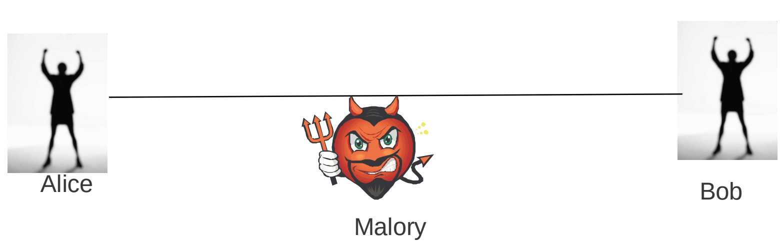
Unconditional Secrecy

Murat Kantarcioglu

Secure Communication

- Our goal is to provide secure channel between Alice and Bob so that they can securely communicate with each other remotely even if malicious Malory is eavesdropping on their communication.
- We will assume that Alice and Bob shares a common secret in this setting



Definitions of Security

- Computational Security
  - Assuming that Malory has limited computational resources, it will be infeasible for Malory to infer anything useful from the communication between Alice and Bob
  - In practice, we will prove that if a certain problem is hard (e.g. factoring large integers) than breaking a certain cryptographic primitive will be computationally infeasible (also known as provable security)

Definitions of Security

- Unconditional Security (i.e. Perfect Security)
  - Even if Malory has infinite amount of computational resources, he cannot learn anything from the communication
- Pros: Better Protection compared Computational Security
- Cons: Secret keys have to be as large as the message size

Review of Elementary Probability

- A discrete random variable $\mathbf{X}$ is defined by specifying
  - A finite set X
    (e.g. the possible values a tossed dice can take.)
  - A probability distribution on X such that the probability of $\mathbf{X}$ takes on the value x is denoted as $Pr[\mathbf{X} = x]$ (e.g. the probability that we get tails after a coin flip)
- If $\mathbf{X}$ is fixed define $Pr[\mathbf{X} = x]$ as $Pr[x]$
- $Pr[x] >= 0$ for all $x \in X$
- $\left(\sum_{x \in X} Pr[x]\right) = 1$

Review of Elementary Probability Theory

- Given an event $E \subset X$, define
  $Pr[x \in E] = \sum_{x \in E} Pr[x]$
- *Example:*
  - Random variable $\mathbf{Z}$: result of throwing a pair of dice
  - Defined on set $Z = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}$
  - Define event S_4 as the sum of the dices is 4.
  - $S_4 = \{(1, 3), (2, 2), (3, 1)\}$
  - $Pr[S_4] = 1/12$

Review of Elementary Probability Theory

- Given two random variables $\mathbf{X}$ and $\mathbf{Y}$
  - $Pr[x, y]$ is the joint probability
  - $Pr[x|y]$ is the conditional probability
- Random variables $\mathbf{X}$ and $\mathbf{Y}$ are independent if
  - $Pr[x, y] = Pr[x].Pr[y]$
- $Pr[x, y] = Pr[x|y].Pr[y]$
- Bayes Theorem
  - If $Pr[y] > 0$ then $Pr[x|y] = \frac{Pr[y|x].Pr[x]}{Pr[y]}$

Formal Definitions of Perfect Secrecy

- A CryptoSystem Definition:
  - A cryptosystem is a five tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where
    1. $\mathcal{P}$ is a finite set of plaintexts
    2. $\mathcal{C}$ is a finite set of ciphertexts
    3. $\mathcal{K}$ is a finite set of possible keys
    4. $\mathcal{E}$ is the set of encryption rules for each key
    5. $\mathcal{D}$ is the set of correct decryption rules for each key

Perfect Secrecy

- **Perfect Secrecy:** A cryptosystem has perfect secrecy if $Pr[x|y] = Pr[x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$
- This definition states that **a posteriori** probability that the plaintext is x given that ciphertext is y is equal to the **a priori probability** that the plaintext is x
- Perfectly Secure CryptoSystem Example (Onetime Pad):
  - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$ where $n \geq 1$, $x \in \mathcal{P}$, $y \in \mathcal{C}$
  - Define encryption with one-time random key K, $e_K(x) = x \oplus K$ (i.e., bitwise)
  - Define decryption with one-time random key K, $d_K(y) = y \oplus K$ (i.e., bitwise xor)

Perfect Secrecy Proof for One-Time Pad

- We need to prove that perfect secrecy definition is satisfied
- We need to show $Pr[x|y] = Pr[x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$
- Note that

$$
\begin{aligned}
Pr[x|y] &= \frac{Pr[x].Pr[y|x]}{Pr[y]} \\
&= \frac{Pr[x].Pr[\mathbf{K} = y \oplus x]}{Pr[y]} \\
&= \frac{Pr[x].2^{-n}}{\sum_{k \in \mathcal{K}} Pr[\mathbf{K} = k].Pr[\mathbf{x} = d_k(y)]} \\
&= \frac{Pr[x].2^{-n}}{2^{-n}.\sum_{k \in \mathcal{K}} Pr[\mathbf{x} = d_k(y)]} \\
&= Pr[x]
\end{aligned}
$$

Properties of Crytosystems that have Perfect Secrecy

- A cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ that has perfect secrecy satisfies $Pr[x|y] = Pr[x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
- This implies (assuming $Pr[y] > 0$) (why can we assume this??)

$$
\begin{aligned}
&\implies \forall x \in \mathcal{P}, Pr[y] = Pr[y|x] > 0 \\
&\implies \forall x \in \mathcal{P}, \exists k \in \mathcal{K} \text{s.t.} e_k(x) = y \\
&\implies |\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{P}|
\end{aligned}
$$

- We can also show other properties about perfectly secure cryptosystems. See Thm 2.4 in the book.