Perfect Secrecy（完美保密性）

S. Zhong Y. Zhang

Computer Science and Technology Department
Nanjing University

Outline

1. Let's play a game
2. Brief review of Probability
3. Perfectly-Secret Encryption
   - Definition of an encryption scheme
   - Let us be an adversary
   - Definition of perfectly secrecy
4. The One-Time Pad (Vernam's Cipher)
5. Limitations of Perfect Secrecy
6. Shannon's Theorem

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

Let’s play a game called “10 questions”

Use up-to-10 YES or NO questions to guess which province do I come from.

图: China map (courtesy of chinadiscovery.com)

Game review

Q: What guides your guesses? Why do you make new guesses?
A: Probabilities. You are actually reasoning about the probabilities.

1. Let's play a game
2. Brief review of Probability
3. Perfectly-Secret Encryption
4. The One-Time Pad (Vernam's Cipher)
5. Limitations of Perfect Secrecy
6. Shannon's Theorem

Probability[1]

Many events cannot be predicted with total certainty. The probability (概率) is introduced to define or refer to how likely events are to happen. For instance,

$$\mathit{Pr}[\text{女神, 男神, 霸道总裁统统爱上我}] = 0.00001$$

$$\mathit{Pr}[\text{你此刻正在看/听这段文字}] = 0.99999$$

[1] materials courtesy of mathsisfun.com

Defining Classical Probability

Consider a game or experiment (试验) with a set of possible outcomes $\mathcal{O}$ called sample space (样本空间). An event (事件) A is any collection of possible outcomes, that is, any subset of $\mathcal{O}$. Define the probability of event A as

$$Pr[A] = \frac{\text{number of outcomes in } A}{\text{total number of possible outcomes}}$$

- The above definition is called "classical definition of probability" (古典概率定义)
- It assumes the sample space is finite.
- It assumes outcomes are equally likely to happen.

An example of dice-throwing

Take "throwing a dice" for instance. Let X be the point we will get,

$$\mathcal{O} = \{X = 1, X = 2, \ldots, X = 6\}$$

$$Pr[X = 6] = |\{\text{X=6}\}|/|\mathcal{O}| = 1/6$$

$$Pr[X \geq 5] = |\{\text{X= 5, X= 6}\}|/|\mathcal{O}| = 2/6$$

Defining Probability Statistically

The two assumptions of classical probability definition often do not hold. People usually use a statistical definition:

`Repeat the experiment for` n `times and let` n_A `be the number of times that event A happens. Call` $\frac{n_A}{n}$ `event A's` `cumulative relative frequency` `or CRF(A). Define the probability of A as`

$$Pr[A] = \lim_{n \to \infty} CRF(A)$$

- The above experiment is called the Bernouli experiment .
- Modern axiom-systematic definition of probability is proposed by Andrey Nikolaevich Kolmogorov based on measure theory.

Conditional probability

Consider two events A and B. The conditional probability (条件概率) of A given B happens is defined as

$$Pr[A|B] = \frac{Pr[A \wedge B]}{Pr[B]},$$

where $A \wedge B$ refers to the event that A and B both happen and is defined as

$$Pr[A \wedge B] = Pr[A \cap B].$$

For instance in the dice-throwing game,

$$Pr[X = 6|X >= 5] = |\{X = 5\} \cap \{X = 5, X = 6\}|/|\{X = 5, X = 6\}| = 1/2$$

$$Pr[X >= 5|X = 6] = |\{X = 5\} \cap \{X = 5, X = 6\}|||\{X = 6\}| = 1$$

Considering a game of sampling random variables

Let X and Y be two random variables, and let $\mathcal{X}$ and $\mathcal{Y}$ be their samping spaces. The conditional probability of event $X = x$ happens given event $Y = y$ happens is

$$Pr[X = x | Y = y] = \frac{Pr[X = x \wedge Y = y]}{Pr[Y = y]}.$$

- X and Y are (mutually) independent (独立) iff (if and only if) for all possible x and y

$$Pr[X = x \wedge Y = y] = Pr[X = x] \cdot Pr[Y = y].$$

- Thus, X and Y are independent iff for all x and y

$$Pr[X = x | Y = y] = Pr[X = x].$$

Extending to n variables

Given n random variables $X_1, X_2, \ldots, X_n$ with sampling spaces $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$,

