of $\mathcal{K}$ in term of ϵ [Challenging]

Question 4 (20 points)

We say that a PRG $G : \{0,1\}^n \to \{0,1\}^{2n}$ is (t, ϵ)-secure if for all distinguishers $\mathcal{D}$ running in time at most t we have

$$\mathbf{Adv}_{\mathcal{D},G} = \left| Pr_{s \leftarrow \{0,1\}^n}\left[\mathcal{D}(G(s)) = 1\right] - Pr_{r \leftarrow \{0,1\}^{2n}}\left[\mathcal{D}(r) = 1\right] \right| \leq \epsilon \ .$$

Suppose that G is $\left(t, \epsilon_t = \frac{1.5t}{2^n}\right)$-secure PRG for all $t \leq 2^n$. Show that for all $t \leq 2^n$ the encryption scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ (defined below) is $\left(t' = t - O(n), \epsilon_t = \frac{1.5t}{2^n}\right)$-EAV Secure.

- $\mathtt{Gen}$: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it.
- $\mathtt{Enc}$: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^{2n}$ output the ciphertext:
$$c := \langle G(k) \oplus m \rangle \tag{1}$$
- $\mathtt{Dec}$: on input a $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^{2n}$, output the plaintext message
$$m := G(k) \oplus c \tag{2}$$

Question 5 (30 points)

For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}(.)$ to be a probabilistic oracle that, on input 1^n, choose uniform $r \in \{0,1\}^n$ and return $(r, g(r))$. A keyed function F is a *weak pseudorandom function* if for all PPT algorithm D, there exists a negligible function **negl** such that:

$$\left| \Pr[D^{F_k^{\$}(.)}(1^n) = 1] - \Pr[D^{f^{\$}(.)}(1^n) = 1] \right| \leq \mathsf{negl}(n) \tag{3}$$

where $k \in \{0,1\}^n$ and $f \in Func_n$ and chosen uniformly.

1. Let F' be a pseudorandom function, and define
$$\mathrm{F_k(x)} \stackrel{\mathrm{def}}{=} \begin{cases} \mathrm{F'_k(x)} & \text{if x is even} \\ \mathrm{F'_k(x+1)} & \text{if x is odd} \end{cases} \tag{4}$$

   Prove that F is weakly pseudorandom.

2. Is CTR-mode encryption using a weak pseudorandom function necessary CPA-secure? Does it necessarily have indistinguishable encryptions in the presence of an eavesdropper? Prove your answers.

3. Prove that the following construction is CPA-secure if F is a weak pseudorandom function.

   Construction: Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:

   - Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it.
   - Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext:

   $$c := \langle r, F_k(r) \oplus m \rangle \tag{5}$$

   - Dec: on input a $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message

   $$m := F_k(r) \oplus s \tag{6}$$