Perfect Secrecy

Diego F. Aranha

Institute of Computing
UNICAMP

Introduction

Objectives:

- How can we determine if a system is secure?
- We need more precise metrics than simple guidelines.

Introduction

Objectives:

- How can we determine if a system is secure?
- We need more precise metrics than simple guidelines.

Hidden intentions:

- Discuss an upper bound for security.
- Detect if the requirements for attaining the upper bound are viable in practice.

Security notions

1. Computational Security(asymptotic):
   - Cost of best known attack exceeds adversary power.
   - Security against one type of attack does not exclude others.
2. Provable security (conditional):
   - Reduction from a conjectured hard problem to the cryptosystem problem.
   - Sometimes, the problem was not as hard as it seemed.
   - Analogous to NP-completeness reductions.
3. Unconditional security:
   - Resists attacks with unlimited computational power.
   - The only possible Cryptanalysis must be outside the threat model.

Security notions

1. Computational Security(asymptotic):
   - Cost of best known attack exceeds adversary power.
   - Security against one type of attack does not exclude others.
2. Provable security (conditional):
   - Reduction from a conjectured hard problem to the cryptosystem problem.
   - Sometimes, the problem was not as hard as it seemed.
   - Analogous to NP-completeness reductions.
3. Unconditional security:
   - Resists attacks with unlimited computational power.
   - The only possible Cryptanalysis must be outside the threat model.

Focus: Unconditionally secure cryptosystems against passive attacks.

Security notions

1. Computational Security(asymptotic):
   - Cost of best known attack exceeds adversary power.
   - Security against one type of attack does not exclude others.

2. Provable security (conditional):
   - Reduction from a conjectured hard problem to the cryptosystem problem.
   - Sometimes, the problem was not as hard as it seemed.
   - Analogous to NP-completeness reductions.

3. Unconditional security:
   - Resists attacks with unlimited computational power.
   - The only possible Cryptanalysis must be outside the threat model.

Focus: Unconditionally secure cryptosystems against passive attacks.

Note: We need probability, not complexity theory!

Importance of precise definitions

Example: How to formalize security of a cryptosystem with relation to confidentiality?

Answer 1

Secure if an adversary cannot obtain the key from ciphertext.

Importance of precise definitions

Example: How to formalize security of a cryptosystem with relation to confidentiality?

Answer 1

Secure if an adversary cannot obtain the key from ciphertext.

Answer 2

Secure if an adversary cannot obtain the plaintext from ciphertext.

Importance of precise definitions

Example: How to formalize security of a cryptosystem with relation to confidentiality?

Answer 1

Secure if an adversary cannot obtain the key from ciphertext.

Answer 2

Secure if an adversary cannot obtain the plaintext from ciphertext.

Answer 3

Secure if an adversary cannot determine a single letter of the plaintext from the ciphertext.

Importance of precise definitions

Example: How to formalize security of a cryptosystem with relation to confidentiality?

Answer 1

Secure if an adversary cannot obtain the key from ciphertext.

Answer 2

Secure if an adversary cannot obtain the plaintext from ciphertext.

Answer 3

Secure if an adversary cannot determine a single letter of the plaintext from the ciphertext.

Answer 4

Secure if an adversary cannot obtain plaintext information from ciphertext only.

Importance of precise definitions

Example: How to formalize security of a cryptosystem with relation to confidentiality?

Answer 1

Secure if an adversary cannot obtain the key from ciphertext.

Answer 2

Secure if an adversary cannot obtain the plaintext from ciphertext.

Answer 3

Secure if an adversary cannot determine a single letter of the plaintext from the ciphertext.

Answer 4

Secure if an adversary cannot obtain plaintext information from ciphertext only.

Final Answer

Secure if an adversary cannot compute a function of the plaintext from ciphertext only.

Probability

Definition

A **discrete random variable** $\boldsymbol{X}$ consists in a finite set X and a **probability distribution** defined over X. The probability of a symbol $\boldsymbol{X}$ taking value x is denoted by $\boldsymbol{Pr}[\boldsymbol{X} = x]$ or $\boldsymbol{Pr}[x]$ and is such that $0 \leq \boldsymbol{Pr}[x]$ and $\forall x \in X, \sum_{x \in X} \boldsymbol{Pr}[x] = 1$.

Event

A subset $E \subseteq X$ is an **event** if $\boldsymbol{Pr}[x \in E] = \sum_{x \in E} \boldsymbol{Pr}[x]$.

