Cryptology

Sabyasachi Karati

Assistant Professor
Cryptology and Security Research Unit (C.S.R.U)
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute (ISI)
Kolkata, India

Lecture 03

One-Time Pad and Perfect Security

One-Time Pad

- In 1917, Vernam patented a cipher now called the one-time pad.

One-Time Pad

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^L$.
- $\mathcal{G} : k \xleftarrow{R} \mathcal{K}$
- $\mathcal{E} : c := m \oplus k$.
- $\mathcal{D} : m := c \oplus k$.

One-Time Pad

- In 1917, Vernam patented a cipher now called the one-time pad.

One-Time Pad

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^L$.
- $\mathcal{G} : k \xleftarrow{R} \mathcal{K}$
- $\mathcal{E} : c := m \oplus k$.
- $\mathcal{D} : m := c \oplus k$.

Correctness

$$\mathcal{D}(k, \mathcal{E}(k,m)) = \mathcal{D}(k, m \oplus k) = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0^L = m.$$

One-Time Pad

Example

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^8$.
- $k = 00101101$.
- **Plaintext:** $m = 01110111$

One-Time Pad

Example

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^8$.
- $k = 00101101$.
- **Plaintext:** $m = 01110111$
- $\mathcal{E} : c := m \oplus k$.

	m :	0	1	1	1	0	1	1	1
$\oplus$	k :	0	0	1	0	1	1	0	1
	c :	0	1	0	1	1	0	1	0

One-Time Pad

Example

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^8$.
- $k = 00101101$.
- **Plaintext:** $m = 01110111$
- $\mathcal{E} : c := m \oplus k$.

	m :	0	1	1	1	0	1	1	1
$\oplus$	k :	0	0	1	0	1	1	0	1
	c :	0	1	0	1	1	0	1	0

- $\mathcal{D} : m := c \oplus k$.

	c :	0	1	0	1	1	0	1	0
$\oplus$	k :	0	0	1	0	1	1	0	1
	m :	0	1	1	1	0	1	1	1

Variable length One-Time Pad

Variable length One-Time Pad

- $\mathcal{K} = \{0,1\}^L$.
- $\mathcal{M} = C = \cup_{1 \leqslant \ell \leqslant L} \{0,1\}^\ell$.
- $\mathcal{G} : k \xleftarrow{R} \mathcal{K}$.
- $\mathcal{E} : c := m \oplus k[0 \ldots \ell - 1]$, where $k[0 \ldots \ell - 1]$ means least significant ℓ bits of k.
- $\mathcal{D} : m := c \oplus k[0 \ldots \ell - 1]$.

Variable length One-Time Pad

Variable length One-Time Pad

- $\mathcal{K} = \{0,1\}^L$.
- $\mathcal{M} = \mathcal{C} = \cup_{1 \leqslant \ell \leqslant L} \{0,1\}^\ell$.
- $\mathcal{G} : k \xleftarrow{R} \mathcal{K}$.
- $\mathcal{E} : c := m \oplus k[0 \ldots \ell - 1]$, where $k[0 \ldots \ell - 1]$ means least significant ℓ bits of k.
- $\mathcal{D} : m := c \oplus k[0 \ldots \ell - 1]$.

Correctness

$$\begin{aligned} \mathcal{D}(k, \mathcal{E}(k,m)) &= \mathcal{D}(k, m \oplus k[0 \ldots \ell - 1]) = (m \oplus k[0 \ldots \ell - 1]) \oplus k[0 \ldots \ell - 1] \\ &= m \oplus (k[0 \ldots \ell - 1] \oplus k[0 \ldots \ell - 1]) = m \oplus 0^\ell \\ &= m. \end{aligned}$$

Variable length One-Time Pad

Example

- $\mathcal{K} = \{0,1\}^8$.
- $\mathcal{M} = \mathcal{C} = \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^8$.
- $k = 00101101$.
- **Plaintext:** $m = 110111$

Variable length One-Time Pad

Example

- $\mathcal{K} = \{0,1\}^8$.
- $\mathcal{M} = \mathcal{C} = \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^8$.
- $k = 00101101$.
- **Plaintext:** $m = 110111$
- $\mathcal{E} : c := m \oplus k[0 \ldots 5]$.

	m :	1	1	0	1	1	1
$\oplus$	$k[0 \ldots 5]$:	1	0	1	1	0	1
	c :	0	1	1	0	1	0

Variable length One-Time Pad

Example

- $\mathcal{K} = \{0,1\}^8$.
- $\mathcal{M} = \mathcal{C} = \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^8$.
- $k = 00101101$.
- **Plaintext:** $m = 110111$
- $\mathcal{E} : c := m \oplus k[0 \ldots 5]$.

	m :	1	1	0	1	1	1
$\oplus$	$k[0 \ldots 5]$:	1	0	1	1	0	1
	c :	0	1	1	0	1	0

- $\mathcal{D} : m := c \oplus k[0 \ldots 5]$.

	c :	0	1	1	0	1	0
$\oplus$	$k[0 \ldots 5]$:	1	0	1	1	0	1
	m :	1	1	0	1	1	1

Additive One-Time Pad

Additive One-Time Pad

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1, \ldots, n-1\}$.
- $\mathcal{G} : k \xleftarrow{R} \mathcal{K}$
- $\mathcal{E} : c := m + k \pmod{n}$.
- $\mathcal{D} : m := c - k \pmod{n}$.

Additive One-Time Pad

Additive One-Time Pad

- $\mathcal{M} = C = \mathcal{K} = \{0, 1, \ldots, n-1\}$.
- $\mathcal{G} : k \xleftarrow{R} \mathcal{K}$
- $\mathcal{E} : c := m + k \pmod{n}$.
- $\mathcal{D} : m := c - k \pmod{n}$.

Correctness

$$\begin{aligned} \mathcal{D}(k, \mathcal{E}(k, m)) &= \mathcal{D}(k, m + k \pmod{n}) = (m + k \pmod{n}) - k \pmod{n} \\ &= (m + (k - k)) \pmod{n} = m. \end{aligned}$$

Additive One-Time Pad

Example

- $n = 256$ and $\mathcal{M} = \mathcal{C} = \{0, 1, \ldots, 255\}$.
- $k = 55$.
- **Plaintext:** $m = 213$.

Additive One-Time Pad

Example

- $n = 256$ and $\mathcal{M} = \mathcal{C} = \{0, 1, \ldots, 255\}$.
- $k = 55$.
- **Plaintext:** $m = 213$.
- $\mathcal{E} : c := m + k \pmod{n} = 213 + 55 \pmod{256} = 12$.

Additive One-Time Pad

Example

- $n = 256$ and $\mathcal{M} = \mathcal{C} = \{0, 1, \ldots, 255\}$.
- $k = 55$.
- **Plaintext:** $m = 213$.
- $\mathcal{E} : c := m + k \pmod{n} = 213 + 55 \pmod{256} = 12$.
- $\mathcal{D} : m := c - k \pmod{n} = 12 - 55 \pmod{256} = 213$.

