# Cryptography

Lecture 3: Indistinguishability & Limits of Perfect Secrecy

October 30, 2026



## Perfectly Secret Encryption

Notes

- Use consistent variable naming (messages, keys, ciphertext)
- Drop distribution marker — write $\mathrm{P}(m)$ instead of $\mathrm{P}_{\mathcal{M}}(m)$
- Utilize usual probability notation — $\mathrm{P}(m, c)$ for joint probability
- Assume message & key selection is independent

$$\mathrm{P}(k, m) = \mathrm{P}(k) \cdot \mathrm{P}(m)$$

- Then

$$\mathrm{P}(c) = \sum_{k \in K, m \in \mathcal{M}} \mathrm{P}(k, m) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

and in perfectly secret encryption scheme $\mathcal{E}$ for any message $m' \in \mathcal{M}$

$$\mathrm{P}(c) = O_{\mathcal{E}}(c, m') = \sum_{k \in K} \mathrm{P}(k) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m')\big]$$



## Perfectly Secret Encryption

**§2.7 Lemma**

Encryption scheme $\mathcal{E}$ is perfectly secret if and only if
in every scenario $(\mathcal{E}, \mathrm{P}_{\mathcal{M}})$ we have $\mathrm{P}(m \mid c) = \mathrm{P}(m)$
for all messages $m \in \mathcal{M}$ and possible ciphertexts $c \in C$ with $\mathrm{P}(c) \neq 0$

**Proof (1/2)**

($\rightarrow$) Let $\mathrm{P}_{\mathcal{M}} \colon \mathcal{M} \to [0,1]$, $m, m' \in \mathcal{M}$, and $c \in C$ with $\mathrm{P}(c) \neq 0$

$$\mathrm{P}(m \mid c) = \frac{\mathrm{P}(m, c)}{\mathrm{P}(c)} = \frac{\overbrace{\sum_{k \in K} \mathrm{P}(k) \cdot \mathrm{P}(m) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]}^{=\mathrm{P}(m,c)}}{\underbrace{O_{\mathcal{E}}(c, m')}_{=\mathrm{P}(c)}}$$

$$= \mathrm{P}(m) \cdot \frac{\sum_{k \in K} \mathrm{P}(k) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]}{O_{\mathcal{E}}(c, m')} = \mathrm{P}(m) \cdot \frac{\cancel{O_{\mathcal{E}}(c, m)}}{\cancel{O_{\mathcal{E}}(c, m')}}$$



## Perfectly Secret Encryption

**Proof (2/2)**

($\leftarrow$) Let $c \in C$ and $m, m' \in \mathcal{M}$. Consider distribution $\mathrm{P}_{\mathcal{M}} \colon \mathcal{M} \to [0,1]$ such that $\mathrm{P}_{\mathcal{M}}(m) = \mathrm{P}_{\mathcal{M}}(m') = \frac{1}{2}$ and $\mathrm{P}_{\mathcal{M}}(m'') = 0$ otherwise. First suppose that $\mathrm{P}(c) = 0$. Then

$$\mathrm{P}(k) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] = 0 = \mathrm{P}(k) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m')\big]$$

for all $k \in K$. Hence $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ as required.

Otherwise $\mathrm{P}(c) \neq 0$ and we prove that $\mathrm{P}(c) = O_{\mathcal{E}}(c, m'')$ for all $m'' \in \{m, m'\}$, which also proves $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$

$$\mathrm{P}(c) = \frac{\mathrm{P}(m'', c)}{\mathrm{P}(m'' \mid c)} = \frac{\sum_{k \in K} \mathrm{P}(k) \cdot \cancel{\mathrm{P}(m'')} \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m'')\big]}{\cancel{\mathrm{P}(m'')}} = O_{\mathcal{E}}(c, m'')$$

□

## One-Time Pad

**§2.8 Example (One-time pad; Vernam 1917)**

Let $\ell \in \mathbb{N}$ and $K = M = C = \{0,1\}^\ell$. Lenght $\ell$ one-time pad is given by