Examples:

1. Coin: $\boldsymbol{Pr}[heads] = \boldsymbol{Pr}[tails] = 1/2$.
2. Sum of two unbiased dice: $\boldsymbol{Pr}[2] = \boldsymbol{Pr}[12] = 1/36, \boldsymbol{Pr}[3] = \boldsymbol{Pr}[11] = 1/18, \boldsymbol{Pr}[4] = 1/12$.

Probability

Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ discrete random variables in the sets X e Y, respectively.

Joint probability

The **joint probability** $\boldsymbol{Pr}[x, y]$ is the probability of $\boldsymbol{X}$ taking value x and $\boldsymbol{Y}$ taking value y.

Conditional probability

The **conditional probability** $\boldsymbol{Pr}[x|y]$ is the probability of $\boldsymbol{X}$ taking value x, given that $\boldsymbol{Y}$ takes value y.

Independent random variables

Random variables $\boldsymbol{X}$ and $\boldsymbol{Y}$ are independent if
$\forall x \in X, \forall y \in Y, \boldsymbol{Pr}[x, y] = \boldsymbol{Pr}[x]\boldsymbol{Pr}[y]$.

Probability

We have that $\boldsymbol{Pr}[x, y] = \boldsymbol{Pr}[x|y]\boldsymbol{Pr}[y] = \boldsymbol{Pr}[y|x]\boldsymbol{Pr}[x]$.

Probability

We have that $\boldsymbol{Pr}[x, y] = \boldsymbol{Pr}[x|y]\boldsymbol{Pr}[y] = \boldsymbol{Pr}[y|x]\boldsymbol{Pr}[x]$.

Bayes' Theorem

If $\boldsymbol{Pr}[y] > 0$ then:

$$\boldsymbol{Pr}[x|y] = \frac{\boldsymbol{Pr}[x]\boldsymbol{Pr}[y|x]}{\boldsymbol{Pr}[y]}$$

Corollary: $\boldsymbol{X}$ and $\boldsymbol{Y}$ are independent variables iff $\forall x \in X, \forall y \in Y, \boldsymbol{Pr}[x|y] = \boldsymbol{Pr}[x]$.

Probability

We have that $\boldsymbol{Pr}[x, y] = \boldsymbol{Pr}[x|y]\boldsymbol{Pr}[y] = \boldsymbol{Pr}[y|x]\boldsymbol{Pr}[x]$.

Bayes' Theorem

If $\boldsymbol{Pr}[y] > 0$ then:

$$\boldsymbol{Pr}[x|y] = \frac{\boldsymbol{Pr}[x]\boldsymbol{Pr}[y|x]}{\boldsymbol{Pr}[y]}$$

Corollary: $\boldsymbol{X}$ and $\boldsymbol{Y}$ are independent variables iff $\forall x \in X, \forall y \in Y, \boldsymbol{Pr}[x|y] = \boldsymbol{Pr}[x]$.

Example: $\boldsymbol{X}$ is the sum of two dice, $\boldsymbol{Y}$ is the equality of two sides: $\boldsymbol{Pr}[equal] = \frac{1}{6}, \boldsymbol{Pr}[\neg equal] = \frac{5}{6}, \boldsymbol{Pr}[equal|4] = \frac{1}{3}, \boldsymbol{Pr}[4|equal] = \frac{1}{6}$.

Application to cryptography

Suppose the following probabilities:

- Random variable $\boldsymbol{K}$ (key).
- Random variable $\boldsymbol{M}$ (plaintext).
- Random variable $\boldsymbol{C}$ (ciphertext).
- $\boldsymbol{K}$ and $\boldsymbol{M}$ are independent.

We have that:

- Probability of a certain key is $\boldsymbol{Pr}[\boldsymbol{K} = K]$.
- Probability *a priori* of a certain plaintext is $\boldsymbol{Pr}[\boldsymbol{M} = m]$.
- Probability *a posteriori* of a certain ciphertext is $\boldsymbol{Pr}[\boldsymbol{C} = c]$.

Convention: Consider non-zero probabilities only.