- these n variables are (mutually) independent (独立) iff for all possible $x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2, \ldots, x_n \in \mathcal{X}_n$

$$Pr[X_1 = x_1 \wedge X_2 = x_2 \wedge \ldots, \wedge X_n = x_n] = Pr[X_1 = x_1] \cdot \ldots \cdot Pr[X_n = x_n].$$

- these n variables are pairwise independent (两两独立) iff for all possible $x_i \in \mathcal{X}_i, x_j \in \mathcal{X}_j$ and all possible $i, j \in \{1, 2, \ldots, n\}$ and $i \neq j$

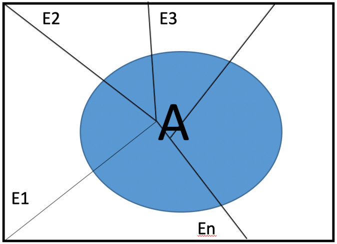
$$Pr[X_i = x_i \wedge X_j = x_j] = Pr[X_i = x_i] \cdot Pr[X_j = x_j].$$

`Q: Can you give an example that random variables` X, Y, Z `are mutually independent but not pairwise independent?`
`Q: Can you give an example that` X, Y, Z `are pairwise independent but not independent?`

Total Probability Formula

Given n mutally exclusive events $E_1, E_2, \ldots, E_n$ that form a partition of the sample space $\mathcal{O}$, the total probability formula or law (**全概率公式**) specifies that the probability of any event A can be computed as

$$Pr[A] = \sum_{i=1}^{n} Pr[A|E_i] \cdot Pr[E_i].$$



Bayes' Theorem

Given two events A and B, the Bayes' Theorem (贝叶斯定理) states

$$Pr[A|B] = \frac{Pr[A] \cdot Pr[B|A]}{Pr[B]}.$$

- It can help you to reason about the chance of one event given another has happened.

A "Cloud in the morning and Rain in the day" example

You are planning a picnic, but the morning is cloudy. You know the following

- 50% of all rainy days start off cloudy! :(

$$Pr[Cloud|Rain] = 50\%$$

- Cloudy mornings are common (about 40% of days start cloudy)

$$Pr[Cloud] = 40\%$$

- And this is a dry month (only 3 of 30 days tend to be rainy, or 10%)

$$Pr[Rain] = 10\%$$

Should you go?

$$Pr[Rain|Cloud] = ?$$

Bayes' Theorem in sampling-random-variables game

Let X and Y be two random variables, and let $\mathcal{X}$ and $\mathcal{Y}$ be the range spaces of X and Y respectively. Bayes' Theorem states

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \cdot Pr[Y = y | X = x]}{Pr[Y = y]}.$$

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption
- Definition of an encryption scheme
- Let us be an adversary
- Definition of perfectly secrecy

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

The start of "unbreakable cipher"

In 1949, C.E. Shannon published a paper named "Communication Theory of Secrecy Systems"

- In 1948, Shannon published his landmark paper "A Mathematical Theory of Communication" which founds the Information Theory
- In the CTSS paper, Shannon proved criteria of a unbreakable crypgraphy.
- Shannon proved Vernam cipher was unbreakable.

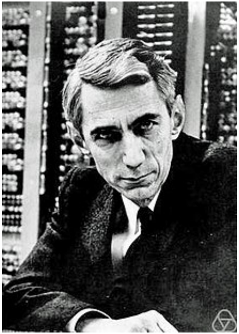


图: Claude E. Shannon (1916-2001), founder of Information Theory. Photo courtesy of wiki

Shannon's definition of a cipher system

In "Communication Theory of Secrecy Systems", Shannon defines a secrecy communication system or a cipher system as follows.

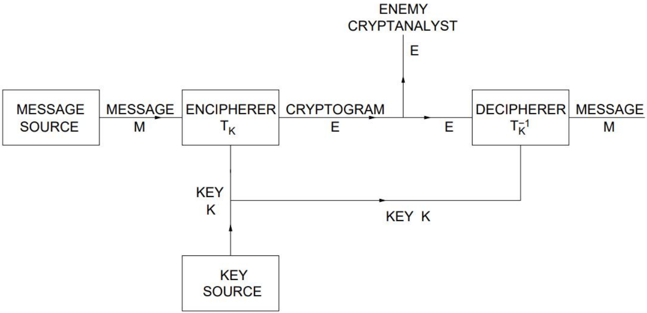


图: The cipher system proposed in Shannon's paper "Communication Theory of Secrecy Systems"

Defining an encryption scheme[3]

A encryption scheme Π, also called a cipher or a cryptosystem, is defined by three algorithms **Gen**, **Enc**, and **Dec**, as well as a specification of a finite message space $\mathcal{M}$ with $|\mathcal{M}| > 1$.

