Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Here C is the random variable that results from sampling $m \leftarrow M$, $k \leftarrow \mathsf{Gen}$, and outputting $\mathsf{Enc}(k, m)$.

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{``}a\text{''}] = .7$ and $Pr[m = \text{``}z\text{''}] = .3$

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{``}a\text{''}] = .7$ and $Pr[m = \text{``}z\text{''}] = .3$

$$\Pr[m = \text{``}a\text{''} \mid C = b] = \frac{\Pr[C = b \mid m = \text{``}a\text{''}]\Pr[m = \text{``}a\text{''}]}{\Pr[C = b]}$$

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{“}a\text{''}] = .7$ and $Pr[m = \text{“}z\text{''}] = .3$

$$\begin{aligned}
\Pr[m = \text{“}a\text{''} \mid C = b] &= \frac{\Pr[C = b \mid m = \text{“}a\text{''}]\Pr[m = \text{“}a\text{''}]}{\Pr[C = b]} \\
&= \frac{\Pr[k = 1]\Pr[m = \text{“}a\text{''}]}{\Pr[C = b]}
\end{aligned}$$

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{“}a\text{''}] = .7$ and $Pr[m = \text{“}z\text{''}] = .3$

$$\begin{aligned}
\Pr[m = \text{“}a\text{''} \mid C = b] &= \frac{\Pr[C = b \mid m = \text{“}a\text{''}]\Pr[m = \text{“}a\text{''}]}{\Pr[C = b]} \\
&= \frac{\Pr[k = 1]\Pr[m = \text{“}a\text{''}]}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\Pr[C = b]}
\end{aligned}$$

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{``}a\text{''}] = .7$ and $Pr[m = \text{``}z\text{''}] = .3$

$$
\begin{aligned}
\Pr[m = \text{``}a\text{''} \mid C = b] &= \frac{\Pr[C = b \mid m = \text{``}a\text{''}] \Pr[m = \text{``}a\text{''}]}{\Pr[C = b]} \\
&= \frac{\Pr[k = 1] \Pr[m = \text{``}a\text{''}]}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\sum_{m' \in \mathcal{M}} \Pr[C = b \mid m = m'] \Pr[m = m']}
\end{aligned}
$$

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{“}a\text{''}] = .7$ and $Pr[m = \text{“}z\text{''}] = .3$

$$
\begin{aligned}
\Pr[m = \text{“}a\text{''} \mid C = b] &= \frac{\Pr[C = b \mid m = \text{“}a\text{''}]\Pr[m = \text{“}a\text{''}]}{\Pr[C = b]} \\
&= \frac{\Pr[k = 1]\Pr[m = \text{“}a\text{''}]}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\sum_{m' \in \mathcal{M}} \Pr[C = b \mid m = m']\Pr[m = m']} \\
&= \frac{(\frac{1}{26})(.7)}{\Pr[C = b \mid m = \text{“}a\text{''}](.7) + \Pr[C = b \mid m = \text{“}z\text{''}](.3)}
\end{aligned}
$$

Perfect Secrecy

Definition

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Consider the Caesar Cipher, with messages that are at most 1 character long.
Consider the following message distribution, $\mathcal{M}$:
$Pr[m = \text{``}a\text{''}] = .7$ and $Pr[m = \text{``}z\text{''}] = .3$

$$\begin{aligned}
\Pr[m = \text{``}a\text{''} \mid C = b] &= \frac{\Pr[C = b \mid m = \text{``}a\text{''}] \Pr[m = \text{``}a\text{''}]}{\Pr[C = b]} \\
&= \frac{\Pr[k = 1] \Pr[m = \text{``}a\text{''}]}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\Pr[C = b]} \\
&= \frac{(\frac{1}{26})(.7)}{\sum_{m' \in \mathcal{M}} \Pr[C = b \mid m = m'] \Pr[m = m']} \\
&= \frac{(\frac{1}{26})(.7)}{\Pr[C = b \mid m = \text{``}a\text{''}](.7) + \Pr[C = b \mid m = \text{``}z\text{''}](.3)} \\
&= \frac{(\frac{1}{26})(.7)}{\frac{1}{26}(.7) + \frac{1}{26}(.3)} = \frac{.7}{.7 + .3} = .7
\end{aligned}$$