Ciphertext probability

Definitions

Let $C(k) = Enc_k(m), m \in \mathcal{M}$ the **set of valid ciphertexts** for key k.

$$\forall c \in \mathcal{C}, \boldsymbol{Pr}[\boldsymbol{C} = c] = \sum_{k, c \in C(k)} \boldsymbol{Pr}[\boldsymbol{K} = k]\boldsymbol{Pr}[\boldsymbol{M} = Dec_k(c)].$$

We can compute conditional probabilities:

- $$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m] = \sum_{k, m = Dec_k(c)} \boldsymbol{Pr}[\boldsymbol{K} = k]$$
- $$\boldsymbol{Pr}[\boldsymbol{M} = m | \boldsymbol{C} = c] = \frac{\boldsymbol{Pr}[\boldsymbol{M} = m] \cdot \sum_{k, m = Dec_k(c)} \boldsymbol{Pr}[\boldsymbol{K} = k]}{\sum_{k, c \in C(k)} \boldsymbol{Pr}[\boldsymbol{K} = k]\boldsymbol{Pr}[\boldsymbol{M} = Dec_k(c)]}.$$

Perfect Secrecy

Definition

Let Gen, Enc, Dec functions for key generation, encryption and decryption. A cryptosystem (Gen, Enc, Dec) provides **perfect secrecy** iff $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$ and over any probability distribution over $\mathcal{M}$:

$$\boldsymbol{Pr}[\boldsymbol{M} = m | \boldsymbol{C} = c] = \boldsymbol{Pr}[\boldsymbol{M} = m].$$

In other words:

$$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m] = \boldsymbol{Pr}[\boldsymbol{C} = c].$$

The probability of a plaintext m, given that the ciphertext c was observed is identical to the *a priori* probability of plaintext m.

Important: Do transposition ciphers attain perfect secrecy?

Perfect indistinguishability

Lemma

A cryptosystem (Gen, Enc, Dec) over a message space $\mathcal{M}$ provides perfect secrecy iff $\forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C}$ for all probability distributions over $\mathcal{M}$:

$$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1].$$

Prova:

$\rightarrow$ If a system provides perfect secrecy, $\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1]$.

$\leftarrow$ Let $m_0 \in \mathcal{M}$ and $p = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m]$.

Perfect indistinguishability

Lemma

A cryptosystem (Gen, Enc, Dec) over a message space $\mathcal{M}$ provides perfect secrecy iff $\forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C}$ for all probability distributions over $\mathcal{M}$:
$$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1].$$

Prova:

$\rightarrow$ If a system provides perfect secrecy,
$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1].$

$\leftarrow$ Let $m_0 \in \mathcal{M}$ and $p = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m].$

$$\boldsymbol{Pr}[\boldsymbol{C} = c] = \sum_{m \in \mathcal{M}} \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m] \boldsymbol{Pr}[\boldsymbol{M} = m]$$

Perfect indistinguishability

Lemma

A cryptosystem (Gen, Enc, Dec) over a message space $\mathcal{M}$ provides perfect secrecy iff $\forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C}$ for all probability distributions over $\mathcal{M}$:

$$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1].$$

Prova:

- $\rightarrow$ If a system provides perfect secrecy,
  $\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1]$.

- $\leftarrow$ Let $m_0 \in \mathcal{M}$ and $p = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m]$.

$$\begin{aligned} \boldsymbol{Pr}[\boldsymbol{C} = c] &= \sum_{m \in \mathcal{M}} \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m] \boldsymbol{Pr}[\boldsymbol{M} = m] \\ &= \sum_{m \in \mathcal{M}} p \cdot \boldsymbol{Pr}[\boldsymbol{M} = m] = p \cdot \sum_{m \in \mathcal{M}} \boldsymbol{Pr}[\boldsymbol{M} = m] \end{aligned}$$

Perfect indistinguishability

Lemma

A cryptosystem (Gen, Enc, Dec) over a message space $\mathcal{M}$ provides perfect secrecy iff $\forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C}$ for all probability distributions over $\mathcal{M}$:
$$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1].$$

Prova:

$\rightarrow$ If a system provides perfect secrecy,
$\boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_1]$.

$\leftarrow$ Let $m_0 \in \mathcal{M}$ and $p = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0] = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m]$.

$$\begin{aligned}
\boldsymbol{Pr}[\boldsymbol{C} = c] &= \sum_{m \in \mathcal{M}} \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m] \boldsymbol{Pr}[\boldsymbol{M} = m] \\
&= \sum_{m \in \mathcal{M}} p \cdot \boldsymbol{Pr}[\boldsymbol{M} = m] = p \cdot \sum_{m \in \mathcal{M}} \boldsymbol{Pr}[\boldsymbol{M} = m] \\
&= p = \boldsymbol{Pr}[\boldsymbol{C} = c | \boldsymbol{M} = m_0]. \qquad \square
\end{aligned}$$

