Introduction to Cryptology

Lecture 3
Announcements

• HW1 due today
• HW2 up on course webpage, due Tuesday 2/14
• Readings/quizzes on Canvas due Tuesday 2/14
• Looking ahead: next class we will do a longer class exercise on intractability
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:
  – One time pad (OTP) (K/L 2.2)
  – Limitations of perfect secrecy (K/L 2.2)
  – Shannon’s Theorem (K/L 2.4)
  – Intro to computational security
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:

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

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

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 $c \in C$

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

• Is the following scheme perfectly secret?
• Message space $M = \{0,1, \ldots, n - 1\}$. Key space $K = \{0,1, \ldots, n - 1\}$.
• $\text{Gen}()$ 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 $M = \{0,1, ..., n - 1\}$. Key space $K = \{0,1, ..., n - 1\}$.
• Gen() chooses a key $k$ at random from $K$.
• $Enc_k(m)$ returns $m + k \ mod \ n$.
• $Dec_k(c)$ returns $c - k \ mod \ n$. 
Limitations of Perfect Secrecy

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

$M(c) := \{\hat{m} \mid \hat{m} = Dec_{\hat{k}}(c) \text{ for some } \hat{k} \in K\}$
Proof

\[ M(c) := \{ \hat{m} | \hat{m} = Dec_k(c) \text{ for some } \hat{k} \in K \} \]

- \(|M(c)| \leq |K|\). Why?

- Since we assumed \(|K| < |M|\), this means that there is some \(m' \in M\) such that \(m' \notin M(c)\).

- But then
  \[ \Pr[M = m' | C = c] = 0 \neq \Pr[M = m'] \]

  And so the scheme is not perfectly secret.
Shannon’s Theorem

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

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

***Theorem only applies when \(|M| = |K| = |C|\).***
Some Examples

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