Perfect Security

Intuition: Case 1

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

Perfect Security

Intuition: Case 1

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

- Let $\Pr[m_0] = 0.5$ and $\Pr[m_1] = 0.5$.

Perfect Security

Intuition: Case 1

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

- Let $\Pr[m_0] = 0.5$ and $\Pr[m_1] = 0.5$.
- Let c be the ciphertext observed by the adversary.
- Can Adversary tell which message has been encrypted?

Perfect Security

Intuition: Case 1

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

- Let $\Pr[m_0] = 0.5$ and $\Pr[m_1] = 0.5$.
- Let c be the ciphertext observed by the adversary.
- Can Adversary tell which message has been encrypted?
  - There may exists a key k_0, such that $\mathcal{E}(k_0, m_0) = c$.
  - There may exists a key k_1, such that $\mathcal{E}(k_1, m_1) = c$.
  - Probabilities of k_0 and k_1 are the same.
  - Therefore, adversary can not tell with more than 0.5 probability.

Intuition: Case 2

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

Intuition: Case 2

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

- Let $\Pr[m_0] = 0.75$ and $\Pr[m_1] = 0.25$.
- Let the probability distributions of $\mathcal{M}$ and C be independent.

Intuition: Case 2

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

- Let $\Pr[m_0] = 0.75$ and $\Pr[m_1] = 0.25$.
- Let the probability distributions of $\mathcal{M}$ and C be independent.
- Does ciphertext adds any more information to the prior knowledge of plaintext?

Intuition: Case 2

- We have a large key space $\mathcal{K}$ and we choose a key k uniformly at random from $\mathcal{K}$.
- Suppose that we have two messages:

$$\begin{aligned} m_0 &: \quad \text{Attack at dawn, and} \\ m_1 &: \quad \text{Attack at dusk.} \end{aligned}$$

- Let $\Pr[m_0] = 0.75$ and $\Pr[m_1] = 0.25$.
- Let the probability distributions of $\mathcal{M}$ and C be independent.
- Does ciphertext adds any more information to the prior knowledge of plaintext?
  - No

Perfect Security

Notion

Just ciphertext must not add any new information to the prior knowledge of about message being encrypted.

Perfect Security

- In 1949, Shannon introduced the concept of perfect security after 32 years of Vernam.
- He also showed that one-time pad is perfectly secure.

Perfect Security

- In 1949, Shannon introduced the concept of perfect security after 32 years of Vernam.
- He also showed that one-time pad is perfectly secure.

Definition (Perfect Security)

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. If for all $m_0, m_1 \in \mathcal{M}$, and all $c \in C$, we have

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = \Pr[\mathcal{E}(\mathbf{k}, m_1) = c],$$

then we say that $\mathfrak{E}$ is a perfectly secure cipher.

Perfect Security

- Given c, adversary can not tell if m_0 has been encrypted or m_1.

Perfect Security

- Given c, adversary can not tell if m_0 has been encrypted or m_1.
- Most powerful adversary learns nothing about plaintext from ciphertext.

Perfect Security

- Given c, adversary can not tell if m_0 has been encrypted or m_1.
- Most powerful adversary learns nothing about plaintext from ciphertext.
- No Ciphertext-only attack possible. But other attacks are possible.

Perfect Security

Theorem 1

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. The following are equivalent:

1. $\mathfrak{E}$ is perfectly secure.
2. For every $c \in C$, there exists N_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have
$$| \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} | = N_c .$$
3. If the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$, then each of the random variables $\mathcal{E}(\mathbf{k}, m)$, for $m \in \mathcal{M}$, has the same distribution.

Perfect Security

Statement (3)

- Let $\mathcal{M} = \{m_0, m_1, m_2, \ldots\}$.
- Let $C = \{c_0, c_1, c_2, \ldots\}$.
- Let $\mathbf{k}$ be an uniformly distributed over $\mathcal{K}$ in key generation algorithm $\mathcal{G}$.

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_0] = \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_0] = \cdots = \Pr[\mathcal{E}(\mathbf{k}, m_i) = c_0] = \cdots = P_{c_0}$$
$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_1] = \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_1] = \cdots = \Pr[\mathcal{E}(\mathbf{k}, m_i) = c_1] = \cdots = P_{c_1}$$
$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_2] = \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_2] = \cdots = \Pr[\mathcal{E}(\mathbf{k}, m_i) = c_2] = \cdots = P_{c_2}$$
$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

Proof (Equivalence of (2) and (3))

(2) For every $c \in C$, there exists N_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have

$$| \{k \in \mathcal{K} : \mathcal{E}(k,m) = c\} | = N_c .$$

Proof (Equivalence of (2) and (3))

(2) For every $c \in \mathcal{C}$, there exists N_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have

$$| \{k \in \mathcal{K} : \mathcal{E}(k,m) = c\} | = N_c .$$

$\Leftrightarrow$ For every $c \in \mathcal{C}$, for all $m \in \mathcal{M}$, we have

$$\Pr[\mathcal{E}(\mathbf{k},m) = c] = \frac{| \{k \in \mathcal{K} : \mathcal{E}(k,m) = c\} |}{| \mathcal{K} |} = \frac{N_c}{| \mathcal{K} |},$$

where $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$ in key generation algorithm $\mathcal{G}$.

Proof (Equivalence of (2) and (3))

(2) For every $c \in \mathcal{C}$, there exists N_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have

$$|\{k \in \mathcal{K} : \mathcal{E}(k,m) = c\}| = N_c.$$

$\Leftrightarrow$ For every $c \in \mathcal{C}$, for all $m \in \mathcal{M}$, we have

$$\Pr[\mathcal{E}(\mathbf{k},m) = c] = \frac{|\{k \in \mathcal{K} : \mathcal{E}(k,m) = c\}|}{|\mathcal{K}|} = \frac{N_c}{|\mathcal{K}|},$$

where $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$ in key generation algorithm $\mathcal{G}$.

$\Leftrightarrow$ For every $c \in \mathcal{C}$, there exists P_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have

$$P_c = \Pr[\mathcal{E}(\mathbf{k},m) = c] \text{ where } P_c = \frac{N_c}{|\mathcal{K}|}.$$

Proof (Equivalence of (2) and (3))

(2) For every $c \in \mathcal{C}$, there exists N_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have

$$|\{k \in \mathcal{K} : \mathcal{E}(k,m) = c\}| = N_c.$$

$\Leftrightarrow$ For every $c \in \mathcal{C}$, for all $m \in \mathcal{M}$, we have

$$\Pr[\mathcal{E}(\mathbf{k},m) = c] = \frac{|\{k \in \mathcal{K} : \mathcal{E}(k,m) = c\}|}{|\mathcal{K}|} = \frac{N_c}{|\mathcal{K}|},$$

where $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$ in key generation algorithm $\mathcal{G}$.