One Time Pad

Message space $\mathcal{M}$: $\{\mathrm{a}, \ldots, \mathrm{z}\}^\ell$
Keyspace $\mathcal{K}$: $\{0, \ldots, 25\}^\ell$
Ciphertext space $\mathcal{C}$: $\{\mathrm{a}, \ldots, \mathrm{z}\}^\ell$

One Time Pad

Message space $\mathcal{M}$: $\{\mathrm{a}, \ldots, \mathrm{z}\}^\ell$
Keyspace $\mathcal{K}$: $\{0, \ldots, 25\}^\ell$
Ciphertext space $\mathcal{C}$: $\{\mathrm{a}, \ldots, \mathrm{z}\}^\ell$

Gen : $k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
Enc(k, m) : $c_i = m_i + k_i \mod 26$
Dec(k, c) : $m_i = c_i - k_i \mod 26$

One Time Pad

Message space $\mathcal{M}$: $\{\mathrm{a}, \ldots, \mathrm{z}\}^\ell$
Keyspace $\mathcal{K}$: $\{0, \ldots, 25\}^\ell$
Ciphertext space $\mathcal{C}$: $\{\mathrm{a}, \ldots, \mathrm{z}\}^\ell$

Gen : $k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
Enc(k, m) : $c_i = m_i + k_i \mod 26$
Dec(k, c) : $m_i = c_i - k_i \mod 26$

Consider the following message distribution, M:

$$\Pr_{m \leftarrow M}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow M}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow M}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

Prove that:

$$\Pr[m = \text{“kim”} \mid c = \text{“DQQ”}] = \Pr[m = \text{“kim”}]$$
$$\Pr[m = \text{“ann”} \mid c = \text{“DQQ”}] = \Pr[m = \text{“ann”}]$$
$$\Pr[m = \text{“boo”} \mid c = \text{“DQQ”}] = \Pr[m = \text{“boo”}]$$

One Time Pad

Usually we use Binary strings instead of the alphabet $\{a, \ldots, z\}$.
Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

$\text{Gen} : k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\text{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\text{Dec}(k, c) : m_i = c_i + k_i \mod 2$

Example, for $\ell = 3$:
$k = 101$
$\text{Enc}(k, 111) = 010$

One Time Pad

Usually we use Binary strings instead of the alphabet $\{a, \ldots, z\}$.
Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

$\text{Gen} : k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\text{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\text{Dec}(k, c) : m_i = c_i + k_i \mod 2$

Example, for $\ell = 3$:
$k = 101$
$\text{Enc}(k, 111) = 010$

$$
\begin{aligned}
\Pr[c = 010] = {} & \Pr[c = 010 \mid m = 000] \Pr[m = 000] \\
& + \Pr[c = 010 \mid m = 001] \Pr[m = 001] \\
& + \Pr[c = 010 \mid m = 010] \Pr[m = 010] \\
& + \Pr[c = 010 \mid m = 011] \Pr[m = 011] \\
& + \Pr[c = 010 \mid m = 100] \Pr[m = 100] \\
& + \Pr[c = 010 \mid m = 101] \Pr[m = 101] \\
& + \Pr[c = 010 \mid m = 110] \Pr[m = 110] \\
& + \Pr[c = 010 \mid m = 111] \Pr[m = 111]
\end{aligned}
$$

One Time Pad

Usually we use Binary strings instead of the alphabet $\{a, \ldots, z\}$.
Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

$\text{Gen} : k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\text{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\text{Dec}(k, c) : m_i = c_i + k_i \mod 2$

