

Cryptography

Lecture 4

Announcements

- HW1 due Wednesday, 2/8 at beginning of class
- Discrete Math Readings/Quizzes due Friday, 2/10 @ 11:59pm

Agenda

- Last time:
 - Perfect Secrecy (K/L 2.1)
 - One time pad (OTP) (K/L 2.2)
- This time:
 - 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 \mathbf{M} , and let \mathbf{K} be the key space as determined by Gen . Then $|\mathbf{K}| \geq |\mathbf{M}|$.

Proof

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

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

$$M(c) := \{m' \mid m' = Dec_k(c) \text{ for some } k \in K\}$$

Proof

$\mathbf{M}(c) := \{ m' \mid m' = Dec_k(c) \text{ for some } k \in \mathbf{K} \}$

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

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

And so the scheme is not perfectly secret.

Shannon's Theorem

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

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

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

Some Examples

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

Some Examples

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