Introduction to Cryptology

Lecture 5

Announcements

- HW1 due today
- HW2 up on course webpage, due Thursday 2/15
- Readings/quizzes on Canvas due Tuesday 2/13

Agenda

- Last time:
  - Definition of info-theoretic security (K/L 2.1)
  - Equivalent def’s and proofs of equivalence (K/L 2.1)
- This time:
  - Go over class exercise from 2/6
  - One time pad (OTP) (K/L 2.2)
  - Limitations of perfect secrecy (K/L 2.3)

The One-Time Pad (Vernam's Cipher)

- In 1917, Vernam patented a cipher now called the one-time pad that obtains perfect secrecy.
- There was no proof of this fact at the time.
- 25 years later, Shannon introduced the notion of perfect secrecy and demonstrated that the one-time pad achieves this level of security.

The One-Time Pad Scheme

1. Fix an integer $\ell > 0$. Then the message space M, key space K, and ciphertext space C are all equal to $\{0,1\}^\ell$.
2. The key-generation algorithm Gen works by choosing a string from $K = \{0,1\}^\ell$ according to the uniform distribution.
3. Encryption Enc works as follows: given a key $k \in \{0,1\}^\ell$, and a message $m \in \{0,1\}^\ell$,output $c := k \oplus m$.
4. Decryption Dec works as follows: given a key $k \in \{0,1\}^\ell$, and a ciphertext $c \in \{0,1\}^\ell$, output $m := k \oplus c$.

Security of OTP

Theorem: The one-time pad encryption scheme is perfectly secure.

Proof

Proof: Fix some distribution over M and fix an arbitrary $m \in M$ and $c \in C$. For one-time pad:

$$\Pr[C = c | \, M = m] = \Pr[M \oplus K = c \mid M = m]$$

$$= \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = \frac{1}{2^{\ell}}$$

Since this holds for all distributions and all m, we have that for every probability distribution over M, every $m_0, m_1 \in M$ and every $c \in C$

$$\Pr[C = c \mid M = m_0] = \frac{1}{2^{\ell}} = \Pr[C = c | M = m_1]$$

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.

$$\boldsymbol{M}(c) \coloneqq \{\widehat{\hat{m}} \mid \hat{m} = Dec_k(c) for\ some\ \hat{k} \in \boldsymbol{K}\}$$

Proof

$$\boldsymbol{M}(c) \coloneqq \{\, \widehat{m} \mid \widehat{m} = Dec_k(c) for\ some\ \hat{k} \in \boldsymbol{K}\}$$

- $|\boldsymbol{M}(c)| \leq |\boldsymbol{K}|$. 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

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

And so the scheme is not perfectly secret.