Example, for $\ell = 3$:
$k = 101$
$\text{Enc}(k, 111) = 010$

$$\begin{aligned}
\Pr[c = 010] = {} & \Pr[c = 010 \mid m = 000] \Pr[m = 000] = (1/8) \Pr[m = 000] \\
& + \Pr[c = 010 \mid m = 001] \Pr[m = 001] = (1/8) \Pr[m = 001] \\
& + \Pr[c = 010 \mid m = 010] \Pr[m = 010] = (1/8) \Pr[m = 010] \\
& + \Pr[c = 010 \mid m = 011] \Pr[m = 011] = (1/8) \Pr[m = 011] \\
& + \Pr[c = 010 \mid m = 100] \Pr[m = 100] = (1/8) \Pr[m = 100] \\
& + \Pr[c = 010 \mid m = 101] \Pr[m = 101] = (1/8) \Pr[m = 101] \\
& + \Pr[c = 010 \mid m = 110] \Pr[m = 110] = (1/8) \Pr[m = 110] \\
& + \Pr[c = 010 \mid m = 111] \Pr[m = 111] = (1/8) \Pr[m = 111]
\end{aligned}$$

One Time Pad

Usually we use Binary strings instead of the alphabet $\{a, \ldots, z\}$.
Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

$\mathsf{Gen} : k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\mathsf{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\mathsf{Dec}(k, c) : m_i = c_i + k_i \mod 2$

Example, for $\ell = 3$:
$k = 101$
$\mathsf{Enc}(k, 111) = 010$

$$
\begin{aligned}
\Pr[c = 010] = {} & \Pr[c = 010 \mid m = 000]\Pr[m = 000] = (1/8)\Pr[m = 000] \\
& + \Pr[c = 010 \mid m = 001]\Pr[m = 001] = (1/8)\Pr[m = 001] \\
& + \Pr[c = 010 \mid m = 010]\Pr[m = 010] = (1/8)\Pr[m = 010] \\
& + \Pr[c = 010 \mid m = 011]\Pr[m = 011] = (1/8)\Pr[m = 011] \\
& + \Pr[c = 010 \mid m = 100]\Pr[m = 100] = (1/8)\Pr[m = 100] \\
& + \Pr[c = 010 \mid m = 101]\Pr[m = 101] = (1/8)\Pr[m = 101] \\
& + \Pr[c = 010 \mid m = 110]\Pr[m = 110] = (1/8)\Pr[m = 110] \\
& + \Pr[c = 010 \mid m = 111]\Pr[m = 111] = (1/8)\Pr[m = 111] \\
= {} & 1/8
\end{aligned}
$$

One Time Pad

Usually we use Binary strings instead of the alphabet $\{a, \dots, z\}$.
Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

Gen : $k = k_1 \dots k_\ell \leftarrow \mathcal{K}$
Enc(k, m) : $c_i = m_i + k_i \mod 2$
Dec(k, c) : $m_i = c_i + k_i \mod 2$

Example, for $\ell = 3$:
$k = 101$
$\text{Enc}(k, 111) = 010$

$$\Pr[c = 010] = \frac{1}{8} = \Pr[c = 010 \mid M = m]$$

One Time Pad

Usually we use Binary strings instead of the alphabet $\{a, \dots, z\}$.
Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

Gen : $k = k_1 \dots k_\ell \leftarrow \mathcal{K}$
Enc(k, m) : $c_i = m_i + k_i \mod 2$
Dec(k, c) : $m_i = c_i + k_i \mod 2$

Example, for $\ell = 3$:
$k = 101$
Enc$(k, 111) = 010$

$$\Pr[c = 010] = \frac{1}{8} = \Pr[c = 010 \mid M = m]$$

$$\begin{aligned}\Pr[M = m \mid C = c] &= \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]} \\ &= \frac{\frac{1}{8} \Pr[M = m]}{\frac{1}{8}} \\ &= \Pr[M = m]\end{aligned}$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.
$\Pr[Enc_k(m_1) = c] = \Pr[C = c \mid M = m_1]$,

