Secure Computational Models: Weekly Paper 1

Siddarth Ijju

September 17th, 2018

1 Introduction

This week's lecture revolved around the introduction of security and how to show it for a simple model such as the One-Time Pad cipher. We explored the structure of the cipher itself, as well as proving the security of the model to an eavesdropper.

2 One-Time Pad

The One-Time Pad cipher has 3 main functions - Keygen, Encrypt, and Decrypt. Keygen generates a key, $\mathbf{k}$ of the form $\{0,1\}^\lambda$, that is sent to both the Encrypt and Decrypt functions. Both the Encrypt and Decrypt functions use the binary operation XOR, otherwise known as exclusive OR and represented by the symbol $\oplus$. The Encrypt function recieves an input of a message $\mathbf{m}$ and $\mathbf{k}$. It returns $\mathbf{k} \oplus \mathbf{m}$ and sends this result to the Decrypt function as the ciphertext $\mathbf{c}$. The Decrypt function returns $\mathbf{k} \oplus \mathbf{c}$, which outputs $\mathbf{m}$.

2.1 Proof of Decrypt

The way the Decrypt function works is not very obvious to the eye. In this section we demonstrated the validity of the Decrypt function is deciphering the ciphertext $\mathbf{c}$ back into $\mathbf{m}$. First, we defined the Decrypt function as Decrypt($\mathbf{k}$, $\mathbf{c}$), where $\mathbf{c}$ is the ciphertext returned by the Encrypt function. Thus, we can replace $\mathbf{c}$ with the Encrypt function Encrypt($\mathbf{k}$, $\mathbf{m}$) where $\mathbf{m}$ is the message passed to the cipher. Therefore, Decrypt($\mathbf{k}$, $\mathbf{c}$) = Decrypt($\mathbf{k}$, Encrypt($\mathbf{k}$, $\mathbf{m}$)).

From this we evaluated the output of the Decrypt function. Since Encrypt($\mathbf{k}$, $\mathbf{m}$) = $\mathbf{k} \oplus \mathbf{m}$ and Decrypt($\mathbf{k}$, $\mathbf{c}$) = $\mathbf{k} \oplus \mathbf{c}$, we have that Decrypt($\mathbf{k}$, Encrypt($\mathbf{k}$, $\mathbf{m}$)) = Decrypt($\mathbf{k}$, $\mathbf{k} \oplus \mathbf{m}$) = $\mathbf{k} \oplus \mathbf{k} \oplus \mathbf{m}$. Since one of the properties of $\oplus$ is that a binary number $\oplus$ itself is of the form 0^λ, we have $\mathbf{k} \oplus \mathbf{k} \oplus \mathbf{m} = 0^\lambda \oplus \mathbf{m}$ = $\mathbf{m}$. Thus, Decrypt($\mathbf{k}$, $\mathbf{c}$) = $\mathbf{m}$.

2.2 Security of Cipher

Now that the basis for One-Time Pad is established, we must also show that the cipher is secure for an eavesdropper who recovers $\mathbf{c}$. That is, does $\mathbf{c}$ reveal $\mathbf{m}$ to

an eavesdropper without any other external information? For this, we defined a function View($\mathbf{m}$) that demostrated this process. We then showed that for any $\mathbf{k}$ with $\lambda = 3$, an eavesdropper has a $\frac{1}{2^\lambda}$ probability of guessing $\mathbf{m}$ from $\mathbf{c}$. There are a few loopholes to this approach though, because if $\mathbf{c}$ is all 1s or all 0s then $\mathbf{m}$ is either $\mathbf{k}$ or $\tilde{}\mathbf{k}$. We then extended this idea to the statement that for all $\mathbf{m}$, $\mathbf{m'}$ $\epsilon\{0,1\}^\lambda$, the probability distribution of View($\mathbf{m}$) and View($\mathbf{m'}$) are identical