CS 5158/6058 Data Security and Privacy, Spring 2018 Homework 2

Instructor: Dr. Boyang Wang

Due Date: 02/13/2018 (Tuesday), 11:59pm.
Format: Please submit a pdf of your homework in Blackboard.
Total Points: 6 points

Problem 1 (CS5158 only, 1 point). Assume we use Shift Cipher, and the message space is $\mathcal{M} = \{\mathtt{aa}, \mathtt{ab}, \mathtt{bc}\}$, where $\Pr[M = \mathtt{aa}] = 0.3$, $\Pr[M = \mathtt{ab}] = 0.2$, $\Pr[M = \mathtt{bc}] = 0.5$. In addition, we assume the key space is $\mathcal{K} = \{0, 1, 2, ..., 25\}$ and it is uniformly distributed, i.e., $\Pr[K = k] = 1/26$, for any $k \in [0, 25]$. What is the probability of a ciphertext is `XY`?

Problem 1 (CS6058 only, 1 point). Assume we have Vigenere Cipher $\Pi = \{\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}\}$. Message space is $\mathcal{M} = \{\mathtt{aaaa}, \mathtt{faaa}\}$, and the key length could be 1, 2, 3, or 4, and it is uniformly distributed. In addition, assume an adversary $\mathcal{A}$ plays a security game $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ as below:

1. $\mathcal{A}$ chooses $m_0 = \mathtt{aaaa}$ and $m_1 = \mathtt{faaa}$, and gives m_0 and m_1 to challenger;
2. Challenger flips a fair coin, gets a bit b, computes $c_b \leftarrow \mathsf{Enc}_k(m_b)$, where $k \leftarrow \mathsf{KeyGen}(\cdot)$, and returns ciphertext c_b to $\mathcal{A}$.
3. Given $c_b = c_{b1}c_{b2}c_{b3}c_{b4}$, $\mathcal{A}$ guesses $b' = 0$ if $c_{b1} = c_{b2}$, otherwise it guesses $b' = 1$
4. Outputs 1 if $b' = b$, and 0 otherwise; and we say $\mathcal{A}$ wins the game if $b' = b$.

Prove that this adversary can win this game with a probability greater than 1/2.

Problem 2 (1 point). Describe the formal definition of perfect secrecy. Assume each key has θ bits in a one-time pad, prove this one-time pad is perfectly secure.

Problem 3 (1 point). Although one-time pad is perfectly secure, it has two major assumptions/limitations, which makes it impractical for real applications. Describe the two major limitations of one-time pad.

Problem 4 (1 point). Compared to an adversary in perfect security, what are the two main differences for an adversary in computational security?

Problem 5 (1 point). Explain what is a negligible function, and describe the properties of negligible functions.

Problem 6 (1 point). Describe the details of the security game/experiment for computational security, and formally explain what is (computationally) indistinguishable.