Homework 2

Due date: Thursday, September 29thth 9:00 AM

Question 1 (20 points)

State whether the following claim is true or false. Justify your answer:
If G is a pseudorandom generator defined over $(\{0,1\}^{\ell}, \{0,1\}^{L})$ where $L > \ell$, then

$$G'(r_1||r_2||...||r_n) = G(r_1)||G(r_2)||...||G(r_n)$$

is pseudorandom generator defined over $(\{0,1\}^{n\cdot\ell}, \{0,1\}^{n\cdot L})$

Question 2 (20 points)

Let F be a pseudorandom permutation, and define a fixed-length encryption scheme (Enc, Dec) as follows: On input $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^{n}$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ of length $n/2$ and computes $c := F_k(r||m)$.

Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

Question 3 (20 points)

Show that the CBC, OFB, and CTR modes of encryption do not yield CCA-secure encryptions scheme.

Question 4 (20 points)

In this question, we explore what happens when the basic CBC-MAC construction is used with messages of different lengths.

- Say the sender and receiver do not agree on the message length in advance (and so $\text{Vrfy}_k(\text{m}, \text{t}) = 1$ iff $\text{t} \stackrel{?}{=} \text{Mac}_k(m)$, regardless of the length of m), but the sender is careful to only authenticate messages of length 2n. Show that an adversary can forge a valid tag on a message of length 4n.
- Say the receiver only accepts 3-block messages (so $\text{Vrfy}_k(\text{m}, \text{t}) = 1$) only if m has length 3n and $\text{t} = \text{Mac}_k(m)$, but the sender authenticates messages of any length a multiple of n. Show that an adversary can forge a valid tag on a new message.

Question 5 (20 points)

Let $H : \{0,1\}^* \to \{0,1\}^n$ be the random oracle. A "cover"-tripple is a tripple (m_1, m_2, m_3) such that

$$\bigwedge_{i=1}^{n} (\ (H(m_1)_i = H(m_2)_i) \vee (H(m_1)_i = H(m_3)_i)) = 1$$

Where $H(\cdot)_i$ denotes the i bit of the output.

1. What is the probability that (m_1, m_2, m_3) is a "cover"-triple for random m_1, m_2, m_3?

2. Lower bound the number of queries to the random oracle one needs to make in order to find a "cover"-tripple with a probability greater than $1/2$? Your lower bound should be as tight as possible.