601.745: Advanced Topics in Applied Cryptography	January 31, 2018
Assignment 1	
Instructor: Matthew Green	*Due: 11:59pm, February 12*

Name: ____

The assignment should be completed individually. You are permitted to use the Internet and any printed references.

Please submit the completed assignment via Blackboard.

Problem 1: PRFs as MACs.

Let $f : \{0,1\}^\kappa \times \{0,1\}^* \rightarrow \{0,1\}^\ell$ be a pseudorandom function (PRF) family, such that $f_k(m)$ represents the evaluation with key k at point m, and the result is an ℓ bit string.[1] Sketch an informal proof that if f is pseudorandom (and ℓ is long enough, say 128 bits), then $f_k(m)$ is a secure MAC on key k and message m in the SUF-CMA definition.[2]

To help you with this, we will sketch out parts of the theorem and proof below.

Theorem 1 Let $f : \{0,1\}^\kappa \times \{0,1\}^* \rightarrow \{0,1\}^\ell$ be a PRF family. Then the construction $f_k(m)$ is an SUF-CMA MAC.

Proof sketch 1 Our proof proceeds as follows. Let us assume by contradiction that $f_k(m)$ is not a secure MAC scheme, *i.e.,* that there exists some p.p.t. adversary $\mathcal{A}$ that wins the SUF-CMA MAC game with non-negligible advantage.[3] Then we show that there exists a p.p.t. algorithm $\mathcal{B}$ that wins the PRF game, *i.e.,* that distinguishes the function f from a random function with non-negligible advantage.

$\mathcal{B}$ operates as follows. It plays the PRF game with a challenger. It also runs $\mathcal{A}$ internally, and interacts with it as in the SUF-CMA game. When $\mathcal{A}$ queries the MAC oracle on a message m_i, $\mathcal{B}$ answers the query as follows:

Fill in this part.

When $\mathcal{A}$ outputs the "forgery" pair (m^*, T^*) (such that, by the definition of $\mathcal{A}$, with non-negligible probability $T^* = f_k(m^*)$), $\mathcal{B}$ does the following, and outputs a bit b as its guess in the PRF game.

Fill in this part.

[1] For a formal definition, see *e.g.,* `https://cseweb.ucsd.edu/~mihir/cse207/w-prf.pdf` and specifically the security game in Definition 3.4.1.

[2] See *e.g.,* `https://www.cs.jhu.edu/~astubble/dss/ae.pdf`.

[3] As a reminder, in the SUF-CMA game the adversary is allowed to query an oracle on any number of messages m_i, and receives MACs of the form $T = f_k(m_i)$ for each query. At the end of the game it wins if it outputs a pair (m^*, T^*) such that no previous oracle query (resp. response) was (m^*, T^*) and $T^* = f_k(m^*)$. The advantage of $\mathcal{A}$ is the probability that it succeeds in this game.

We argue that if the PRF oracle implements a random function, then:

Here explain why $\mathcal{B}$ is able to distinguish whether the oracle implements a PRF or a random function with non-negligible advantage.

This completes the proof.

Problem 2: **Encrypt-and-MAC.**

Let k_1, k_2 be two secret keys. Let $\mathsf{Encrypt}(k_1, M)$ represent encryption of M using a $\mathsf{IND\text{-}CPA}$ encryption scheme under key k_1. Let $\mathsf{MAC}(k_2, M')$ represent the computation of a (deterministic) MAC on message M' using key k_2. Let us define the following authenticated encryption scheme:

$$C = \mathsf{Encrypt}(k_1, M) \| \mathsf{MAC}(k_2, M)$$

In class we discussed how this scheme is not secure, because there is a simple attack that breaks the $\mathsf{IND\text{-}CPA}$ (and hence the $\mathsf{IND\text{-}CCA}$) security of the scheme. Despite this, I want you to *attempt* to sketch the reduction proof showing that the above scheme is $\mathsf{IND\text{-}CCA}$, similar to the one that we discussed in class. Tell me where in the proof your attempt breaks down. This can be a quick explanation, not a full proof.

Problem 3: **Encrypt-and-Counter-MAC.**

Many versions of the `ssh` protocol use a variant of the following scheme. Let k_1, k_2 be two secret keys. Let $\mathsf{Encrypt}(k_1, M)$ represent encryption of M using a $\mathsf{IND\text{-}CPA}$ encryption scheme under key k_1. Let $f_{k_2}(M')$ represent the computation of a pseudorandom function on message M' using key k_2 (this acts as a MAC; see Problem 1).

Finally, let i be a counter value that begins with $i = 0$ on the first message encrypted, and increments for every subsequent message (*i.e.,* you can trust that i will never repeat). The overall authenticated encryption algorithm for message M using counter i is:

$$C = \mathsf{Encrypt}(k_1, M) \| f_{k_2}(M \| i)$$

Is this scheme a secure $\mathsf{IND\text{-}CCA}$ authenticated encryption scheme? If so, sketch a proof that this is true. If not, demonstrate an attack on the scheme that wins the game with non-negligible probability.

To help you with this, we will sketch out parts of the theorem and proof below.

Theorem 2 Let $f : \{0,1\}^\kappa \times \{0,1\}^* \rightarrow \{0,1\}^\ell$ be a PRF family, and let $(\mathsf{Encrypt}, \mathsf{Decrypt})$ be an $\mathsf{IND\text{-}CPA}$-secure encryption scheme. Then the construction above is an $\mathsf{IND\text{-}CCA}$ encryption scheme.

Proof sketch 2 Our proof proceeds as follows. Let us assume by contradiction that the scheme above is *not* $\mathsf{IND\text{-}CCA}$ secure *i.e.,* that there exists some p.p.t. adversary $\mathcal{A}$ that wins the $\mathsf{IND\text{-}CCA}$ game with non-negligible advantage. Then we show that there exists a p.p.t. algorithm $\mathcal{B}$ that wins either the $\mathsf{IND\text{-}CPA}$ game against the encryption scheme, or the PRF game, *i.e.,* that distinguishes the function f from a random function with non-negligible advantage.

$\mathcal{B}$ operates as follows. It plays the IND-CPA game with a challenger. It also runs $\mathcal{A}$ internally, and interacts with it as in the IND-CCA game. First, each time $\mathcal{A}$ requests the encryption of a message m_i, $\mathcal{B}$ requests the encryption of m_i from the IND-CPA challenger, to obtain c_i. $\mathcal{B}$ then generates a random string $T_i \leftarrow \{0,1\}^\ell$ and records (m_i, c_i, T_i) in a table. It returns $C_i = c_i \| T_i$. When $\mathcal{A}$ queries for the decryption of some C_i', $\mathcal{B}$ parses this as $C_i' = c_i' \| T_i'$ and checks its table for an entry of the form (m_i', c_i', T_i'). If one is present, it returns m_i'. Otherwise it returns $\perp$ to $\mathcal{A}$.

Explain the rest of the operation of $\mathcal{B}$ here.

Now argue that as long as $\mathcal{A}$ cannot distinguish the random strings T_i from correctly-generated tags $f_k(m_i)$ except with negligible probability, then $\mathcal{B}$ succeeds against the IND-CPA game with non-negligible probability.

Finally, present a second proof that $\mathcal{A}$ cannot distinguish these strings.