$\Leftrightarrow$ For every $c \in \mathcal{C}$, there exists P_c (possibly depending on c) such that for all $m \in \mathcal{M}$, we have

$$P_c = \Pr[\mathcal{E}(\mathbf{k},m) = c] \text{ where } P_c = \frac{N_c}{|\mathcal{K}|}.$$

$\Leftrightarrow$ (3) If the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$, then each of the random variables $\Pr[\mathcal{E}(\mathbf{k},m)]$, for $m \in \mathcal{M}$, has the same distribution.

Perfect Security

Proof ((1)⇒ (2))

- Assuem that (1) is true.
- Let $c \in C$ be some fixed cipher.
- Select any arbitrary $m_0 \in \mathcal{M}$.
- Let $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c$.

Perfect Security

Proof ((1)⇒ (2))

- Assuem that (1) is true.
- Let $c \in C$ be some fixed cipher.
- Select any arbitrary $m_0 \in \mathcal{M}$.
- Let $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c$.
- Let $N_c = \mid \{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\} \mid$.
- $P_c = \dfrac{\mid \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} \mid}{\mid \mathcal{K} \mid} = \dfrac{N_c}{\mid \mathcal{K} \mid}$.

Perfect Security

Proof ((1)⇒ (2))

- Assuem that (1) is true.
- Let $c \in C$ be some fixed cipher.
- Select any arbitrary $m_0 \in \mathcal{M}$.
- Let $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c$.
- Let $N_c = \mid \{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\} \mid$.
- $P_c = \dfrac{\mid \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} \mid}{\mid \mathcal{K} \mid} = \dfrac{N_c}{\mid \mathcal{K} \mid}$.
- As $\mathfrak{E}$ has perfect security, for c

$$\forall m \in \mathcal{M}, \Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c.$$

Proof ((1)⇒ (2))

- Assuem that (1) is true.
- Let $c \in C$ be some fixed cipher.
- Select any arbitrary $m_0 \in \mathcal{M}$.
- Let $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c$.
- Let $N_c = \mid \{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\} \mid$.
- $P_c = \dfrac{\mid \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} \mid}{\mid \mathcal{K} \mid} = \dfrac{N_c}{\mid \mathcal{K} \mid}$.
- As $\mathfrak{E}$ has perfect security, for c

$$\forall m \in \mathcal{M}, \Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c.$$

- Therefore, there exists a constant N_c for $c \in C$ such that

$$\forall m \in \mathcal{M}, \mid \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} \mid = N_c.$$

Proof ((1)⇒ (2))

- Assuem that (1) is true.
- Let $c \in C$ be some fixed cipher.
- Select any arbitrary $m_0 \in \mathcal{M}$.
- Let $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c$.
- Let $N_c = \mid \{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\} \mid$.
- $P_c = \dfrac{\mid \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} \mid}{\mid \mathcal{K} \mid} = \dfrac{N_c}{\mid \mathcal{K} \mid}$.
- As $\mathfrak{E}$ has perfect security, for c

$$\forall m \in \mathcal{M}, \Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = P_c.$$

- Therefore, there exists a constant N_c for $c \in C$ such that

$$\forall m \in \mathcal{M}, \mid \{k \in \mathcal{K} : \mathcal{E}(k, m) = c\} \mid = N_c.$$

- This is true for all $c \in C$ and hence (2).

Perfect Security

Proof ((2) $\Rightarrow$ (1))

- Assuem that (2) is true.
- Let the keys be chosen at random from the keyspace $\mathcal{K}$.
- Let $m_0, m_1 \in \mathcal{M}$ be any two plaintexts.
- Select any arbitrary $c \in C$.

Perfect Security

Proof ((2) $\Rightarrow$ (1))

- Assuem that (2) is true.
- Let the keys be chosen at random from the keyspace $\mathcal{K}$.
- Let $m_0, m_1 \in \mathcal{M}$ be any two plaintexts.
- Select any arbitrary $c \in C$.
- By (2)

$$| \{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\} | \quad = N_c = \quad | \{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\} |$$

Perfect Security

Proof ((2) $\Rightarrow$ (1))

- Assuem that (2) is true.
- Let the keys be chosen at random from the keyspace $\mathcal{K}$.
- Let $m_0, m_1 \in \mathcal{M}$ be any two plaintexts.
- Select any arbitrary $c \in C$.
- By (2)

$$\begin{aligned} |\{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\}| &= N_c = |\{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\}| \\ \Leftrightarrow \frac{\{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\}|}{|\mathcal{K}|} &= \frac{N_c}{|\mathcal{K}|} = \frac{|\{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\}|}{|\mathcal{K}|} \end{aligned}$$

Proof ((2) ⇒ (1))

- Assuem that (2) is true.
- Let the keys be chosen at random from the keyspace $\mathcal{K}$.
- Let $m_0, m_1 \in \mathcal{M}$ be any two plaintexts.
- Select any arbitrary $c \in C$.
- By (2)

$$
\begin{aligned}
& |\{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\}| && = N_c = && |\{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\}| \\
\Leftrightarrow & \frac{\{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\}|}{|\mathcal{K}|} && = \frac{N_c}{|\mathcal{K}|} = && \frac{|\{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\}|}{|\mathcal{K}|} \\
& \Leftrightarrow \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] && = P_c = && \Pr[\mathcal{E}(\mathbf{k}, m_1) = c],
\end{aligned}
$$

where $\mathbf{k}$ be a random variable distributed over $\mathcal{K}$.

Proof ((2) ⇒ (1))

- Assuem that (2) is true.
- Let the keys be chosen at random from the keyspace $\mathcal{K}$.
- Let $m_0, m_1 \in \mathcal{M}$ be any two plaintexts.
- Select any arbitrary $c \in C$.
- By (2)

$$
\begin{aligned}
& |\{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\}| && = N_c = && |\{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\}| \\
\Leftrightarrow & \frac{\{k \in \mathcal{K} : \mathcal{E}(k, m_0) = c\}|}{|\mathcal{K}|} && = \frac{N_c}{|\mathcal{K}|} = && \frac{|\{k \in \mathcal{K} : \mathcal{E}(k, m_1) = c\}|}{|\mathcal{K}|} \\
& \Leftrightarrow \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] && = P_c = && \Pr[\mathcal{E}(\mathbf{k}, m_1) = c],
\end{aligned}
$$

  where $\mathbf{k}$ be a random variable distributed over $\mathcal{K}$.

- N_c is a constant ⇒ P_c is also a constant.
- Hence (1).

One-Time Pad and Perfect Security

Theorem 2

The one-time pad is a perfectly secure cipher.

One-Time Pad and Perfect Security

Theorem 2

The one-time pad is a perfectly secure cipher.

Proof

- Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^L$.

One-Time Pad and Perfect Security

Theorem 2

The one-time pad is a perfectly secure cipher.