- **Gen**: a probabilistic algorithm that outputs a key k according to some distribution[2] from a finite key space $\mathcal{K}$.

$$k \leftarrow Gen.$$

- **Enc**: an algorithm that takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c:

$$c \leftarrow Enc_k(m)(\text{probabilistic}) \text{ OR } c := Enc_k(m)(\text{deterministic}).$$

- **Dec**: a deterministic algorithm that takes as input a ciphertext c from the set of all ciphertexts $\mathcal{C}$ and a key $k \in \mathcal{K}$, and outputs a message $m \in \mathcal{M}$.

$$m := Dec_k(c).$$

[2] Often a uniformly random distribution is used

[3] In fact we are defining a symmetric or private-key cipher here

Example 1: the shift cipher Π_{shft1}

The cipher Π_{shft1} is defined as

- $\mathcal{M} = \{0, \ldots, 25\}$ or $\{a, \ldots, z\}$
- **Gen**: a probabilistic algorithm that outputs a key k uniformly chosen from a finite key space $\mathcal{K}$.

$$k \xleftarrow{\$} \{0, \ldots, 25\}$$

- **Enc**: an algorithm that takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c:

$$C = M + k \mod 26$$

- **Dec**: a deterministic algorithm that takes as input a ciphertext c from the set of all ciphertexts $\mathcal{C}$ and a key $k \in \mathcal{K}$, and outputs a message $m \in \mathcal{M}$.

$$M := C - k \mod 26.$$

Example 2: the shift cipher Π_{shft2}

The cipher Π_{shft2} is defined as

- $\mathcal{M} = \{0, \ldots, 25\}^3$ or $\{a, \ldots, z\}^3$
- **Gen**: a probabilistic algorithm that outputs a key k uniformly chosen from a finite key space $\mathcal{K}$.

$$k \xleftarrow{\$} \{0, \ldots, 25\}$$

- **Enc**: an algorithm that takes as input a key $k \in \mathcal{K}$ and a message $M = m_1||m_2||m_3 \in \mathcal{M}$, and outputs a ciphertext c:

$$C = (m_1 + k \mod 26)||(m_2 + k \mod 26)||(m_3 + k \mod 26)$$

- **Dec**: a deterministic algorithm that takes as input a ciphertext c from the set of all ciphertexts $\mathcal{C} = \{c_1||c_2||c_3\}$ and a key $k \in \mathcal{K}$, and outputs a message $m \in \mathcal{M}$.

$$M := (c_1 - k \mod 26)||(c_2 - k \mod 26)||(c_3 - k \mod 26).$$

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption
- Definition of an encryption scheme
- Let us be an adversary
- Definition of perfectly secrecy

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

Probabilistic analysis on Π_{shft2}

Recall the shift cipher Π_{shft2}:
$\mathcal{M} = \{0, \ldots, 25\}^3 or \{a, \ldots, z\}^3$
Gen: $k \xleftarrow{\$} \{0, \ldots, 25\}$.
Enc: $C = (m_1 + k \mod 26) || (m_2 + k \mod 26) || (m_3 + k \mod 26)$.

- Q: Say a message M is sampled following the distribution

$$Pr[M = ann] = 0.6 \text{ and } Pr[M = bob] = 0.4.$$

  After encrypting M with Π_{shft2}, the adversary sees the ciphertext DQQ. Can it know M?
- A: Unfortunately yes, the adversary can know M is ann. :(

Adversary's reasoning

A smart adversary can know M according to the following reasoning. According to Total Probability Theorm,

$$\begin{aligned}
& Pr[C = DQQ] \\
= \;& Pr[M = ann] \cdot Pr[C = DQQ | M = ann] \\
& + Pr[M = bob] \cdot Pr[C = DQQ | M = bob] \\
= \;& Pr[M = ann] \cdot Pr[K = 3] + Pr[M = bob] \cdot Pr[K = \emptyset] \\
= \;& 0.6 \cdot 1/26 + 0.4 \cdot 0 \\
= \;& 3/130.
\end{aligned}$$

Based on Bayes' Theorem,

$$Pr[M = ann | C = DQQ] = \frac{Pr[M = ann] \cdot Pr[C = DQQ | M = ann]}{Pr[C = DQQ]} = 1.$$

Similar probabilistic analysis on Π_{shft1}

Recall cipher Π_{shft1}:

Gen: $k \stackrel{\$}{\leftarrow} \{0, \ldots, 25\}$.