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.
$\Pr[Enc_k(m_1) = c] = \Pr[C = c \mid M = m_1]$, so, our assumption says that:
$\forall m_1, m_2 \in \mathcal{M}, \Pr[C = c \mid M = m_1] = \Pr[C = c \mid M = m_2] = \delta$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.
$\Pr[Enc_k(m_1) = c] = \Pr[C = c \mid M = m_1]$, so, our assumption says that:
$\forall m_1, m_2 \in \mathcal{M}, \Pr[C = c \mid M = m_1] = \Pr[C = c \mid M = m_2] = \delta$

$$\Pr[M = m \mid C = c] = \Pr[C = c \mid M = m] \Pr[M = m] / \Pr[C = c]$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.
$\Pr[Enc_k(m_1) = c] = \Pr[C = c \mid M = m_1]$, so, our assumption says that:
$\forall m_1, m_2 \in \mathcal{M}, \Pr[C = c \mid M = m_1] = \Pr[C = c \mid M = m_2] = \delta$

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

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.
$\Pr[Enc_k(m_1) = c] = \Pr[C = c \mid M = m_1]$, so, our assumption says that:
$\forall m_1, m_2 \in \mathcal{M}, \Pr[C = c \mid M = m_1] = \Pr[C = c \mid M = m_2] = \delta$

$$\begin{aligned}
\Pr[M = m \mid C = c] &= \Pr[C = c \mid M = m] \Pr[M = m] / \Pr[C = c] \\
&= \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \Pr[M = m']} \\
&= \frac{\delta \Pr[M = m]}{\delta \sum_{m' \in \mathcal{M}} \Pr[M = m']}
\end{aligned}$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 2.
$\Pr[Enc_k(m_1) = c] = \Pr[C = c \mid M = m_1]$, so, our assumption says that:
$\forall m_1, m_2 \in \mathcal{M}, \Pr[C = c \mid M = m_1] = \Pr[C = c \mid M = m_2] = \delta$

$$
\begin{aligned}
\Pr[M = m \mid C = c] &= \Pr[C = c \mid M = m] \Pr[M = m] / \Pr[C = c] \\
&= \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \Pr[M = m']} \\
&= \frac{\delta \Pr[M = m]}{\delta \sum_{m' \in \mathcal{M}} \Pr[M = m']} \\
&= \Pr[M = m]
\end{aligned}
$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 1.

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 1.
$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \forall M \text{ over } \mathcal{M}$,
$\Pr[M = m \mid C = c] = \Pr[M = m]$.

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 1.
$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \forall M \text{ over } \mathcal{M},$
$\Pr[M = m \mid C = c] = \Pr[M = m]$.

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]} = \Pr[M = m]$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 1.
$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \forall M \text{ over } \mathcal{M},$
$\Pr[M = m \mid C = c] = \Pr[M = m]$.

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]} = \Pr[M = m]$$

$$\Rightarrow \frac{\Pr[C = c \mid M = m]}{\Pr[C = c]} = 1$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 1.
$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \forall M \text{ over } \mathcal{M},$
$\Pr[M = m \mid C = c] = \Pr[M = m]$.

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]} = \Pr[M = m]$$
$$\Rightarrow \frac{\Pr[C = c \mid M = m]}{\Pr[C = c]} = 1$$
$$\Rightarrow \Pr[C = c \mid M = m] = \Pr[C = c]$$

Perfect Secrecy, another way

Definition 1

An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[\mathcal{C} = c] > 0$: $\Pr[M = m \mid C = c] = \Pr[M = m]$.

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Suppose $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ satisfy Definition 1.
$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \forall M \text{ over } \mathcal{M},$
$\Pr[M = m \mid C = c] = \Pr[M = m]$.

