Homework 1

Due date: Friday, Feb 3rd 11:30 AM

Question 1 (30 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 {0,....,9}. Suppose $\mathrm{Enc_k(m)} = \mathrm{k} + \mathrm{m} \bmod 9$ and $\mathrm{Dec_k(c)} = \mathrm{c} - \mathrm{k} \bmod 9$.
- 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 $\mathrm{Enc_k(m)} = \mathrm{m} \oplus (\mathrm{k} \,||\, 0)$ and $\mathrm{Dec_k(c)} = \mathrm{c} \oplus (\mathrm{k} \,||\, 0)$.

Question 2 (10 points)

Consider a crypto system in which M={a,b}, $K = \{K_1, K_2, K_3, K_4\}$, and $C = \{1, 2, 3, 4, 5\}$. Suppose that the keys are chosen with the following probability distribution:

$$P_k(K_1) = \frac{2}{3}, P_k(K_2) = P_k(K_3) = \frac{1}{6} \ ,$$

the plaintext probability distribution is given by:

$$P_M(a) = P_M(b) = \frac{1}{2}$$

and the encryption matrix is as follows:

	a	b
K_1	1	2
K_2	2	4
K_3	3	1
K_4	4	5

State whether the encryption system is perfectly secret or not? Justify your answer.

Question 3 (20 points)

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

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

Question 4 (25 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 5 (15 points)

Suppose that an adversary obtains a message ciphertext pair with $c = \text{Enc}_\text{k}(\text{m})$. The brute force attack (trying all keys $k \in \mathcal{K}$) takes, on average, time $\sim \frac{|\mathcal{K}|}{2}$ where the $|\mathcal{K}|$ is the size of keyspace. If we encrypt the message m twice (double encryption) using two different keys ($c = \text{Enc}_{\text{k}_2}(\text{Enc}_{\text{k}_1}(\text{m}))$), so the size of the new keyspace has size $|\mathcal{K}|^2$ and the time for the brute force attack is increased to $\sim \frac{|\mathcal{K}|^2}{2}$.

The meet-in-the-middle attack is one of the types of *known plaintext attacks*. The attacker first computes and stores $\left(k', \text{Enc}_{\text{k}'}(\text{m})\right)$ and $\left(k', \text{Dec}_{\text{k}'}(\text{c})\right)$ for each $k' \in \mathcal{K}$.

- Suppose that $\text{Enc}_\text{x}(\text{m}) \neq \text{Dec}_\text{y}(\text{c})$ for some keys $x, y \in \mathcal{K}$. Show that either $k_1 \neq x$ or $k_2 \neq y$.
- Suppose that the attacker has several aditional message ciphertext pairs (m_1, c_1), $(m_2, c_2), ...(m_{10}, c_{10})$ where $c_i = \text{Enc}_{\text{k}_2}(\text{Enc}_{\text{k}_1}(\text{m}))$. Explain how the attacker can recover k_1 and k_2 in time $O\left(|\mathcal{K}| \log |\mathcal{K}|\right)$. Hint: What famous algorithm runs in time $O(n \log n)$? Note: You may assume that if $c_i = Enc_{k''}(Enc_{k'}(m_i))$ for all $i \leq 10$ that $k' = k_1$ and $k'' = k_2$.
- Consider a triple encryption scheme (i.e., $c = \text{Enc}_{\text{k}_3}(\text{Enc}_{\text{k}_2}(\text{Enc}_{\text{k}_1}(\text{m})))$) scheme. Describe an attack with running time $O\left(|\mathcal{K}|^2 \log |\mathcal{K}|\right)$. What is the running time for quadruple-encryption? Quintuple-encryption?