601.445/601.645: Practical Cryptographic Systems	February 3, 2020

Weekly Homework 2

Instructor: Matthew Green *Due: 11:59pm, February 10*

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: For the following questions, let $\mathcal{K}$ be the set of possible keys for a cryptosystem, let $\mathcal{C}$ be the set of possible ciphertexts, and let $\mathcal{P}$ be the set of plaintexts. The notation $|\mathcal{C}|$ refers to the cardinality of the set $\mathcal{C}$. Answer the following questions:

1. If the cryptosystem is a block cipher, explain why $|\mathcal{C}| = |\mathcal{P}|$.
2. How many distinct keys would be needed to capture every *unique* permutation between input and output?
3. Assume the cryptosystem is the CBC mode operation using a block cipher. Explain what happens when the same Initialization Vector (IV) is re-used? Now do the same for CTR mode.
4. Imagine that E is the encipherment mode of a block cipher, with $|\mathcal{P}| = 2^{\ell}$. Give an argument for why $T = E(k, M)$ might be a good Message Authentication Code for message M using key k.

Problem 2: Let $H : \{0,1\}^{\ell} \to \{0,1\}^k$ be a hash function with an input size of ℓ bits, and an output size of k bits. Answer the following questions:

1. Let $\ell > k$. Do there exist collisions in H? Give a simple argument for why or why not.
2. Imagine that H is *collision-resistant*, in the sense that, on receiving H, no efficient attacker can find a pair (M_1, M_2) such that $H(M_1) = H(M_2)$. Show that this does not necessarily mean H is pre-image resistant. Hint: build an example hash function that is collision resistant, but not pre-image resistant (note: you can use another collision-resistant hash function H' as the ingredient for building your function.)
3. The Merkle-Damgard construction allows us to convert a fixed-input-size "compression function" $f : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ into a variable-length-input hash function of the form $H : \{0,1\}^* \to \{0,1\}^k$. Sketch the construction.

4. Explain how length-extension attacks work in Merkle-Damgard.
5. Assume a block cipher with block size ℓ bits. Approximately how many messages can we expect to encrypt using CBC-mode encryption before a (random) initialization vector repeats, with probability 0.5?