Adversarial indistinguishability

Definition

Let $\mathcal{A}$ a passive adversary, $\Pi = (Gen, Enc, Dec)$ a cryptosystem and $Priv^{eav}_{\mathcal{A},\Pi}$ the execution of an experiment with $\mathcal{A}$:

1. $\mathcal{A}$ produces messages $m_0, m_1 \in \mathcal{M}$.
2. Key k is generated from Gen and a random bit b is chosen. Then $c = Enc_k(m_b)$ is computed and given to $\mathcal{A}$.
3. $\mathcal{A}$ outputs bit b'
4. The output of the experiment is 1 if $b' = b$ and 0 otherwise. $\mathcal{A}$ is successful when $Priv^{eav}_{\mathcal{A},\Pi} = 1$.

A cryptosystem $\Pi = (Gen, Enc, Dec)$ over a message space $\mathcal{M}$ provides perfect secrecy if for all adversaries $\mathcal{A}$:

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

Perfect secrecy

Theorem

Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, with integer n. Suppose that the n keys from the shift cipher are used with uniform probability. Then, for any plaintext probability distribution, the shift cipher provides perfect secrecy.

Perfect secrecy

Theorem

Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, with integer n. Suppose that the n keys from the shift cipher are used with uniform probability. Then, for any plaintext probability distribution, the shift cipher provides perfect secrecy.

$$\boldsymbol{Pr}[\boldsymbol{C} = c] \quad = \quad \sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{K} = k]\boldsymbol{Pr}[\boldsymbol{M} = Dec_k(c)]$$

Perfect secrecy

Theorem

Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, with integer n. Suppose that the n keys from the shift cipher are used with uniform probability. Then, for any plaintext probability distribution, the shift cipher provides perfect secrecy.

$$\begin{aligned} \boldsymbol{Pr}[\boldsymbol{C} = c] &= \sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{K} = k]\boldsymbol{Pr}[\boldsymbol{M} = Dec_k(c)] \\ &= \sum_{k \in \mathbb{Z}_n} \frac{1}{n}\boldsymbol{Pr}[\boldsymbol{M} = (c-k) \bmod n] \end{aligned}$$

Perfect secrecy

Theorem

Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, with integer n. Suppose that the n keys from the shift cipher are used with uniform probability. Then, for any plaintext probability distribution, the shift cipher provides perfect secrecy.

$$\begin{aligned}
\boldsymbol{Pr}[\boldsymbol{C} = c] &= \sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{K} = k] \boldsymbol{Pr}[\boldsymbol{M} = Dec_k(c)] \\
&= \sum_{k \in \mathbb{Z}_n} \frac{1}{n} \boldsymbol{Pr}[\boldsymbol{M} = (c - k) \bmod n] \\
&= \frac{1}{n} \sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = (c - k) \bmod n]
\end{aligned}$$

Perfect Secrecy

For a fixed c, values $(c - k) \bmod n$ form a permutation of $\mathbb{Z}_n$. Then:

$$\sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = (c - k) \bmod n] = \sum_{m \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = m] = 1$$

Perfect Secrecy

For a fixed c, values $(c - k) \bmod n$ form a permutation of $\mathbb{Z}_n$. Then:

$$\sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = (c - k) \bmod n] = \sum_{m \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = m] = 1$$

Thus:

$$\boldsymbol{Pr}[c] = \frac{1}{n}$$

Perfect Secrecy

For a fixed c, values $(c - k) \bmod n$ form a permutation of $\mathbb{Z}_n$. Then:

$$\sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = (c - k) \bmod n] = \sum_{m \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = m] = 1$$

Thus:

$$\boldsymbol{Pr}[c] = \frac{1}{n}$$

We also have that:

$$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \boldsymbol{Pr}[c|m] = \boldsymbol{Pr}[\boldsymbol{K} = (y - c) \bmod n] = \frac{1}{n}$$

Perfect Secrecy

For a fixed c, values $(c-k) \bmod n$ form a permutation of $\mathbb{Z}_n$. Then:

$$\sum_{k \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = (c-k) \bmod n] = \sum_{m \in \mathbb{Z}_n} \boldsymbol{Pr}[\boldsymbol{M} = m] = 1$$

Thus:

$$\boldsymbol{Pr}[c] = \frac{1}{n}$$

We also have that:

$$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \boldsymbol{Pr}[c|m] = \boldsymbol{Pr}[\boldsymbol{K} = (y-c) \bmod n] = \frac{1}{n}$$

By Bayes' Theorem:

$$\boldsymbol{Pr}[m|c] = \frac{\boldsymbol{Pr}[m]\boldsymbol{Pr}[c|m]}{\boldsymbol{Pr}[c]} = \frac{\boldsymbol{Pr}[m]\frac{1}{n}}{\frac{1}{n}} = \boldsymbol{Pr}[m]. \qquad \square$$

Perfect Secrecy

Shannon Theorem

Let S be a cryptosystem with $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|$. S provides perfect secrecy iff all possible keys are chosen with probability $1/|\mathcal{K}|$ and $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$ there is a single key such that $c = Enc_k(m)$.