Proof

- Let $\mathcal{M} = C = \mathcal{K} = \{0,1\}^L$.
- For any fixed message $m \in \mathcal{M}$ and any fixed ciphertext $c \in C$, there is a unique key k such that

$$\mathcal{E}(k,m) = c \Leftrightarrow k \oplus m = c \Rightarrow k = m \oplus c.$$

One-Time Pad and Perfect Security

Theorem 2

The one-time pad is a perfectly secure cipher.

Proof

- Let $\mathcal{M} = C = \mathcal{K} = \{0,1\}^L$.
- For any fixed message $m \in \mathcal{M}$ and any fixed ciphertext $c \in C$, there is a unique key k such that

$$\mathcal{E}(k,m) = c \Leftrightarrow k \oplus m = c \Rightarrow k = m \oplus c.$$

- Therefore, For every $c \in C$, all $m \in \mathcal{M}$, we have

$$N_c = 1.$$

One-Time Pad and Perfect Security

Theorem 2

The one-time pad is a perfectly secure cipher.

Proof

- Let $\mathcal{M} = C = \mathcal{K} = \{0,1\}^L$.
- For any fixed message $m \in \mathcal{M}$ and any fixed ciphertext $c \in C$, there is a unique key k such that
$$\mathcal{E}(k,m) = c \Leftrightarrow k \oplus m = c \Rightarrow k = m \oplus c.$$
- Therefore, For every $c \in C$, all $m \in \mathcal{M}$, we have
$$N_c = 1.$$
- Therefore, The one-time pad is a perfectly secure cipher.

Variable Length One-Time Pad and Perfect Security

Corollary

The variable length one-time pad is not perfectly secure.

Variable Length One-Time Pad and Perfect Security

Corollary

The variable length one-time pad is not perfectly secure.

Proof

- Let $\mathcal{K} = \{0,1\}^L$.
- $\mathcal{M} = C = \cup_{1 \leqslant \ell \leqslant L} \{0,1\}^\ell$.

Variable Length One-Time Pad and Perfect Security

Corollary

The variable length one-time pad is not perfectly secure.

Proof

- Let $\mathcal{K} = \{0,1\}^L$.
- $\mathcal{M} = C = \cup_{1 \leqslant \ell \leqslant L} \{0,1\}^\ell$.
- Let m_0 = a string of length 2.
- Let m_1 = a string of length 1.
- $k \xleftarrow{R} \mathcal{K}$.
- Let c = a string of length 1.

Variable Length One-Time Pad and Perfect Security

Corollary

The variable length one-time pad is not perfectly secure.

Proof

- Let $\mathcal{K} = \{0,1\}^L$.
- $\mathcal{M} = C = \cup_{1 \leqslant \ell \leqslant L} \{0,1\}^\ell$.
- Let m_0 = a string of length 2.
- Let m_1 = a string of length 1.
- $k \xleftarrow{R} \mathcal{K}$.
- Let c = a string of length 1.
- $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = 0$, and $\Pr[\mathcal{E}(\mathbf{k}, m_1) = c] = \frac{1}{2}$.

Variable Length One-Time Pad and Perfect Security

Corollary

The variable length one-time pad is not perfectly secure.

Proof

- Let $\mathcal{K} = \{0,1\}^L$.
- $\mathcal{M} = C = \cup_{1 \leqslant \ell \leqslant L} \{0,1\}^\ell$.
- Let m_0 = a string of length 2.
- Let m_1 = a string of length 1.
- $k \xleftarrow{R} \mathcal{K}$.
- Let c = a string of length 1.
- $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] = 0$, and $\Pr[\mathcal{E}(\mathbf{k}, m_1) = c] = \frac{1}{2}$.

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c].$$

- Hence proved

Is Substitute Cipher Perfectly Secure?

Is Substitute Cipher Perfectly Secure?

Corollary

Substitute cipher is not perfectly secure.

Is Substitute Cipher Perfectly Secure?

Corollary

Substitute cipher is not perfectly secure.

Proof

- Assume two messages: m_0 and m_1, such that
  - $m_0[0] = m_0[1]$ and $m_1[0] \neq m_1[1]$.
- Let the key be $\pi \xleftarrow{R} \Pi$.
- Let $c_0 := \mathcal{E}(\pi, m_0)$ and $c_1 := \mathcal{E}(\pi, m_1)$.

Is Substitute Cipher Perfectly Secure?

Corollary

Substitute cipher is not perfectly secure.

Proof

- Assume two messages: m_0 and m_1, such that
  - $m_0[0] = m_0[1]$ and $m_1[0] \neq m_1[1]$.
- Let the key be $\pi \xleftarrow{R} \Pi$.
- Let $c_0 := \mathcal{E}(\pi, m_0)$ and $c_1 := \mathcal{E}(\pi, m_1)$.
- As Substitute cipher is mono-alphabetic, for each key π:
  - $c_0[0] = c_0[1]$, and $c_1[0] \neq c_1[1]$.

Is Substitute Cipher Perfectly Secure?

Corollary

Substitute cipher is not perfectly secure.

Proof

- Assume two messages: m_0 and m_1, such that
  - $m_0[0] = m_0[1]$ and $m_1[0] \neq m_1[1]$.
- Let the key be $\pi \xleftarrow{R} \Pi$.
- Let $c_0 := \mathcal{E}(\pi, m_0)$ and $c_1 := \mathcal{E}(\pi, m_1)$.
- As Substitute cipher is mono-alphabetic, for each key π:
  - $c_0[0] = c_0[1]$, and $c_1[0] \neq c_1[1]$.
  - $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_0] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_0]$, and $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_1] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_1]$.

Is Substitute Cipher Perfectly Secure?

Corollary

Substitute cipher is not perfectly secure.

Proof

- Assume two messages: m_0 and m_1, such that
  - $m_0[0] = m_0[1]$ and $m_1[0] \neq m_1[1]$.
- Let the key be $\pi \xleftarrow{R} \Pi$.
- Let $c_0 := \mathcal{E}(\pi, m_0)$ and $c_1 := \mathcal{E}(\pi, m_1)$.
- As Substitute cipher is mono-alphabetic, for each key π:
  - $c_0[0] = c_0[1]$, and $c_1[0] \neq c_1[1]$.
  - $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_0] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_0]$, and $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c_1] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c_1]$.
- Therefore, the probability distributions of random variables $\mathcal{E}(\mathbf{k}, m_0)$ and $\mathcal{E}(\mathbf{k}, m_1)$ are different.
- Hence proved.

Perfect Security

Theorem 3

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In probabilistic algorithm $\mathcal{G}$, $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$. Then $\mathfrak{E}$ is perfectly secure if and only if for every predicate ϕ on C, for all $m_0, m_1 \in \mathcal{M}$, we have

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] = \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}].$$

Perfect Security

Theorem 3

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In probabilistic algorithm $\mathcal{G}$, $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$. Then $\mathfrak{E}$ is perfectly secure if and only if for every predicate ϕ on C, for all $m_0, m_1 \in \mathcal{M}$, we have

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] = \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}].$$

Proof

- Let $\mathfrak{E}$ be perfectly secure.
  - Take a predicate ϕ at random.
  - Choose two arbitrary messages $m_0, m_1 \in \mathcal{M}$.
  - Let $S := \{c \mid c \in C \text{ and } \phi(c) = \text{True}\}$.

