Homework 1

September 12 2018

(25 pt) Perfect Secrecy and One Time Pad Encryption

1.(a) Prove or refute: If an encryption schem is perfecly secret, then the encryption of any message is *uniformly random* over the ciphertext space $\mathcal{C}$. Formally, prove or disprove the following statement: For any fixed $m \in \mathcal{M}$, and c $\in \mathcal{C}$:

$$Pr_{k \leftarrow \mathsf{KeyGen}}[\mathsf{Enc}_k(m) = c] = \frac{1}{|\mathcal{C}|}$$

If the statement is true give a formal proof otherwise give a counterexample to show it is false.

(*Hint.* While we know that in one-time pad $|\mathcal{M}| = |\mathcal{C}|$, this is not a necessary requirement for a perfectly secure schemes. For example, we can have a perfectly secure scheme where $|\mathcal{C}| > |\mathcal{M}|$.)

1.(b) Assume we have a set of strings $S = \{000, 001, 010, 011, 100, 101, 110\}$, that is the set of 3 bit strings, but with 111 missing. For each of the following one-time pad variants, state if it can be perfectly secure and why.

1) $\mathcal{M} = S$ and $\mathcal{K} = \{0,1\}^3$

2) $\mathcal{M} = \{0,1\}^3$ and $\mathcal{K} = S$

3) $\mathcal{M} = \mathcal{K} = S$

(30 pt) Pseudorandom Generators

2. Let $G : \{0,1\}^n \to \{0,1\}^{p(n)}$ be a pseudorandom generator with expansion factor $p(n) > 2n$. Namely, for any n, on input a seed of size n, G outputs a string of size $p(n)$. In each of the following cases say whether G' is necessarily a pseudorandom generator. If yes, give a proof (by reduction); if not show an efficient distinguisher and its probability of success.

(a) $G'(s) \overset{def}{=} s||G(s)$, where $\|$ stands for concatenation.

(b) $G'(s) \overset{def}{=} f(G(f(s)))$, where $f(x)$ is a function that takes as input a string of size l (with $l > 1$) and outputs a string of size $l-1$ with the least significant bit of x removed. (For inputs of length 1, you can ignore the fact that $G'(s)$ is not defined.)

(25 pt)Pseudorandom Functions

3.(a) Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a pseudorandom function mapping n-bit input to n-bit output with a n-bit key. Consider a function $F' : \{0,1\}^{2n} \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ such that

$$F'(k,x) = F(k_1, x_1) \| F(k_2, x_2)$$

where $k \in \{0,1\}^{2n}$ is the key and $x \in \{0,1\}^{2n}$ is the input and $k = k_1 \| k_2, x = x_1 \| x_2, k_1, k_2, x_1, x_2 \in \{0,1\}^n$. Prove or disprove that F' is a pseudorandom function. If it is a pseudorandom function, give a formal proof by reduction; If it is not a pseudorandom function, give an efficient attack. (Notation $\|$ means concatenation, e.g., $000110 = 000\|110$.

3.(b) Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a pseudorandom function from n-bit input to n-bit output with a n-bit key. Consider a function $F' : \{0,1\}^{2n} \times \{0,1\}^n \rightarrow \{0,1\}^n$ such that

$$F'(k,x) = F(k_1, x) \oplus k_2$$

where $k \in \{0,1\}^{2n}$ is the key and $x \in \{0,1\}^n$ is the input, $k = k_1 \| k_2, k_1, k_2 \in \{0,1\}^n$. Prove or disprove that F' is a pseudorandom function. If it is a pseudorandom function, give a formal proof by reduction. If it is not a pseudorandom function, give an efficient attack.

(20 pt) CPA security

4 Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one is CPA-secure. The problem is that you do not know which one is CPA-secure and which one may not be. Show how to construct an encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ that is guaranteed to be CPA secure as long as at least one of Π_1 or Π_2 is CPA-secure. Try to provide a formal proof of your answer. (*Hint.*: Generate two plaintext messages from the original plaintext so that knowledge of either one of the parts reveals nothing about the plaintext, but knowledge of both does yield the original plaintext.)