Cryptography

Lecture 4

Announcements

- HW1 due on Monday, 2/10 at the start of class.
- Readings/quizzes on Canvas due Thursday 2/13 @11:59pm.
- Instructor Office Hours: 4-5pm on Thursday, 2/6, no office hours on Friday this week.

Agenda

- Last time:
  - Perfect Secrecy (K/L 2.1)
  - One time pad (OTP) (K/L 2.2)
- This time:
  - Class Exercise
  - Limitations of perfect secrecy (K/L 2.3)
  - Shannon's Theorem (K/L 2.4)
  - The Computational Approach (K/L 3.1)

Drawbacks of OTP

- Key length is the same as the message length.
  - For every bit communicated over a public channel, a bit must be shared privately.
  - We will see this is not just a problem with the OTP scheme, but an inherent problem in perfectly secret encryption schemes.
- Key can only be used once.
  - You will see in the homework that this is also an inherent problem.

Limitations of Perfect Secrecy

Theorem: Let (Gen, Enc, Dec) be a perfectly-secret encryption scheme over a message space $\boldsymbol{M}$, and let $\boldsymbol{K}$ be the key space as determined by Gen. Then $|\boldsymbol{K}| \geq |\boldsymbol{M}|$.

Proof

Proof (by contradiction): We show that if $|\boldsymbol{K}| < |\boldsymbol{M}|$ then the scheme cannot be perfectly secret.

- Assume $|\boldsymbol{K}| < |\boldsymbol{M}|$. Consider the uniform distribution over $\boldsymbol{M}$ and let $c \in \boldsymbol{C}$.
- Let $\boldsymbol{M}(c)$ be the set of all possible messages which are possible decryptions of c.

$$\boldsymbol{M}(c) \coloneqq \{m' |\ m' = Dec_k(c) for\ some\ k \in \boldsymbol{K}\}$$

Proof

$$\boldsymbol{M}(c) \coloneqq \{\, m' \,|\, m' = Dec_k(c) for\ some\ k \in \boldsymbol{K}\}$$

- $|\boldsymbol{M}(c)| \leq |\boldsymbol{K}|$. Why?
- Since we assumed $|\boldsymbol{K}| < |\boldsymbol{M}|$, this means that there is some $m' \in \boldsymbol{M}$ such that $m' \notin \boldsymbol{M}(c)$.
- But then

$$\Pr[M = m' |\, C = c] = 0 \neq \Pr[M = m']$$

And so the scheme is not perfectly secret.

Shannon's Theorem

Let (Gen, Enc, Dec) be an encryption scheme with message space $\boldsymbol{M}$, for which $|\boldsymbol{M}| = |\boldsymbol{K}| = |\boldsymbol{C}|$. The scheme is perfectly secret if and only if:

1. Every key $k \in \boldsymbol{K}$ is chosen with equal probability $1/|\boldsymbol{K}|$ by algorithm Gen.
2. For every $m \in \boldsymbol{M}$ and every $c \in \boldsymbol{C}$, there exists a unique key $k \in \boldsymbol{K}$ such that $Enc_k(m)$ outputs c.

**Theorem only applies when $|\boldsymbol{M}| = |\boldsymbol{K}| = |\boldsymbol{C}|$.

Some Examples

- Is the following scheme perfectly secret?
- Message space $\boldsymbol{M} = \{0,1,\dots,n-1\}$. Key space $\boldsymbol{K} = \{0,1,\dots,n-1\}$.
- $\mathrm{Gen}()$ chooses a key k at random from $\boldsymbol{K}$.
- $\mathrm{Enc}_k(m)$ returns $m + k$.
- $Dec_k(c)$ returns $c - k$.

Some Examples

- Is the following scheme perfectly secret?
- Message space $\boldsymbol{M} = \{0,1, \ldots, n-1\}$. Key space $\boldsymbol{K} = \{0,1, \ldots, n-1\}$.
- $\mathrm{Gen}()$ chooses a key k at random from $\boldsymbol{K}$.
- $\mathrm{Enc}_k(m)$ returns $m + k \bmod n$.
- $Dec_k(c)$ returns $c - k \bmod n$.

The Computational Approach

Two main relaxations:

1. Security is only guaranteed against efficient adversaries that run for some feasible amount of time.
2. Adversaries can potentially succeed with some very small probability.