Perfect Security

Theorem 3

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In probabilistic algorithm $\mathcal{G}$, $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$. Then $\mathfrak{E}$ is perfectly secure if and only if for every predicate ϕ on C, for all $m_0, m_1 \in \mathcal{M}$, we have

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] = \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}].$$

Proof

- Let $\mathfrak{E}$ be perfectly secure.
  - Take a predicate ϕ at random.
  - Choose two arbitrary messages $m_0, m_1 \in \mathcal{M}$.
  - Let $S := \{c \mid c \in C \text{ and } \phi(c) = \text{True}\}$.

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] \quad = \quad \sum_{c \in S} \Pr[\mathcal{E}(\mathbf{k}, m_0) = c]$$

Perfect Security

Theorem 3

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In probabilistic algorithm $\mathcal{G}$, $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$. Then $\mathfrak{E}$ is perfectly secure if and only if for every predicate ϕ on C, for all $m_0, m_1 \in \mathcal{M}$, we have

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] = \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}].$$

Proof

- Let $\mathfrak{E}$ be perfectly secure.
  - Take a predicate ϕ at random.
  - Choose two arbitrary messages $m_0, m_1 \in \mathcal{M}$.
  - Let $S := \{c \mid c \in C \text{ and } \phi(c) = \text{True}\}$.

$$\begin{aligned} \Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] &= \sum_{c \in S} \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \\ &= \sum_{c \in S} \Pr[\mathcal{E}(\mathbf{k}, m_1) = c], \quad [\text{ as } \mathfrak{E} \text{ is perfectly secure}] \end{aligned}$$

Perfect Security

Theorem 3

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In probabilistic algorithm $\mathcal{G}$, $\mathbf{k}$ is a random variable uniformly distributed over $\mathcal{K}$. Then $\mathfrak{E}$ is perfectly secure if and only if for every predicate ϕ on C, for all $m_0, m_1 \in \mathcal{M}$, we have

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] = \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}].$$

Proof

- Let $\mathfrak{E}$ be perfectly secure.
  - Take a predicate ϕ at random.
  - Choose two arbitrary messages $m_0, m_1 \in \mathcal{M}$.
  - Let $S := \{c \mid c \in C \text{ and } \phi(c) = \text{True}\}$.

$$\begin{aligned} \Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] &= \sum_{c \in S} \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \\ &= \sum_{c \in S} \Pr[\mathcal{E}(\mathbf{k}, m_1) = c], \quad [\text{ as } \mathfrak{E} \text{ is perfectly secure}] \\ &= \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}] \end{aligned}$$

- Hence proved.

Perfect Security

Proof (Other direction by Contrapositive)

- Assume that $\mathfrak{E}$ is not perfectly secure.
  - Then there exists two plaintexts $m_0, m_1 \in \mathcal{M}$ and a $c \in C$ such that

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c].$$

Perfect Security

Proof (Other direction by Contrapositive)

- Assume that $\mathfrak{E}$ is not perfectly secure.
  - Then there exists two plaintexts $m_0, m_1 \in \mathcal{M}$ and a $c \in C$ such that

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c].$$

  - Define predicate ϕ such that it is true only at c, otherwise false.

$$\Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] \quad = \quad \Pr[\mathcal{E}(\mathbf{k}, m_0) = c]$$

Perfect Security

Proof (Other direction by Contrapositive)

- Assume that $\mathfrak{E}$ is not perfectly secure.
  - Then there exists two plaintexts $m_0, m_1 \in \mathcal{M}$ and a $c \in C$ such that

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c].$$

  - Define predicate ϕ such that it is true only at c, otherwise false.

$$\begin{aligned} \Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] &= \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \\ &\neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c] \end{aligned}$$

Perfect Security

Proof (Other direction by Contrapositive)

- Assume that $\mathfrak{E}$ is not perfectly secure.
  - Then there exists two plaintexts $m_0, m_1 \in \mathcal{M}$ and a $c \in C$ such that

$$\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c].$$

  - Define predicate ϕ such that it is true only at c, otherwise false.

$$\begin{aligned} \Pr[\phi(\mathcal{E}(\mathbf{k}, m_0)) = \text{True}] &= \Pr[\mathcal{E}(\mathbf{k}, m_0) = c] \\ &\neq \Pr[\mathcal{E}(\mathbf{k}, m_1) = c] \\ &= \Pr[\phi(\mathcal{E}(\mathbf{k}, m_1)) = \text{True}]. \end{aligned}$$

- Hence proved.

Perfect Security

Theorem 4

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Consider a random experiment in which $\mathbf{k}$ and $\mathbf{m}$ are random variables, such that

- $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$,

Perfect Security

Theorem 4

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Consider a random experiment in which **k** and **m** are random variables, such that

- **k** is uniformly distributed over $\mathcal{K}$,
- **m** is distributed over $\mathcal{M}$, and

Perfect Security

Theorem 4

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Consider a random experiment in which $\mathbf{k}$ and $\mathbf{m}$ are random variables, such that

- $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$,
- $\mathbf{m}$ is distributed over $\mathcal{M}$, and
- $\mathbf{k}$ and $\mathbf{m}$ are independent.

Define the random variable $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. Then we have:

Perfect Security

Theorem 4

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Consider a random experiment in which $\mathbf{k}$ and $\mathbf{m}$ are random variables, such that

- $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$,
- $\mathbf{m}$ is distributed over $\mathcal{M}$, and
- $\mathbf{k}$ and $\mathbf{m}$ are independent.

Define the random variable $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. Then we have:

1. If $\mathfrak{E}$ is perfectly secure, then $\mathbf{c}$ and $\mathbf{m}$ are independent.
2. Conversely, if $\mathbf{c}$ and $\mathbf{m}$ are independent, and each message in $\mathcal{M}$ occurs with nonzero probability, then $\mathfrak{E}$ is perfectly secure.