- Key generation $\mathsf{P}_K(k) = 2^{-\ell}$ for all $k \in K = \{0,1\}^\ell$
  (uniform selection from key space of all keys of length $\ell$)
- Encryption enc: $K \times M \to C$ with $K = M = C = \{0,1\}^\ell$

$$\mathrm{enc}_k(m_1, \ldots, m_\ell) = (m_1 \oplus k_1, \ldots, m_\ell \oplus k_\ell)$$

  with $k = (k_1, \ldots, k_\ell)$ (bitwise XOR of message & key)
- Decryption dec = enc

**Gilbert Sandford Vernam (* 1890; † 1960)**

- US engineer at AT&T Bell Labs
- Cipher patented in 1919; used by allies in WW2
- Shannon (also at Bell Labs) proved it unbreakable

## One-Time Pad

Illustration

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $m$ | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| $k$ | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| $\mathrm{enc}_k(m)$ | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| $k$ | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| $\mathrm{dec}_k(m)$ | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |

Notes

- Correctness of one-time pad obvious $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m$
- Key length = message length (biggest drawback)



## One-Time Pad

**§2.9 Theorem**

(Length $\ell$) One-time pad encryption scheme (§2.8) is perfectly secret

**Proof**

Let $c \in C$ and $m, m' \in M$. Since key distribution is uniform, we just prove

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m)\right] = \sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m')\right]$$

$\mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m)\right]$ is 1 for $k = m \oplus c$ and 0 otherwise. Hence left-hand side is 1 and with same argument also right-hand side is 1. □



## One-Time Pad

Notes

- XOR removes message bias
  (ciphertexts uniformly distributed for any message distribution)
- In general $k \leftarrow U_n$ ; $m \leftarrow \mathsf{P}_M$ ; $c = k \oplus m$ yields uniformly distributed $c$
  ($k \leftarrow U_n$ means draw $k$ from uniform distribution on $\{0,1\}^n$)
- XOR used in modern cryptography for this reason

Question

- Are uniformly distributed ciphertexts needed for perfect secrecy?

## Recall

**Definition (§2.5 Perfectly secret)**

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly secret if $O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m')$ for all messages $m, m' \in M$ and ciphertexts $c \in C$

Notes

- One-time pad is perfectly secret
- Reveals no information about message from ciphertext (Lemma §2.7)
  (length of message already part of scheme)
- Protocol-based (two-player game) characterization follows
  (as preparation for later definitions)
- Stateful algorithms
  = algorithms with persistent memory, aware of protocol step



## Perfect Indistinguishability

**§3.1 Definition (Perfect indistinguishability game)**

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme and $\mathcal{A}$ stateful probabilistic algorithm. Adversarial indistinguishability game $\text{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})$ is

$\mathcal{A}$ selects messages $m_0, m_1 \in M$ ❶

❷ $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0,1\}$
$c \leftarrow \text{enc}_k(m_b)$ sent to $\mathcal{A}$ (challenge ciphertext)

$\mathcal{A}$ outputs bit $b' \in \{0,1\}$ ❸

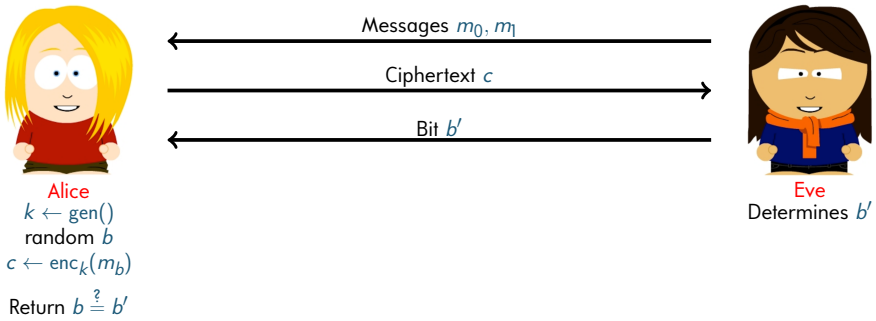
❹ Return 1 if $b = b'$ ($\mathcal{A}$ wins)
Return 0 otherwise

Notes

❶ Adversary selects messages to be distinguished
❷ System encrypts randomly selected message with random key
❸ Adversary predicts which message was encrypted based on ciphertext
❹ Adversary wins if prediction correct