Enc: $C = M + k \mod 26$.

$\mathcal{M} = \{0, \ldots, 25\}$ or $\{a, \ldots, z\}$.

Q1: Say our message M follows the distribution

$$Pr[M = b] = 0.6 \text{ and } Pr[M = g] = 0.4.$$

What the probability that the ciphertext is Z given M as above?

A: $$\begin{aligned} Pr[C = Z] &= Pr[M = b \wedge K = 24] + Pr[M = g \wedge K = 19] \\ &= Pr[M = b] \cdot Pr[K = 24] + Pr[M = g] \cdot Pr[K = 19] \\ &= 0.6 \cdot 1/26 + 0.4 \cdot 1/26 = 1/26. \end{aligned}$$

After-encryption probabilistic analysis

Q2: Now we sample a message M follows the distribution $Pr[M = b] = 0.6 \text{ and } Pr[M = g] = 0.4.$, encrypt it and get a ciphertext Z. What the probability that $M = b$?

A: Based on Bayes' Theorem, we have

$$Pr[M = b | C = Z] = \frac{Pr[M=b] \cdot Pr[C=Z | M=b]}{Pr[C=Z]} = \frac{Pr[M=b] \cdot Pr[K=24]}{Pr[C=Z]} = \frac{Pr[M=b] \cdot 1/26}{1/26} = Pr[M = b] = 0.6$$

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption
- Definition of an encryption scheme
- Let us be an adversary
- Definition of perfectly secrecy

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

Revisit the definition of Perfectly Secret Encryption

定义 3.1 (Perfectly Secret Encryption).

An encryption scheme (**Gen**,**Enc**,**Dec**) over a massage space $\mathcal{M}$ is **perfect secret** if for every possible distribution over $\mathcal{M}$,

$$Pr[M = m | C = c] = Pr[M = m]$$

holds for every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$ that $Pr[C = c] > 0$.

Revisiting Π_{shft1} and Π_{shft2}

- According to the definition, it is easy to know Π_{shft2} is not perfectly-secret:

$$Pr[M = ann | C = DQQ] = 1 \neq Pr[M = ann] = 0.6.$$

- Q: Is $\Pi_{shft1} perfectly - secret?$
  A: Probably yes, but we still need to prove it.

定理 3.2.

Π_{shft1} *is a perfectly-secret encryption scheme.*

Proof: For any $m \in \mathcal{M} = \{0, \ldots, 25\}$, any $c \in \mathcal{C}$ and any possible distribution over $\mathcal{M}$ we have:

$$
\begin{aligned}
& Pr[M = m | C = c] \\
= & Pr[M = m \wedge C = c] / Pr[C = c] \\
= & \frac{Pr[M = m] \cdot Pr[C = c | M = m]}{Pr[M = 0 \wedge C = c] + \ldots + Pr[M = 25 \wedge C = c]} \\
= & \frac{Pr[M = m] \cdot Pr[k = c - m \mod 26]}{Pr[M = 0] \cdot Pr[C = c | M = 0] + \ldots + Pr[M = 25] \cdot Pr[C = c | M = 25]} \\
= & \frac{Pr[M = m] Pr[k = c - m \mod 26]}{Pr[M = 0] Pr[k = c \mod 26] + \ldots + Pr[M = 25] Pr[k = c - 25 \mod 26]} \\
= & Pr[M = m].
\end{aligned}
$$

An equivalent definition of perfect secrecy

We have an equivalent and useful formulation of perfect secrecy.

引理 3.3.