Proof of (1)

- Let $\mathfrak{E}$ be perfectly secure.
- Choose a $c \in \mathcal{C}$ and $m \in \mathcal{M}$.
- To show **c** and **m** are independent, we have to prove

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

Perfect Security

Proof of (1)

- Let $\mathfrak{E}$ be perfectly secure.
- Choose a $c \in \mathcal{C}$ and $m \in \mathcal{M}$.
- To show $\mathbf{c}$ and $\mathbf{m}$ are independent, we have to prove

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

- We have

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] \quad = \quad \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$$

Perfect Security

Proof of (1)

- Let $\mathfrak{E}$ be perfectly secure.
- Choose a $c \in \mathcal{C}$ and $m \in \mathcal{M}$.
- To show $\mathbf{c}$ and $\mathbf{m}$ are independent, we have to prove

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

- We have

$$\begin{aligned} \Pr[\mathbf{c} = c \wedge \mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\ &= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{m} = m \end{aligned}$$

Perfect Security

Proof of (1)

- Let $\mathfrak{E}$ be perfectly secure.
- Choose a $c \in \mathcal{C}$ and $m \in \mathcal{M}$.
- To show $\mathbf{c}$ and $\mathbf{m}$ are independent, we have to prove

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

- We have

$$\begin{aligned}
\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{m} = m \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent}
\end{aligned}$$

Perfect Security

Proof of (1)

- Let $\mathfrak{E}$ be perfectly secure.
- Choose a $c \in \mathcal{C}$ and $m \in \mathcal{M}$.
- To show $\mathbf{c}$ and $\mathbf{m}$ are independent, we have to prove

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

- We have

$$\begin{aligned}
\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{m} = m \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent}
\end{aligned}$$

- Now we prove that $\Pr[\mathbf{c} = c] = \Pr[\mathcal{E}(\mathbf{k}, m)]$ to complete the proof.

Perfect Security

Proof of (1) cont.

$$\Pr[\mathbf{c} = c] \quad = \quad \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$$

Perfect Security

Proof of (1) cont.

$$\begin{aligned}\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\ &= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability}\end{aligned}$$

Perfect Security

Proof of (1) cont.

$$
\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c \wedge \mathbf{m} = m']
\end{aligned}
$$

Perfect Security

Proof of (1) cont.

$$
\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c \wedge \mathbf{m} = m'] \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c] \Pr[\mathbf{m} = m'], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent}
\end{aligned}
$$

Perfect Security

Proof of (1) cont.

$$
\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c \wedge \mathbf{m} = m'] \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c] \Pr[\mathbf{m} = m'], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m) = c] \Pr[\mathbf{m} = m'], \text{ as } \mathfrak{E} \text{ is perfectly secure}
\end{aligned}
$$

Perfect Security

Proof of (1) cont.

$$
\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c \wedge \mathbf{m} = m'] \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c] \Pr[\mathbf{m} = m'], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m) = c] \Pr[\mathbf{m} = m'], \text{ as } \mathfrak{E} \text{ is perfectly secure} \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c] \sum_{m' \in \mathcal{M}} \Pr[\mathbf{m} = m']
\end{aligned}
$$

Perfect Security

Proof of (1) cont.

$$
\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c \wedge \mathbf{m} = m'] \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c] \Pr[\mathbf{m} = m'], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m) = c] \Pr[\mathbf{m} = m'], \text{ as } \mathfrak{E} \text{ is perfectly secure} \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c] \sum_{m' \in \mathcal{M}} \Pr[\mathbf{m} = m'] \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c], \text{ as } \sum_{m' \in \mathcal{M}} \Pr[\mathbf{m} = m'] = 1 = \text{ sum of all probabilities.}
\end{aligned}
$$

Perfect Security

Proof of (1) cont.

$$
\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c], \text{ as } \mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m}) \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'], \text{ by total probability} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c \wedge \mathbf{m} = m'] \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m') = c] \Pr[\mathbf{m} = m'], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \sum_{m' \in \mathcal{M}} \Pr[\mathcal{E}(\mathbf{k}, m) = c] \Pr[\mathbf{m} = m'], \text{ as } \mathfrak{E} \text{ is perfectly secure} \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c] \sum_{m' \in \mathcal{M}} \Pr[\mathbf{m} = m'] \\
&= \Pr[\mathcal{E}(\mathbf{k}, m) = c], \text{ as } \sum_{m' \in \mathcal{M}} \Pr[\mathbf{m} = m'] = 1 = \text{ sum of all probabilities.}
\end{aligned}
$$

Now we have:

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathcal{E}(\mathbf{k}, m)] \Pr[\mathbf{m} = m] = \Pr[\mathbf{c} = c] \Pr[\mathbf{m} = m].$$

Perfect Security

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in \mathcal{C}$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in \mathcal{C}$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

to show that random variables $\mathcal{E}(\mathbf{k}, m)$, for all $m \in \mathcal{M}$ have same probability distribution (by the equivalence of (1) and (3) of Theorem 2).

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in \mathcal{C}$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

to show that random variables $\mathcal{E}(\mathbf{k}, m)$, for all $m \in \mathcal{M}$ have same probability distribution (by the equivalence of (1) and (3) of Theorem 2).

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m] \quad = \quad \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent}$$

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in C$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

to show that random variables $\mathcal{E}(\mathbf{k}, m)$, for all $m \in \mathcal{M}$ have same probability distribution (by the equivalence of (1) and (3) of Theorem 2).

$$\begin{aligned} \Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\ &= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m] \end{aligned}$$

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in C$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

to show that random variables $\mathcal{E}(\mathbf{k}, m)$, for all $m \in \mathcal{M}$ have same probability distribution (by the equivalence of (1) and (3) of Theorem 2).

$$\begin{aligned}
\Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m] \\
&= \Pr[\mathbf{c} = c \wedge \mathbf{m} = m]
\end{aligned}$$

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in C$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

to show that random variables $\mathcal{E}(\mathbf{k}, m)$, for all $m \in \mathcal{M}$ have same probability distribution (by the equivalence of (1) and (3) of Theorem 2).

$$\begin{aligned}
\Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m] \\
&= \Pr[\mathbf{c} = c \wedge \mathbf{m} = m] \\
&= \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m], \text{ as } \mathbf{c} \text{ and } \mathbf{m} \text{ are independent.}
\end{aligned}$$

Proof of (2)

- Let $m \in \mathcal{M}$ and $c \in C$.
- We have to show that

$$\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c],$$

to show that random variables $\mathcal{E}(\mathbf{k}, m)$, for all $m \in \mathcal{M}$ have same probability distribution (by the equivalence of (1) and (3) of Theorem 2).

$$\begin{aligned}
\Pr[\mathcal{E}(\mathbf{k}, m) = c]\Pr[\mathbf{m} = m] &= \Pr[\mathcal{E}(\mathbf{k}, m) = c \wedge \mathbf{m} = m], \text{ as } \mathbf{k} \text{ and } \mathbf{m} \text{ are independent} \\
&= \Pr[\mathcal{E}(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m] \\
&= \Pr[\mathbf{c} = c \wedge \mathbf{m} = m] \\
&= \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m], \text{ as } \mathbf{c} \text{ and } \mathbf{m} \text{ are independent.}
\end{aligned}$$

- As $\Pr[\mathbf{m} = m] \neq 0$, we have $\Pr[\mathcal{E}(\mathbf{k}, m) = c] = \Pr[\mathbf{c} = c]$.