Proof: Suppose that S provides perfect secrecy. By assumption, $|\mathcal{C}| = |Enc_k(m), k \in \mathcal{K}| = |\mathcal{K}|$. Hence, there are no $k_1 \neq k_2$ such that $Enc_{k_1}(m) = Enc_{k_2}(m) = c$.

Perfect Secrecy

Shannon Theorem

Let S be a cryptosystem with $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|$. S provides perfect secrecy iff all possible keys are chosen with probability $1/|\mathcal{K}|$ and $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$ there is a single key such that $c = Enc_k(m)$.

Proof: Suppose that S provides perfect secrecy. By assumption, $|\mathcal{C}| = |Enc_k(m), k \in \mathcal{K}| = |\mathcal{K}|$. Hence, there are no $k_1 \neq k_2$ such that $Enc_{k_1}(m) = Enc_{k_2}(m) = c$.

Let $n = |\mathcal{K}|, \mathcal{M} = m_i, 1 \leq i \leq n$ and $c \in \mathcal{C}$ a fixed ciphertext. We can label keys $k_1, k_2, , \ldots, k_n$ such that $Enc_{k_i}(m_i) = c$. By Bayes' Theorem:

$$\boldsymbol{Pr}[m_i|c] = \frac{\boldsymbol{Pr}[c|m_i]\boldsymbol{Pr}[m_i]}{\boldsymbol{Pr}[c]} = \frac{\boldsymbol{Pr}[\boldsymbol{K} = k_i]\boldsymbol{Pr}[m_i]}{\boldsymbol{Pr}[c]}$$

Perfect Secrecy

Shannon Theorem

Let S be a cryptosystem with $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|$. S provides perfect secrecy iff all possible keys are chosen with probability $1/|\mathcal{K}|$ and $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$ there is a single key such that $c = Enc_k(m)$.

Proof: Suppose that S provides perfect secrecy. By assumption, $|\mathcal{C}| = |Enc_k(m), k \in \mathcal{K}| = |\mathcal{K}|$. Hence, there are no $k_1 \neq k_2$ such that $Enc_{k_1}(m) = Enc_{k_2}(m) = c$.

Let $n = |\mathcal{K}|, \mathcal{M} = m_i, 1 \leq i \leq n$ and $c \in \mathcal{C}$ a fixed ciphertext. We can label keys $k_1, k_2, , \ldots, k_n$ such that $Enc_{k_i}(m_i) = c$. By Bayes' Theorem:

$$\boldsymbol{Pr}[m_i|c] = \frac{\boldsymbol{Pr}[c|m_i]\boldsymbol{Pr}[m_i]}{\boldsymbol{Pr}[c]} = \frac{\boldsymbol{Pr}[\boldsymbol{K} = k_i]\boldsymbol{Pr}[m_i]}{\boldsymbol{Pr}[c]}$$

For a system providing perfect secrecy:

$$\boldsymbol{Pr}[m_i|c] = \boldsymbol{Pr}[m_i] \Rightarrow \boldsymbol{Pr}[k_i] = \boldsymbol{Pr}[c] \Rightarrow \boldsymbol{Pr}[k_i] = 1/|\mathcal{K}|. \quad \square$$

One-time pad

Definition

Let $n \geq 1$ and integer and $\mathcal{M} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. For $k \in (\mathbb{Z}_2)^n$, let $Enc_k(m) = m \oplus k$ e $Dec_k(c) = c \oplus k$, with random choice of k.

Advantages:

- Perfect secrecy (shift cipher defined over $\mathbb{Z}_2$).
- Efficiency.

Disadvantages:

- $|\mathcal{K}| \geq |\mathcal{P}|$.
- Per-message random key.
- Vulnerable against known plaintext attacks.
- Complex key management.

Traditionally, cipher used only by military and diplomacy.