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \Pr[M = m]}{\Pr[C = c]} = \Pr[M = m]$$

$$\Rightarrow \frac{\Pr[C = c \mid M = m]}{\Pr[C = c]} = 1$$

$$\Rightarrow \Pr[C = c \mid M = m] = \Pr[C = c]$$

$$\Rightarrow \forall m_1, m_2 \in \mathcal{M}, \forall c \in \mathcal{C}, \Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[\mathrm{Enc}(k, m_2) = c]$$

One Time Pad: Second Proof

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

Gen : $k = k_1 \dots k_\ell \leftarrow \mathcal{K}$
$\mathrm{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\mathrm{Dec}(k, c) : m_i = c_i + k_i \mod 2$

One Time Pad: Second Proof

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\text{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

Gen : $k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\text{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\text{Dec}(k, c) : m_i = c_i + k_i \mod 2$

Claim: $\forall m_1, m_2 \in \mathcal{M}, \forall c \in C$,
$\Pr[\text{Enc}(k, m_1) = c] = \Pr[\text{Enc}(k, m_2) = c]$

One Time Pad: Second Proof

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\text{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

Message space $\mathcal{M}$: $\{0,1\}^\ell$
Keyspace $\mathcal{K}$: $\{0,1\}^\ell$
Ciphertext space $\mathcal{C}$: $\{0,1\}^\ell$

Gen : $k = k_1 \ldots k_\ell \leftarrow \mathcal{K}$
$\text{Enc}(k, m) : c_i = m_i + k_i \mod 2$
$\text{Dec}(k, c) : m_i = c_i + k_i \mod 2$

<u>Claim:</u> $\forall m_1, m_2 \in \mathcal{M}, \forall c \in C$,
$\Pr[\text{Enc}(k, m_1) = c] = \Pr[\text{Enc}(k, m_2) = c]$

Proof: $\forall m \in \mathcal{M}, \Pr[\text{Enc}(k, m) = c] = \Pr[k \oplus m = c] = \Pr[k = m \oplus c] = 2^{-\ell}$

A simple security game

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

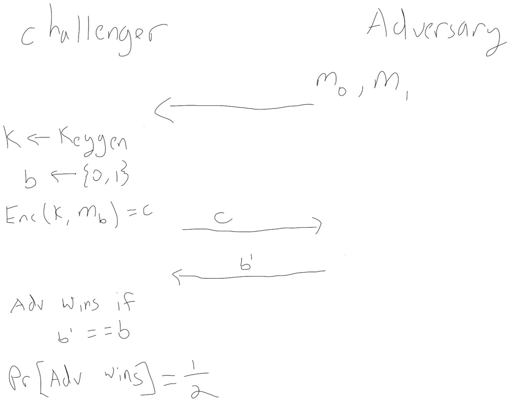
A nice property of this definition is that we don't have to worry about the message distribution.

A simple security game

Definition 2

For every $m_1, m_2 \in \mathcal{M}$, and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}(k, m_1) = c] = \Pr[Enc_k(m_2) = c]$.

A nice property of this definition is that we don't have to worry about the message distribution.



Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!
- You have to know an upper bound on the number of messages you intend to send to the recipient. If you run out of key material, you would have to exchange another key.

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!
- You have to know an upper bound on the number of messages you intend to send to the recipient. If you run out of key material, you would have to exchange another key.

Unfortunately, this problem is inherent for perfect secrecy:

Claim: If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!
- You have to know an upper bound on the number of messages you intend to send to the recipient. If you run out of key material, you would have to exchange another key.

Unfortunately, this problem is inherent for perfect secrecy:

Claim: If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof: Define $M(c) = \{m \mid m = \mathsf{Dec}(k, c) \text{ for some } k \in \mathcal{K}\}$
(Intuitively, $M(c)$ is the set of messages that you *could* decrypt c to.)

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!
- You have to know an upper bound on the number of messages you intend to send to the recipient. If you run out of key material, you would have to exchange another key.

Unfortunately, this problem is inherent for perfect secrecy:

Claim: If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof: Define $M(c) = \{m \mid m = \mathsf{Dec}(k, c) \text{ for some } k \in \mathcal{K}\}$
(Intuitively, $M(c)$ is the set of messages that you *could* decrypt c to.)

$|M(c)| \leq |\mathcal{K}|$, since each key in $\mathcal{K}$ yields a single plaintext when decrypting c.