Perfect Security

Alternate Definition (Perfect Security)

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

Perfect Security

Alternate Definition (Perfect Security)

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

Conceptual View

- A scheme is perfectly secure if the distributions over plaintexts and ciphertexts are independent.

Perfect Security

Equivalence of both the Definitions

- From First Definition to Alternate Definition:
  - Let $\mathfrak{E}$ is perfectly secure by First Definition.
  - In $\mathcal{G}$, let the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$.
  - Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$.
  - Let the random variables $\mathbf{k}$ and $\mathbf{m}$ be independent.
  - Let us define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$.

Equivalence of both the Definitions

- From First Definition to Alternate Definition:
  - Let $\mathfrak{E}$ is perfectly secure by First Definition.
  - In $\mathcal{G}$, let the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$.
  - Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$.
  - Let the random variables $\mathbf{k}$ and $\mathbf{m}$ be independent.
  - Let us define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$.
  - Therefore, by (1) of Theorem 4, we have $\mathbf{m}$ and $\mathbf{c}$ are independent, that is for all $m \in \mathcal{M}$ and $c \in C$:

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

Equivalence of both the Definitions

- From First Definition to Alternate Definition:
  - Let $\mathfrak{E}$ is perfectly secure by First Definition.
  - In $\mathcal{G}$, let the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$.
  - Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$.
  - Let the random variables $\mathbf{k}$ and $\mathbf{m}$ be independent.
  - Let us define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$.
  - Therefore, by (1) of Theorem 4, we have $\mathbf{m}$ and $\mathbf{c}$ are independent, that is for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$:

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

  - If $\Pr[\mathbf{c} = c] > 0$, we have

$$\Pr[\mathbf{m} = m] = \frac{\Pr[\mathbf{c} = c \wedge \mathbf{m} = m]}{\Pr[\mathbf{c} = c]}$$

Equivalence of both the Definitions

- From First Definition to Alternate Definition:
  - Let $\mathfrak{E}$ is perfectly secure by First Definition.
  - In $\mathcal{G}$, let the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$.
  - Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$.
  - Let the random variables $\mathbf{k}$ and $\mathbf{m}$ be independent.
  - Let us define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$.
  - Therefore, by (1) of Theorem 4, we have $\mathbf{m}$ and $\mathbf{c}$ are independent, that is for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$:

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

  - If $\Pr[\mathbf{c} = c] > 0$, we have

$$\Pr[\mathbf{m} = m] = \frac{\Pr[\mathbf{c} = c \wedge \mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]}$$

Equivalence of both the Definitions

- From First Definition to Alternate Definition:
  - Let $\mathfrak{E}$ is perfectly secure by First Definition.
  - In $\mathcal{G}$, let the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$.
  - Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$.
  - Let the random variables $\mathbf{k}$ and $\mathbf{m}$ be independent.
  - Let us define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$.
  - Therefore, by (1) of Theorem 4, we have $\mathbf{m}$ and $\mathbf{c}$ are independent, that is for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$:

$$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c]\Pr[\mathbf{m} = m].$$

  - If $\Pr[\mathbf{c} = c] > 0$, we have

$$\Pr[\mathbf{m} = m] = \frac{\Pr[\mathbf{c} = c \wedge \mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m \mid \mathbf{c} = c].$$

  - Hence Proved.

Equivalence of both the Definitions

- From Alternate Definition to First Definition:
  - Let $\mathfrak{E}$ be perfectly secure by Alternate Definition.
  - Then we have, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

Equivalence of both the Definitions

- From Alternate Definition to First Definition:
  - Let $\mathfrak{E}$ be perfectly secure by Alternate Definition.
  - Then we have, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

  - That is, in other words,

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m]$$

Equivalence of both the Definitions

- From Alternate Definition to First Definition:
  - Let $\mathfrak{E}$ be perfectly secure by Alternate Definition.
  - Then we have, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

  - That is, in other words,

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m]$$

$$\Leftrightarrow \quad \Pr[\mathbf{m} = m \wedge \mathbf{c} = c] = \Pr[\mathbf{m} = m]\Pr[\mathbf{c} = c]$$

Equivalence of both the Definitions

- From Alternate Definition to First Definition:
  - Let $\mathfrak{E}$ be perfectly secure by Alternate Definition.
  - Then we have, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

  - That is, in other words,

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m]$$

$$\Leftrightarrow \quad \Pr[\mathbf{m} = m \wedge \mathbf{c} = c] = \Pr[\mathbf{m} = m]\Pr[\mathbf{c} = c]$$

  - Therefore, random variables **c** and **m** are independent.

Equivalence of both the Definitions

- From Alternate Definition to First Definition:
  - Let $\mathfrak{E}$ be perfectly secure by Alternate Definition.
  - Then we have, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

  - That is, in other words,

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m]$$

$$\Leftrightarrow \quad \Pr[\mathbf{m} = m \wedge \mathbf{c} = c] = \Pr[\mathbf{m} = m]\Pr[\mathbf{c} = c]$$

  - Therefore, random variables **c** and **m** are independent.
  - By (2) of Theorem 4, each message in $\mathcal{M}$ occurs with nonzero probability, then $\mathfrak{E}$ is perfectly secure in First Definition.

Equivalence of both the Definitions

- From Alternate Definition to First Definition:
  - Let $\mathfrak{E}$ be perfectly secure by Alternate Definition.
  - Then we have, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m].$$

  - That is, in other words,

$$\Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \frac{\Pr[\mathbf{m} = m \wedge \mathbf{c} = c]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m]$$

$$\Leftrightarrow \quad \Pr[\mathbf{m} = m \wedge \mathbf{c} = c] = \Pr[\mathbf{m} = m]\Pr[\mathbf{c} = c]$$

  - Therefore, random variables **c** and **m** are independent.
  - By (2) of Theorem 4, each message in $\mathcal{M}$ occurs with nonzero probability, then $\mathfrak{E}$ is perfectly secure in First Definition.
  - Hence Proved.

Perfect Security

Lemma

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if and only if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c].$$

Perfect Security

Lemma

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if and only if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c].$$

Proof

- Arbitrarily choose $m \in \mathcal{M}$ and $c \in C$.

