Homework 1

Due date: Thursday, September 14th 9:00 AM

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 $\mathcal{M} = \{0, ..., 8\}$ and key generation algorithm chooses a uniform key from the key space $\mathcal{K} = \{0, ..., 7\}$. Suppose $\mathrm{Enc_k(m) = k + m \bmod 9}$ and $\mathrm{Dec_k(c) = c - k \bmod 9}$.

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

- 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 $\mathrm{Enc_k}(m) = m \oplus G(k)$ where G is a secure pseudorandom generator with expansion factor $\ell(n) = 2n$.

Question 2 (20 points)

Let F be a length-preserving pseudorandom function. For the following construction of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-2} \rightarrow \{0,1\}^{4n}$, state whether F' is a pseudorandom function: if yes prove it, if not show an attack.

- $F'_k(x) \stackrel{\mathrm{def}}{=} F_k(00||x)||F_k(x||01)||F_k(10||x)||F_k(x||11)$

- $F'_k(x) \stackrel{\mathrm{def}}{=} F_k(0||x||0)||F_k(0||x||1)||F_k(1||x||0)||F_k(1||x||1)$

Question 3 (12 points)

Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryption in the presence of an eavesdropper and whether it is CPA-secure (In each case, the shared key is a uniform $k \in \{0,1\}^n$). Explain your answer.

- To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $(r, G(r) \oplus m)$.
- To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
- To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then chose uniform $r \in \{0,1\}^n$ and send $(r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1))$.

Question 4 (18 points)

- Define a notion of perfect secrecy under a chosen-plaintext attacks. (Hint: Adapt definition 3.22)
- Prove that no encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ can satisfy the definition. (Hint: You may assume that the message space is $\mathcal{M} = \{0,1\}^n$ and that the ciphertext space $\mathcal{C}$ and key-space $\mathcal{K}$ are both finite).

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:

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

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

1. Let F' be a pseudorandom function, and define

   $$\mathrm{F_k(x)} \stackrel{\mathrm{def}}{=} \begin{cases} \mathrm{F'_k(x)} & \text{if x is even} \\ \mathrm{F'_k(x+1)} & \text{if x is odd} \end{cases} \tag{2}$$

   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:

$$c := \langle r, F_k(r) \oplus m \rangle \tag{3}$$

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

$$m := F_k(r) \oplus s \tag{4}$$