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!
- You have to know an upper bound on the number of messages you intend to send to the recipient. If you run out of key material, you would have to exchange another key.

Unfortunately, this problem is inherent for perfect secrecy:

Claim: If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof: Define $M(c) = \{m \mid m = \mathsf{Dec}(k, c) \text{ for some } k \in \mathcal{K}\}$
(Intuitively, $M(c)$ is the set of messages that you *could* decrypt c to.)

$|M(c)| \leq |\mathcal{K}|$, since each key in $\mathcal{K}$ yields a single plaintext when decrypting c. Suppose $|\mathcal{K}| < |\mathcal{M}|$. Then $|M(c)| < |\mathcal{K}| < |\mathcal{M}|$, so there exists some $m^* \in \mathcal{M}$ such that $m^* \notin M(c)$.

Key Length

If the one time pad is perfectly secret, why use any other encryption scheme?

- The key length is as long as the message!
- Imagine encrypting a 4GB hard drive. You would need a 2nd 4GB hard drive!
- You have to know an upper bound on the number of messages you intend to send to the recipient. If you run out of key material, you would have to exchange another key.

Unfortunately, this problem is inherent for perfect secrecy:

Claim: If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof: Define $M(c) = \{m \mid m = \mathsf{Dec}(k, c) \text{ for some } k \in \mathcal{K}\}$
(Intuitively, $M(c)$ is the set of messages that you *could* decrypt c to.)

$|M(c)| \leq |\mathcal{K}|$, since each key in $\mathcal{K}$ yields a single plaintext when decrypting c. Suppose $|\mathcal{K}| < |\mathcal{M}|$. Then $|M(c)| < |\mathcal{K}| < |\mathcal{M}|$, so there exists some $m^* \in \mathcal{M}$ such that $m^* \notin M(c)$.

Let M be the uniform distribution over $\mathcal{M}$.
$\Pr[M = m^*] = \frac{1}{|\mathcal{M}|}$.
$\Pr[M = m^* \mid C = c] = 0$

Reuse One Time Pad

What happens if we reuse the key in the OTP?

$c_1 = \text{Enc}(k, m_1) = k \oplus m_1$

$c_2 = \text{Enc}(k, m_2) = k \oplus m_2$

Reuse One Time Pad

What happens if we reuse the key in the OTP?
$c_1 = \text{Enc}(k, m_1) = k \oplus m_1$
$c_2 = \text{Enc}(k, m_2) = k \oplus m_2$

$c_1 \oplus c_2 = m_1 \oplus m_2$.

Reuse One Time Pad

What happens if we reuse the key in the OTP?
$c_1 = \text{Enc}(k, m_1) = k \oplus m_1$
$c_2 = \text{Enc}(k, m_2) = k \oplus m_2$

$c_1 \oplus c_2 = m_1 \oplus m_2$.

This reveals a lot about the messages!
It tells us exactly where they match and where they don't.

Reuse One Time Pad

What happens if we reuse the key in the OTP?
$c_1 = \text{Enc}(k, m_1) = k \oplus m_1$
$c_2 = \text{Enc}(k, m_2) = k \oplus m_2$

$c_1 \oplus c_2 = m_1 \oplus m_2$.

This reveals a lot about the messages!
It tells us exactly where they match and where they don't.

Even worse, suppose we know that c_1 encrypts m_1.
We can completely recover the key k: $k = c_1 \oplus m_1$.
Then we can decrypt c_2 precisely.

Reuse One Time Pad

What happens if we reuse the key in the OTP?
$c_1 = \text{Enc}(k, m_1) = k \oplus m_1$
$c_2 = \text{Enc}(k, m_2) = k \oplus m_2$

$c_1 \oplus c_2 = m_1 \oplus m_2$.

This reveals a lot about the messages!
It tells us exactly where they match and where they don't.

Even worse, suppose we know that c_1 encrypts m_1.
We can completely recover the key k: $k = c_1 \oplus m_1$.
Then we can decrypt c_2 precisely.
This is called a *Known Plaintext Attack.* We'd like to protect against this.