*An encryption scheme (**Gen**, **Enc**, **Dec**) over message space $\mathcal{M}$ is perfectly secret if and only if for every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:*

$$Pr[C = c|M = m] = Pr[C = c|M = m'].$$

- This formulation states that the probability distribution over $\mathcal{C}$ is independent of the plaintext.
- "It's impossible to distinguish an encryption of m_0 from an encryption of m_1"

An equivalent definition of perfect secrecy

Proof:

"$\Leftarrow$": Assume $Pr[C = c|M = m] = Pr[C = c|M = m']$ holds for every possible $m, m' \in \mathcal{M}$. We have:

$$
\begin{aligned}
& Pr[M = m|C = c] \\
= \quad & Pr[M = m \wedge C = c]/Pr[C = c] \\
= \quad & \frac{Pr[M = m] \cdot Pr[C = c|M = m]}{\sum_{m' \in \mathcal{M}} Pr[M = m' \wedge C = c]} \\
= \quad & \frac{Pr[M = m] \cdot Pr[C = c|M = m]}{\sum_{m' \in \mathcal{M}} Pr[M = m'] \cdot Pr[C = c|M = m']} \\
= \quad & Pr[M = m]
\end{aligned}
$$

Proof (cont'd):"$\Rightarrow$": When $m' = m$, "$\Rightarrow$" is always true.Now we only consider $m' \neq m$. For every such $m' \in \mathcal{M}$, we can construct a message distribution such that $Pr[M = m] = 0.7$ and $Pr[M = m'] = 0.3$. According to the definition of perfect secrecy, we know for every $c \in \mathcal{C}$:

$$
\begin{aligned}
& Pr[M = m] \\
= \;& Pr[M = m | C = c] \\
= \;& Pr[M = m \wedge C = c] / Pr[C = c] \\
= \;& \frac{Pr[M = m] \cdot Pr[C = c | M = m]}{Pr[M = m' \wedge C = c] + Pr[M = m \wedge C = c]} \\
= \;& \frac{Pr[M = m] \cdot Pr[C = c | M = m]}{Pr[M = m'] \cdot Pr[C = c | M = m'] + Pr[M = m] \cdot Pr[C = c | M = m]}
\end{aligned}
$$

Therefore we have

$Pr[C = c | M = m] = 0.3 Pr[C = c | M = m'] + 0.7 Pr[C = c | M = m]$, and

$$Pr[C = c | M = m] = Pr[C = c | M = m'].$$

Perfect adversarial indistinguishability

Now we give a game-based definition of perfect secrecy on an encryption scheme $\Pi = \{Gen, Enc, Dec\}$ with message space $\mathcal{M}$. **The adversarial indistinguishability game/experiment** $PrivK^{eav}_{\mathcal{A},\Pi}$ between the adversary and a challenger:

1. The adversary $\mathcal{A}$ chooses a pair of messages $m_0, m_1 \in \mathcal{M}$, and sends them to the challenger.
2. The challenger runs **Gen** to generate a key k, chooses a uniform bit $b \in \{0, 1\}$, and computes the *challenge ciphertext* by encrypting m_b:
$$c \leftarrow Enc_k(m_b).$$
3. The challenger sends c to the adversary.
4. Based on c, the adversary guess the correct value of b, and outputs b' as its answer to the challenge.
5. The output/result of the game is defined to 1:
$$PrivK^{eav}_{\mathcal{A},\Pi} = 1$$
if $b' = b$ ($\mathcal{A}$ succeeds in the game), and 0 otherwise.

Perfect adversarial indistinguishability

定义 3.4.

Perfect adversary indistinguishability Encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every $\mathcal{A}$ it holds that

$$Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}.$$

- The definition states that every adversary would do no better or worse in the game than making a uniformly random guess.

Perfect (adversarial) indistinguishability

引理 3.5.

Encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$ is ***perfectly secret*** *if and only if it is perfectly indistinguishable.*

Perfect (adversarial) indistinguishability

Example: let Π denote the Vigenere cipher for the message space of two-character strings, and where the period is chosen uniformly in $\{1, 2\}$. We claim Π is NOT perfectly indistinguishable.
To prove this, we construct an adversary $\mathcal{A}$ for which $Pr[PrivK^{eav}_{\mathcal{A},\Pi}] > \frac{1}{2}$.
Specifically $\mathcal{A}$ does:

1. Choose $m_0 = aa$ and $m_1 = ab$.
2. Upon receiving the challenge ciphertext $c = c_1 c_2$, output $b = 0$ if $c_1 = c_2$, and $b = 1$ otherwise.

Now what does $Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1]$ equal?