Perfect Security

Lemma

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if and only if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c].$$

Proof

- Arbitrarily choose $m \in \mathcal{M}$ and $c \in C$.
- We have,

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c]$$

Perfect Security

Lemma

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if and only if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c].$$

Proof

- Arbitrarily choose $m \in \mathcal{M}$ and $c \in C$.
- We have,

$$\begin{aligned} & \Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c] \\ \Leftrightarrow \quad & \Pr[\mathbf{c} = c \mid \mathbf{m} = m] \times \frac{\Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{c} = c] \times \frac{\Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]}, (\text{Let } \Pr[\mathbf{c} = c] > 0) \end{aligned}$$

Perfect Security

Lemma

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if and only if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c].$$

Proof

- Arbitrarily choose $m \in \mathcal{M}$ and $c \in C$.
- We have,

$$\begin{aligned}
& \Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c] \\
\Leftrightarrow \quad & \Pr[\mathbf{c} = c \mid \mathbf{m} = m] \times \frac{\Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{c} = c] \times \frac{\Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]}, (\text{Let } \Pr[\mathbf{c} = c] > 0) \\
\Leftrightarrow \quad & \frac{\Pr[\mathbf{c} = c \mid \mathbf{m} = m] \Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m]
\end{aligned}$$

Perfect Security

Lemma

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. In $\mathcal{G}$, the random variable $\mathbf{k}$ is uniformly distributed over $\mathcal{K}$. Let $\mathbf{m}$ be a random variable distributed over $\mathcal{M}$, and random variables $\mathbf{k}$ and $\mathbf{m}$ are independent. We define random variable $\mathbf{c}$ as $\mathbf{c} := \mathcal{E}(\mathbf{k}, \mathbf{m})$. We say $\mathfrak{E}$ is perfectly secure if and only if for every distribution of $\mathbf{m}$, for every plaintext $m \in \mathcal{M}$ and every ciphertext $c \in C$ with $\Pr[\mathbf{c} = c] > 0$:

$$\Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c].$$

Proof

- Arbitrarily choose $m \in \mathcal{M}$ and $c \in C$.
- We have,

$$\begin{aligned}
& \Pr[\mathbf{c} = c \mid \mathbf{m} = m] = \Pr[\mathbf{c} = c] \\
\Leftrightarrow \quad & \Pr[\mathbf{c} = c \mid \mathbf{m} = m] \times \frac{\Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{c} = c] \times \frac{\Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]}, (\text{Let } \Pr[\mathbf{c} = c] > 0) \\
\Leftrightarrow \quad & \frac{\Pr[\mathbf{c} = c \mid \mathbf{m} = m] \Pr[\mathbf{m} = m]}{\Pr[\mathbf{c} = c]} = \Pr[\mathbf{m} = m] \\
\Leftrightarrow \quad & \Pr[\mathbf{m} = m \mid \mathbf{c} = c] = \Pr[\mathbf{m} = m], (\text{By Bayes' Theorem}) \text{ Proved.}
\end{aligned}$$

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.
- Let $S := \{m \mid m := \mathcal{D}(k, c), \forall k \in \mathcal{K}\}$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.
- Let $S := \{m \mid m := \mathcal{D}(k, c), \forall k \in \mathcal{K}\}$.
- Now we have $|S| \leqslant |\mathcal{K}| < |\mathcal{M}|$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.
- Let $S := \{m \mid m := \mathcal{D}(k, c), \forall k \in \mathcal{K}\}$.
- Now we have $|S| \leqslant |\mathcal{K}| < |\mathcal{M}|$.
- Choose a plaintext m_1 such that $m_1 \in \mathcal{M} \setminus S$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.
- Let $S := \{m \mid m := \mathcal{D}(k, c), \forall k \in \mathcal{K}\}$.
- Now we have $|S| \leqslant |\mathcal{K}| < |\mathcal{M}|$.
- Choose a plaintext m_1 such that $m_1 \in \mathcal{M} \setminus S$.
- There do not exist a key $k' \in \mathcal{K}$ such that $\mathcal{D}(k', \mathcal{E}(m_1, k') = c) = m_1$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.
- Let $S := \{m \mid m := \mathcal{D}(k, c), \forall k \in \mathcal{K}\}$.
- Now we have $|S| \leqslant |\mathcal{K}| < |\mathcal{M}|$.
- Choose a plaintext m_1 such that $m_1 \in \mathcal{M} \setminus S$.
- There do not exist a key $k' \in \mathcal{K}$ such that $\mathcal{D}(k', \mathcal{E}(m_1, k') = c) = m_1$.
- Therefore, we have $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$ and $\Pr[\mathcal{E}(\mathbf{k}, m_1) = c] = 0$.

Bad News

Shannon's Theorem

Let $\mathfrak{E} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, C)$. If $\mathfrak{E}$ is perfectly secure, then $|\mathcal{K}| \geqslant |\mathcal{M}|$.

Proof

- Let $|\mathcal{K}| < |\mathcal{M}|$.
- Let $\mathbf{k}$ be a random variable, uniformly distributed over $\mathcal{K}$.
- Choose arbitrarily a message $m_0 \in \mathcal{M}$ and a key $k_0 \in \mathcal{K}$, and $c := \mathcal{E}(k_0, m_0)$.
- Therefore, $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$.
- Let $S := \{m \mid m := \mathcal{D}(k, c), \forall k \in \mathcal{K}\}$.
- Now we have $|S| \leqslant |\mathcal{K}| < |\mathcal{M}|$.
- Choose a plaintext m_1 such that $m_1 \in \mathcal{M} \setminus S$.
- There do not exist a key $k' \in \mathcal{K}$ such that $\mathcal{D}(k', \mathcal{E}(m_1, k') = c) = m_1$.
- Therefore, we have $\Pr[\mathcal{E}(\mathbf{k}, m_0) = c] > 0$ and $\Pr[\mathcal{E}(\mathbf{k}, m_1) = c] = 0$.
- Therefore, $\mathfrak{E}$ is not perfectly secure.

One-Time Pad and Perfect Security

Advantage

- One-Time Pad achieves perfect security.

One-Time Pad and Perfect Security

Advantage

- One-Time Pad achieves perfect security.

Disadvantage

- Key length must be equal to (or bigger than) the plaintext length.
- Before communicating the first bit of the ciphertext, key must be secretly shared or communicated.
- If we know such a method to share or communicate, we can use that to share or communicate the cipher.
- Impractical!!!

A Computational Approach

Conclusion

A **practical** system must not rely on the impossibility, but on the computational difficulty of breaking the system.

Conclusion

A **practical** system must not rely on the impossibility, but on the computational difficulty of breaking the system.

- Practical means more message bits than key bits.

A Computational Approach

Rather than

It is impossible to break the system.

A Computational Approach

Rather than

It is impossible to break the system.

We might say

No attack using less than 2^{64} time succeeds with probability more than 2^{-80}.

A Computational Approach

Rather than

It is impossible to break the system.

We might say

No attack using less than 2^{64} time succeeds with probability more than 2^{-80}.

- Cost of the attack can be Computational time, memory and so on.

A Computational Approach

Rather than

It is impossible to break the system.

We might say

No attack using less than 2^{64} time succeeds with probability more than 2^{-80}.

- Cost of the attack can be Computational time, memory and so on.

Mathematics and Computer Science

Cryptography is now not just mathematics; It needs Computer Science too.

A Computational Approach

Rather than

It is impossible to break the system.

We might say

No attack using less than 2^{64} time succeeds with probability more than 2^{-80}.

- Cost of the attack can be Computational time, memory and so on.

Mathematics and Computer Science

Cryptography is now not just mathematics; It needs Computer Science too.

- Computational Complexities,
- Algorithm Design,
- Efficient and Secure Software implementations and so on.

End