## Perfect Indistinguishability






## Perfect Indistinguishability

Standard function reformulation

**Definition (§3.1 Perfect indistinguishability game)**

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be encryption scheme, $m_0, m_1 \in M$ messages, and $f : M^2 \times C \to \{0,1\}$. Adversarial indistinguishability game $\text{PrivK}^{\text{one}}(\mathcal{E}, m_0, m_1, f)$ is

❶ $k \leftarrow \text{gen}()$, uniform random bit $b \in \{0,1\}$
$c \leftarrow \text{enc}_k(m_b)$

❷ $b' \leftarrow f(m_0, m_1, c)$

❸ Return 1 if $b = b'$ ($f$ wins)
Return 0 otherwise

## Perfect Indistinguishability

**§3.2 Definition (Perfectly indistinguishable)**

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly indistinguishable if for every probabilistic algorithm $\mathcal{A}$

$$\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})\right] = \frac{1}{2}$$

Notes

- $\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})\right]$ = probability that $\mathcal{A}$ wins game
- $\mathcal{A}$ can trivially win 50% of games by returning uniform random bit $b'$
- Perfectly indistinguishable = $\mathcal{A}$ cannot do better (or worse)



## Perfect Indistinguishability

Standard function reformulation

**Definition (§3.2 Perfectly indistinguishable)**

Encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ is perfectly indistinguishable if for all $m_0, m_1 \in M$ and functions $f : M^2 \times C \to \{0,1\}$

$$\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, m_0, m_1, f)\right] = \frac{1}{2}$$

Notes

- We stick to stateful algorithms in following
- Cleaner grouping of selections (avoid quantifiers on $m_0, m_1$)



## Perfect Indistinguishability

Example: Shift cipher $\mathcal{E}$

- Adversary $\mathcal{A}$ selects messages $m_0 = aa$ and $m_1 = ab$
- Adversary $\mathcal{A}$ receives ciphertext $c = c_1 c_2$
  - Returns 0 if $c_1 = c_2$
  - Returns 1 otherwise

$$\begin{aligned}
&\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A})\right] \\
&= \frac{1}{2}\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 0\right] + \frac{1}{2}\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}) \mid b = 1\right] \\
&= \frac{1}{2}\mathrm{P}[c_1 = c_2 \mid b = 0] + \frac{1}{2}\mathrm{P}[c_1 \neq c_2 \mid b = 1] \\
&= \frac{1}{2} + \frac{1}{2} = 1 > \frac{1}{2}
\end{aligned}$$

$\to$ Shift cipher not perfectly indistinguishable



## Perfect Indistinguishability

**§3.3 Theorem**

Encryption scheme is perfectly secret iff it is perfectly indistinguishable

**Proof (1/2)**

($\to$) Let $\mathcal{A}$ be prob. algorithm, $r \in R$, and $m_0, m_1 \in M$ selected messages. Moreover, let $C_b = \{c \in C \mid \mathcal{A}_r(c) = b\}$ for all $b \in \{0,1\}$. Obviously $C = C_0 \cup C_1$. ($\mathcal{A}_r$ is de-randomized version of $\mathcal{A}$)

$$\begin{aligned}
\mathrm{P}\left[\mathrm{PrivK}^{\text{one}}(\mathcal{E}, \mathcal{A}_r)\right] &= \frac{1}{2}\mathrm{P}\left[\mathcal{A}_r(c) = 0 \mid b = 0\right] + \frac{1}{2}\mathrm{P}\left[\mathcal{A}_r(c) = 1 \mid b = 1\right] \\
&= \frac{1}{2}\Big(\sum_{c \in C_0} O_{\mathcal{E}}(c, m_0)\Big) + \frac{1}{2}\Big(\sum_{c \in C_1} O_{\mathcal{E}}(c, m_1)\Big) \\
&= \frac{1}{2}\sum_{c \in C} O_{\mathcal{E}}(c, m_0) = \frac{1}{2}
\end{aligned}$$

## Perfect Indistinguishability

### Proof (2/2)

($\leftarrow$) Suppose that $\mathcal{E}$ is not perfectly secret. Then there exist messages $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in C$ such that $O_{\mathcal{E}}(c, m_0) \neq O_{\mathcal{E}}(c, m_1)$. Consider adversary $\mathcal{A}$ that selects messages $m_0, m_1$ and then receives ciphertext $c' \in C$. If $c = c'$, then $\mathcal{A}$ returns $b' = 0$. Otherwise it returns uniform random bit $b'$.