Perfect (adversarial) indistinguishability

$$\begin{aligned} & Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1] \\ = \ & 0.5Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1 | b = 0] + 0.5Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1 | b = 1] \\ = \ & 0.5Pr[\mathcal{A} \text{ outputs } 0 | b = 0] + 0.5Pr[\mathcal{A} \text{ outputs } 1 | b = 1] \end{aligned}$$

In addition,
$Pr[\mathcal{A} \text{ outputs } 0 | b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26}$
$Pr[\mathcal{A} \text{ outputs } 1 | b = 1] = 1 - Pr[\mathcal{A} \text{ outputs } 0 | b = 1] = 1 - \frac{1}{2} \cdot \frac{1}{26}$
Then, we have:

$$Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}(\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26} + 1 - \frac{1}{2} \cdot \frac{1}{26}) = 0.75 > \frac{1}{2}$$

Therefore, Π is not perfectly indistinguishable.

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

The One-Time Pad, a perfectly-secret encryption scheme

The One-Time Pad

Let $a \oplus b$ denote the bitwise exclusive-or (XOR) of two binary strings a and b, the **One-Time Pad** is as follows:

1. Fix an integer $l > 0$. $\mathcal{M} = \{0,1\}^l$, $\mathcal{K} = \{0,1\}^l$, $\mathcal{C} = \{0,1\}^l$.
2. **Gen**: $K \xleftarrow{\$} \mathcal{K}$, i.e. $Pr[K = k] = 1/2^l$ for every $k \in \mathcal{K}$.
3. $\mathbf{Enc}_K(M)$: $C := M \oplus K$.
4. $\mathbf{Dec}_K(C)$: $M := C \oplus K$.

Correctness: $M = C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M$.
Secrecy: ?

定理 4.1.

The One-Time Pad is a perfectly-secret encryption scheme.

Proof: Fix arbitrary input distribution over $\mathcal{M}$, for every possible m and c,

$$\begin{aligned}
& Pr[M = m | C = c] \\
= \; & Pr[M = m, C = c] / Pr[C = c] \\
= \; & Pr[K = m \oplus c] \cdot Pr[M = m] / \sum_{m' \in \mathcal{M}} (Pr[M = m'] \cdot Pr[C = c | M = m']) \\
= \; & Pr[K = m \oplus c] \cdot Pr[M = m] / \sum_{m' \in \mathcal{M}} (Pr[M = m'] \cdot Pr[K = m' \oplus c]) \\
= \; & 2^{-l} Pr[M = m] / (2^{-l} \sum_{m' \in \mathcal{M}} Pr[M = m']) \\
= \; & 2^{-l} Pr[M = m] / 2^{-l} \\
= \; & Pr[M = m]
\end{aligned}$$

Limitations of One-Time Pad

Perfect secrecy sounds perfect. But any drawbacks?

- the key is required to be as long as the message.
  $M = 011100001100011100001101010101010100000000000011001......$
  $K = 100011100001100011100001101010101010100000000000011......$
- only secure if used once (with the same key).
  $C_1 = M_1 \oplus K; C_2 = M_2 \oplus K \Rightarrow C_1 \oplus C_2 = M_1 \oplus M_2.$
- only secure against ciphertext-only attack.
  $M = 101,\ Enc_K(M) = 111 \Rightarrow K = 010$

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

Limitations of Perfect Secrecy

定理 5.1.

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

Proof: Consider the uniform distribution over $\mathcal{M}$ (as the input), we know there is a $c \in \mathcal{C}$ such that $Pr[C = c] > 0$. According to the definition of perfect secrecy, we know for every $m \in \mathcal{M}$,

$$Pr[M = m | C = c] = Pr[M = m] = 1/|\mathcal{M}| > 0,$$

which implies there is at least one key k for each m such that $\mathbf{Dec}_k(c) = m$. Accordingly, there are at least $|\mathcal{M}|$ different keys in $\mathcal{K}$, one for each different $m \in \mathcal{M}$. Thus, we have $|\mathcal{K}| \geq |\mathcal{M}|$.

1 Let's play a game

2 Brief review of Probability

3 Perfectly-Secret Encryption

4 The One-Time Pad (Vernam's Cipher)

5 Limitations of Perfect Secrecy

6 Shannon's Theorem

Shannon's Theorem

定理 6.1 (Shannon's Theorem).

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

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

- Only applies when $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$.
- Useful for deciding whether a given scheme is perfectly secret.