Homework 2

Due date: Thursday , February 18$^{\text{nd}}$

Question 1 (20 points)

Define $(t(n), q(n), \epsilon(n))$-CPA security of Π as the statement that any attacker running in time $t(n)$ and making at most $q(n)$ queries to the Left-Right encryption oracle wins the CPA security game with probability at most $\epsilon(n)$. Similarly, for the function $F_K : \{0,1\}^{n'} \times \{0,1\}^n \to \{0,1\}^n$ (mapping n' bits of input to n bits using the key K of size n) we can define $(t_{PRF}(n), q_{PRF}(n), \epsilon_{PRF}(n))$-PRF security, implying that for any distinguisher running in time $t_{PRF}(n)$ and making at most $q_{PRF}(n)$ queries to the PRF oracle distinguishes the $F_K(\cdot)$ from a truly random function with advantage at most $\epsilon_{PRF}(n)$.

- **Part 1**: Assume that F_K is a $(t_{PRF}(n), q_{PRF}(n), \epsilon_{PRF}(n))$-secure PRF mapping n' bit strings to n bit strings. What is the concrete security bound of the encryption scheme $\texttt{Enc}_K(m) = (r, F_K(r) \oplus m)$? Justify your answer.
- **Part 2**: In practice one often assumes that $q_{ENC}(n) \ll t_{ENC}(n)$ e.g., oftentimes one requires that secret keys are rotated after $2^{n/4}$ encryptions. In this case we can sometimes save bandwidth by reducing the length of the nonce r. Suppose that $q_{ENC}(n) = 2^{n/4}$ and for any $t \leq 2^n$ that F_K is a $(t, t, t/2^n)$-secure PRF mapping n' bit nonces to n bit outputs. If we want to ensure that our encryption scheme is $(t, 2^{n/4}, 2^{-n/4} + t2^{-n+1})$-CPA secure. How big does n' need to be? (Justify your answer)

Answer: ...

Resource and Collaborator Statement: ...

Question 2 (20 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 $(r, g(r))$ (On any other input $x \neq 1^n$ the oracle $g^{\$}(x)$ will simply return $\perp$). A keyed function F is a *weak pseudorandom function* if for all PPT algorithm D, there exists a negligible function **negl** such that:

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

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.

Answer: ...

Resource and Collaborator Statement: ...

Question 3 (20 points)

1. Show that the CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption schemes (regardless of F). Briefly describe how an attacker could win the CCA-Security game with non-negligible advantage. (Hint: Suppose that we encrypt a message $m = (m_1, m_2, m_3)$ and get back a ciphertext $c = (c_0, c_1, c_2, c_3)$. What happens if we flip a bit in c_2?)

2. Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $\mathsf{ctr} \in \{0,1\}^n$ is chosen, and the i^{th} ciphertext block c_i is computed as $c_i := F_k(\mathsf{ctr} + i + m_i)$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

Answer: ...

Resource and Collaborator Statement: ...

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 $\mathsf{Vrfy}_k(m,t) = 1$ iff $t \stackrel{?}{=} \mathsf{Mac}_k(m)$, 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 $\mathsf{Vrfy}_k(m,t) = 1$) only if m has length 3n and $t = \mathsf{Mac}_k(m)$, 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.

Answer: ...

Resource and Collaborator Statement: ...

Question 5 (20 points)

Let (Gen_1, H_1) and (Gen_2, H_2) be two hash functions. We define (Gen, H) as follow:

- Gen : runs Gen_1 and Gen_2 to obtain s_1, s_2
- $H^{s_1,s_2}(x) = H_1^{s_1}(x)||H_2^{s_2}(x)$

Prove that if at least one of (Gen_1, H_1) and (Gen_2, H_2) is collision resistant, then (Gen, H) is collision resistant.

Answer: ...

Resource and Collaborator Statement: ...