$$\begin{aligned}
&\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}(\mathcal{E}, \mathcal{A})\big] = \frac{1}{2}\mathrm{P}[b' = 0 \mid b = 0] + \frac{1}{2}\mathrm{P}[b' = 1 \mid b = 1] \\
&= \frac{1}{2}\Big(\frac{1}{2}\mathrm{P}[c' \neq c \mid b = 0] + \mathrm{P}[c' = c \mid b = 0]\Big) + \frac{1}{4}\mathrm{P}[c' \neq c \mid b = 1] \\
&= \frac{1}{4}\Big(1 - O_{\mathcal{E}}(c, m_0)\Big) + \frac{1}{2}O_{\mathcal{E}}(c, m_0) + \frac{1}{4}\Big(1 - O_{\mathcal{E}}(c, m_1)\Big) \\
&= \frac{1}{4}\Big(2 + \underbrace{O_{\mathcal{E}}(c, m_0) - O_{\mathcal{E}}(c, m_1)}_{\neq 0}\Big) \neq \frac{1}{2}
\end{aligned}$$

□



## Limits of Perfect Secrecy

### §3.4 Theorem

If $\mathcal{E} = (\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ is perfectly secret, then $|K| \geq |\mathcal{M}|$

### Proof

By contraposition: Let $|K| < |\mathcal{M}|$ and thus $K$ is finite. Clearly, $|K| \geq 1$, so take $k \in \mathrm{ran}(\mathrm{gen})$. Similarly, take $r \in R$ and $m \in \mathcal{M}$ arbitrarily. Let $c = \mathrm{enc}(r, k, m)$, so $\mathrm{P}(k) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \neq 0$. Select $\mathcal{M}' \subseteq \mathcal{M}$ of size $|K| + 1$ arbitrarily such that $m \in \mathcal{M}'$. Consider scenario $(\mathcal{E}, \mathrm{P}_{\mathcal{M}})$ with uniform distribution on $\mathcal{M}'$. Then $\mathrm{P}(k) \cdot P(m) \cdot \mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \neq 0$ and hence $\mathrm{P}(c) \neq 0$. Let $\mathcal{M}'' = \{\mathrm{dec}_{k'}(c) \mid k' \in K\}$. Obviously $|\mathcal{M}''| \leq |K| < |\mathcal{M}'|$. Hence there exists $m' \in \mathcal{M}' \setminus \mathcal{M}''$.

$$\mathrm{P}(m' \mid c) = 0 \neq \frac{1}{|K| + 1} = \mathrm{P}(m')$$

so $\mathcal{E}$ is not perfectly secret by Lemma §2.7. □



## Limits of Perfect Secrecy

**Consequences**

- Perfect secrecy requires at least as many keys as there are messages
  ($\rightarrow$ perfect secrecy unpractical)
- One-time pad achieves optimal $|K| = |\mathcal{M}|$

**Questions**

- Can keys be reused?
  (Is one-time pad still perfectly secret
  if multiple messages are encrypted with the same key?)
- Are there other optimal perfectly secret encryption schemes?



## Limits of Perfect Secrecy

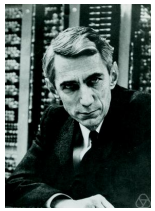
### §3.5 Theorem (Shannon's theorem)

Let $\mathcal{E} = (\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ encryption scheme with $|K| = |\mathcal{M}| = |C| = \ell \in \mathbb{N}$. Then $\mathcal{E}$ is perfectly secret iff

- $\mathrm{P}_K(k) = \ell^{-1}$ for every $k \in K$ (uniform key distribution)
- For every $m \in \mathcal{M}$ and $c \in C$ there exists unique $k \in K$ such that $\mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \neq 0$
  (det. encryption and $\mathrm{enc}(\cdot, m) \colon K \rightarrow C$ bijective for every $m \in \mathcal{M}$)

### Claude Elwood Shannon (* 1916; † 2001)

- US mathematician & electrical engineer
- Father of information theory
- Alfred-Noble-laureate (1939), but not Nobel-laureate
  (different Alfred)



© Konrad Jacobs